La Implementación de la Firma Electrónica en el Centro Nacional de Registros de El Salvador

Oscar Alejandro Martínez Peñate
José Ángel Villeda Castillo
Irma Elena Cartagena Jiménez
Daniela Antonia García de Hernández
Rutilio Selín Batres Martínez

San Salvador, El Salvador, Centro América 29 de abril de 2019

Tabla de Contenido

1. Resumen Ejecutivo

En El Salvador la implementación de la firma electrónica permite facilitar y agilizar los trámites administrativos a las personas naturales y jurídicas, es decir, obtener cualquier documento, acción o servicio de orden administrativo que brindan las instituciones del Estado.

Entre los beneficios de la firma electrónica se pueden citar: la disminución de costos administrativos, ahorro de tiempo, de espacio para la atención a usuarios, mejora el nivel de servicio al cliente, otorga seguridad en los trámites realizados, agiliza las transacciones comerciales y financieras bajo un enfoque de sustentabilidad y protege al medio ambiente con la reducción de uso de papel. Asimismo, garantiza la seguridad jurídica a los titulares de derecho, debido a que permite, no solo vincular el documento a una determinada persona o entidad, sino que impide que dicho documento sea modificado en el proceso.

Uno de los principales propósitos de este trabajo es conocer la forma en que se aplicó en otros países la firma electrónica, las buenas prácticas y dificultades presentadas en el desarrollo de la implementación, con el fin de analizar y comprender su aplicación, para tomar como base, algunos elementos para la propuesta de ejecución en el Centro Nacional de Registros (CNR) de El Salvador.

La propuesta del trabajo está orientada a que el Centro Nacional de Registros incorpore dentro de su estructura organizativa una nueva unidad encargada de proveer el servicio de certificados de firma electrónica, dirigida principalmente a brindar estos servicios a las instituciones públicas y privadas, para facilitar al ciudadano los trámites que estos deben realizar.

2. Introducción

En El Salvador, el no contar con la implementación de la *Ley de firma electrónica* y su respectivo Reglamento, causa diferentes inconvenientes al ciudadano usuario y proveedor para acceder y facilitar los bienes y servicios.

Al no disponer de la firma electrónica se obstaculiza y limita la agilidad en la realización de los trámites en la administración pública e instituciones privadas; de igual forma se produce un desperdicio innecesario, es decir, ineficiencia en el uso de los recursos materiales, infraestructura y humanos, esta situación produce un incremento del costo, pérdida del tiempo en la gestión de los trámites administrativos, y contaminación del medio ambiente.

El Ministerio de Economía (MINEC) de El Salvador como entidad raíz, trabaja en la elaboración de las normas técnicas y en la infraestructura física y tecnológica del centro primario de datos, que albergará la información de las instituciones certificadas para convertirse en proveedores de firma electrónica, mientras no se concluya con este proceso, no se podrá iniciar operaciones.

La carencia de normas técnicas impide, a las instituciones candidatas proveer el servicio de certificación de la firma electrónica, porque mientras no se disponga de un protocolo técnico a aplicar, no se tienen los requisitos respecto a la infraestructura física necesaria, la plataforma tecnológica y la seguridad informática del sistema.

El presente estudio es de tipo diacrónico, porque los procesos y dinámicas, se diagnosticarán, ejecutarán y evaluarán, de acuerdo a su desarrollo, a través de la puesta en práctica en el tiempo, es decir, en la medida que se ejecuten las diferentes etapas del proceso de implementación; se tomará como referentes los hechos de historia contemporánea de las experiencias en otros países, por ejemplo, Colombia y Costa Rica.

En El Salvador, entre los hechos históricos que conducen a la firma electrónica, se puede mencionar: la rendición de cuentas, transparencia, gobierno electrónico y modernización del Estado.

El presente estudio se realizará a partir del análisis de los hechos sucedidos en el período de los años 2009 al 2019.

Este trabajo tiene como propósito contribuir y brindar una visión sistemática que facilite la viabilidad política y técnica de la puesta en marcha de la firma electrónica en El Salvador y en particular en el CNR.

El objetivo general es conocer las condiciones económicas, financieras, técnicas y jurídicas que sirvan de base para que el CNR provea los servicios de certificados de firma electrónica, con el propósito de facilitar los trámites administrativos que realizan las personas naturales y jurídicas en las diferentes instituciones del Estado.

Objetivos específicos

- Analizar los antecedentes históricos sobre el uso y aplicación de la firma electrónica y su contribución en el gobierno electrónico.
- Conocer experiencias de la ejecución de la firma electrónica en algunos países y en particular de Costa Rica y Colombia, para analizar las mejores prácticas aplicables y la factibilidad en el CNR como proveedor del servicio de firma electrónica.
- Examinar la Ley y el Reglamento de la firma electrónica y estudiar la viabilidad de su aplicación en la provisión de servicios de firma electrónica en el CNR.
- Generar una propuesta de creación del Registro responsable de proveer los servicios de firma electrónica en el CNR.

El CNR cumple con las condiciones económicas, financieras, técnicas y jurídicas para convertirse en proveedor de servicios de certificados de firma electrónica, que facilitará los trámites administrativos que realizarán las personas naturales y jurídicas en las diferentes instituciones públicas y privadas.

Para realizar el presente trabajo se consultaron libros, tesis, artículos académicos de investigación, documentos, entre otros, para lo cual se realizaron búsquedas y revisiones bibliográficas en las principales bibliotecas de El Salvador; asimismo, se recurrió a los

repositorios digitales de las bibliotecas de Costa Rica y Colombia, se accedió a las redes sociales de investigación científica de *Researchegate* y *Academic*. Se efectuaron entrevistas a expertos en firma electrónica y a funcionarios públicos nacionales e internacionales. La investigación será cualitativa de tipo exploratoria.

3. Marco teórico

Las instituciones del Estado realizan con la práctica cotidiana, la administración pública, las cuales pueden ser funcionales o no; ya que cada institución se crea de acuerdo con una necesidad. Son eficientes cuando cumplen la misión de su fundación, en la resolución y satisfacción de las necesidades de la ciudadanía, por tal razón, la corriente de gobierno electrónico ha tomado auge.

Entre los instrumentos o medios para la modernización del Estado, se encuentra la firma electrónica, que beneficia al Estado, a los ciudadanos y a las empresas:

Estado:

- Permite mejorar los procesos de gestión interna
- Mejora la comunicación y coordinación intrainstitucional e interinstitucional
- Genera espacios de trabajo colaborativo para brindar servicios, etc.

Ciudadano:

- Posibilita la obtención de mejores servicios del Estado con reducción de tiempo y de costos.
- Fortalece la transparencia de las entidades públicas.
- Mejora la participación ciudadana al brindar nuevos espacios de diálogo horizontal, fomenta el control ciudadano y, por ende, contribuye a la gobernabilidad.

Empresas:

- Permite establecer relaciones comerciales con el Estado con mayor transparencia.
- Agiliza los procesos de los trámites tradicionales, sustituyéndolos por trámites en línea (Aliaga, 2015, p. 59).

La funcionalidad de las instituciones del Estado es el reflejo del sistema político y del modelo económico, cumplen con la finalidad de mantener y prolongar el *statu quo*, si las personas que detentan el poder político no son transparentes en el ejercicio de su rol como funcionarios públicos, no es una sorpresa que las instituciones del Estado carezcan de prácticas de rendición de cuentas. Según John Holloway (1982, p.42)): “La forma en que el Estado categoriza la realidad social y los grupos sociales y, por tanto, la forma en que se organiza en su interior, tiene una importancia política”.

El autoritarismo o la democracia al tener rango de política de Estado, se convierten en eje transversal que afecta a la ciudadanía, mediante las instituciones del Estado, porque se transforman en acciones comunes y devienen cultura, que al final se admiten como formas de vida; a la aceptación generalizada de esas prácticas se le denomina institucionalización. Para crear las condiciones que caracterizan a un Estado democrático y crear cultura de participación y agilización de las instituciones del Estado, “es necesario tomar en cuenta que, con la firma electrónica, el Estado está en condiciones de prestar los servicios las veinticuatro horas, los siete días de la semana” (López, 2007, p. 62).

El Estado no podría existir sin las instituciones que lo constituyen y viceversa, son organismos especializados que cumplen una práctica definida, que contribuyen con la estabilidad y el orden social, de no funcionar la institucionalidad del Estado se entrará en una situación caótica, es decir, la sociedad estaría en anomia, por la falta de o irrespeto de normas, es cuando el ordenamiento jurídico nacional y las instituciones estatales se encuentran en la disfunción (Durkheim, 1928, p. 90); para contrarrestar o en última instancia evitar una situación parecida, la aplicación de un gobierno electrónico podría, en cierta medida contribuir al buen funcionamiento de las instituciones (Reyes, 2002, p. 88)

El Poder Ejecutivo, a través de las instituciones estatales pone en marcha sus políticas públicas, planes y programas de gobierno; asimismo son las entidades encargadas de organizar y normar la estructura macro social, que va más allá de un período presidencial, la administración pública es permanente, mientras que los lapsos presidenciales son temporales, situación que afecta la eficiencia de las instituciones estatales, porque la ejecución de los programas gubernamentales en términos generales son de corto plazo, significa, que periódicamente se cambian las políticas y directrices de funcionamiento de las instituciones del Estado.

El proyecto de firma electrónica es una medida de largo plazo, lo que significa, que trasciende los períodos de gobierno, porque está enfocada en satisfacer las necesidades del Estado, del ciudadano y de la empresa privada, y los beneficios que obtienen estos sectores se pueden observar en el cuadro siguiente:

Cuadro 1. Beneficios de la Firma Electrónica

Sectores	Beneficios
El Estado	Desarrollo del Gobierno Electrónico. Agilización de Trámites de forma electrónica serán electrónicos bajo infraestructura segura Desarrollo del Expediente Clínico Digital Certificado, Recetas Electrónicas. Compras Gubernamentales sin papel. Historial Académico Digital Certificado. Relaciones de Compra Venta y pagos entre el Gobierno y el Sector Privado. Voto Electrónico Certificado Digitalmente y para consultas ciudadanas sobre proyectos e iniciativas de ley. En general todo tipo de actividad electrónica que requiera identificación y certificación. Desarrollo de la Factura Electrónica para la inclusión del Sector Informal a los beneficios de la tributación y desarrollo de la Llave Fiscal. Trazabilidad de todos los actores que interactúan con el Gobierno bajo una Infraestructura de Clave Pública (PKI). Impacto directo en el indicador de *"DoingBusiness".*
El Ciudadano	Seguridad Jurídica en su identidad Facilidad en el uso de las tecnologías de la información para todo trámite legal con el Gobierno y las empresas. Expediente clínico digital y certificado para el ciudadano. Seguridad Jurídica en sus transacciones y/u operaciones financieras o administrativas, tanto con el Gobierno como con empresa privada. Protección y Certeza Jurídica ante los fraudes. Una sola ventanilla para todos sus trámites = Su Computador y su Certificado Digital.
La Empresa Privada	Desarrollo del Comercio Electrónico Seguridad Jurídica en todas las transacciones financieras, legales y administrativas. Seguridad plena en el uso de software certificado digitalmente para la administración de recursos financieros y de gestión administrativa. Facilitación de Trámites Gobierno Ciudadano Empresa Certeza Jurídica para trámites internacionales y ahorro en el manejo documental.

Fuente: elaboración propia, datos proporcionados por el Ministerio de Economía de El Salvador.

Entre los beneficios generales de la puesta en práctica de la firma electrónica se encuentran:

- Conveniencia de una identificación personal con un solo número.

> • Utilización de inspección delictiva utilizando el esquema de la base de datos del ciudadano.
>
> • Información auténtica acerca del ciudadano y el movimiento de residentes de una localización a otra.
>
> • Establecimiento de un gobierno eficiente al utilizar el servicio de administración nacional, tales como: las elecciones, seguridad e impuestos.
>
> • Instalación de una política nacional efectiva y eficiente.
>
> • Provisión del servicio de administración en línea con información apropiada compartida entre los ministerios (SNAP, 2014, p. 12)

El usuario de las instituciones del Estado es el principal afectado, por el cortoplacismo del programa de gobierno del partido político que accede a la presidencia, la improvisación, deficiencia y cambios abruptos en las instituciones; aunado a la falta de una carrera de la función pública, da como resultado una débil institucionalidad, que le dificulta reinventarse, generar procesos dinámicos-evolutivos y mecanismos de mejora continua.

> Talcott Parsons hablaba de un conjunto de prerrequisitos funcionales universales que resultan imprescindibles para que todo el sistema social tenga un orden persistente, dicho de un modo que todo el mundo pueda entender, son aquellas prácticas que una sociedad debe cumplir para que la sociedad pueda seguir funcionando con normalidad (Barajas, 2013, p. 12)

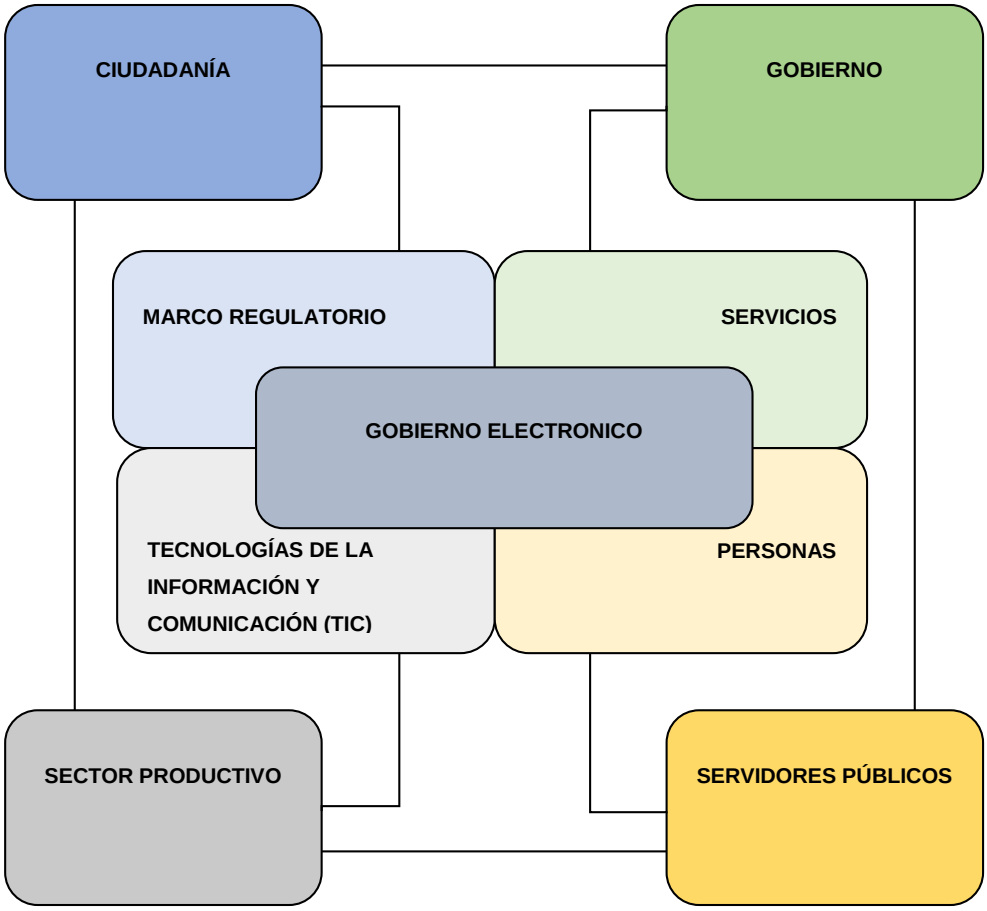
El Estado ha evolucionado, la administración pública y obviamente los recursos o instrumentos para brindarle un mejor servicio a la ciudadanía, así tenemos la utilización de las tecnologías de la información y de la comunicación; de igual forma, la digitalización de los procesos administrativos públicos.

> Pensar y diseñar los servicios desde el origen en formato digital, poniendo en el centro a la ciudadanía, para que podamos prestar servicios de forma personalizada y proactiva, y contar con un modelo de arquitectura de las TIC

> que permita la integración de procesos, información, personas y ahora también «cosas».
>
> Implementar procedimientos electrónicos continuos, de extremo a extremo, accesibles y usables (Moro, 2017, p. 524).

Las instituciones del Estado se han ido complejizando, cada vez más, debido al aparecimiento de prácticas y fenómenos que se suscitaron en la modernidad y contemporáneamente en el posmodernismo, aunado a los avances tecnológicos y científicos, en donde las nuevas tecnologías de la comunicación y de la información en un contexto digital juegan un papel importante, de tal forma, que las tradicionales filas de usuarios en las ventanillas de atención al público, algunas de ellas se han trasladado a la *web* y ahora se realizan vía internet.

Figura 1. Actores y relaciones del gobierno electrónico



Fuente: elaboración propia, datos tomado de SNAP, *Plan Nacional de Gobierno Electrónico 2014 – 2017*, Quito, Secretaria Nacional de la Administración Pública, 2014.

La evolución de las instituciones del Estado, requiere de personal especializado, para ser más eficientes en el desarrollo de su labor burocrática, el nuevo ingreso de funcionarios a las instituciones de Estado, ha dejado paulatinamente de ser a través del compadrazgo, tráfico de influencias, nepotismo, etc.

Es la población la que, de manera informal, mediante la utilización de los servicios de las instituciones del Estado, comprueba si funcionan o no. Los usuarios son los que tienen

una vigilancia y control permanente de la institucionalidad estatal, esta actitud es la que (Foucault, 1980, p. 88) le denomina panoptismo, “De tal modo que, si se quiere captar los mecanismos de poder en su complejidad y en detalle, no se puede uno limitar al análisis de los aparatos del Estado solamente”.

La eficiencia de las instituciones del Estado no se logra a través de *marketing* en medios de comunicación, no se trata de hacer conciencia en la población, para que ésta se convenza de que la institucionalidad del Estado cumple su función de servicio público.

El usuario es precisamente, el que demanda los servicios que prestan las instituciones, y constata el real desempeño de estas, realizar campañas de publicidad y de propaganda, en ocasiones podría ser una estrategia para tratar de dar una imagen, a través de la cual se engaña a la población, con esto lo más probable es que se indigne, al evidenciar, una vez más, la falta de ética de los funcionarios públicos.

Por lo general, las instituciones públicas son el reflejo del tipo del sistema político y del modelo económico, las instituciones influyen en la normalización de las conductas de los funcionarios, la relación funcionario e institución, no es solo de infraestructura, es sobre todo, de dinámicas y procesos sociales, que se sustentan en un ordenamiento jurídico, en un contexto de Estado de derecho.

La disfuncionalidad de las instituciones públicas se puede dar, entre otros, por las razones siguientes:

- La contratación irresponsable de los futuros servidores públicos, que pueden carecer de ética, moralidad y capacidad profesional.
- La falta de evaluaciones periódicas del cumplimiento de sus funciones, por tal razón se debe de, “institucionalizar la evaluación con el propósito de garantizar la eficiencia y eficacia en la prestación de servicios públicos” (Villacorta, 2016, p. 70)
- Ausencia de una política institucional de planes y programas de capacitación *ad hoc.*
- La falta de planes y programas de modernización continua y digitalización de los sistemas que sustentan los procesos de la administración pública.

Las instituciones cumplen su cometido, cuando hay satisfacción del usuario externo, cuando el funcionario público es diligente y expedito en el trámite burocrático o en la prestación de servicios; asimismo, cuando los usuarios son tratados de igual forma y no existen ciudadanos de primera y segunda clase, es decir, sin privilegios ni impunidades de ninguna naturaleza, cuando en la institucionalidad del Estado priva la justicia y la equidad, entonces podríamos afirmar que la institución es eficiente y democrática.

Es de hacer notar, que el funcionamiento de la institucionalidad del Estado, también va a tener una influencia en el ideario de la sociedad, como una manifestación abstracta, consecuencia de la participación de las instituciones en la formación de la cultura nacional, en calidad de agentes secundarios de socialización.

> En ocasiones se encuentra una teorización explícita de concepto de ciudadanía como es el caso del ensayo clásico de T.H. Marshall, *Citizenship and Social Class* (La Ciudadanía y las Clases Sociales), que saluda (*sic*) la extensión gradual de la ciudadanía a todos los aspectos de la sociedad moderna. Sin embargo, es más frecuente que se le dé por descontado; el hecho que la administración pública se interese por la relación entre el Estado y sus ciudadanos es considerado tan obvio que ni siquiera se le reserva una mención aparte (Holloway, 1982, p. 25).

Las acciones sociales del funcionamiento de las instituciones son la objetivación de esa entidad intangible denominada Estado, esas acciones se convierten en conductas públicas consuetudinarias, que pasan a ser parte de la cultura de la sociedad, es decir, que la ciudadanía, al final, las concibe como una práctica consustancial a la sociedad. “Es mediante el inconsciente estatal que se organiza, se fundan las pautas sociales y se niega el proyecto mismo de la sociedad, pero que a la vez se da cabida a procesos instituyentes distintos” (Gil y Manero, 2012, p. 12).

La reforma administrativa al interior de las instituciones del Estado genera relaciones interpersonales conflictivas, no solo porque al funcionario se le sacará de su área de confort, de realizar los trámites de forma similar por décadas, en esos micro espacios

sociales se dan antagonismos ideológicos, sin bien es cierto, que la mayoría de los burócratas se les puede circunscribir como sectores medios sociales, provenientes de los estratos de menos ingreso económico, pero algunos de ellos defienden y se identifican con los intereses de los grupos de poder económico (Gil y Manero, 2012, p. 12).

Al eliminar las trabas burocráticas, modernizar los sistemas en los que se basan los procesos de los servicios públicos, ordenar y convertir a las instituciones del Estado en eficaces y eficientes, por regla general se requiere, entre otros, de uniformar los procesos, mecanismos, reglas y las normas, para eliminar la corrupción, las arbitrariedades del empleado público y disminuir al mínimo el libre albedrío del funcionario, que afecta negativamente al usuario, por no haber certeza en la gestión administrativa que él tramita en determinada institución estatal. “El institucionalismo normativo fundamenta el cambio en armonizar las reglas, identidades y situaciones, a partir de reformas que consideren la cultura organizacional que se pretenda modificar” (Gil y Manero, 2012, p. 12).

CAPÍTULO I

Breve esbozo histórico de la implementación de la firma electrónica

La importancia que existe en las legislaciones que regulan las actividades relacionadas con transacciones electrónicas, en un entorno cada vez más interconectado y globalizado, son de mayor relevancia a nivel institucional; la firma electrónica es una de las herramientas más importantes en este ámbito, en el contexto de la modernización del Estado.

En diversos países se han creado normas, y adoptado tecnologías en la prestación de bienes y servicios públicos que, permiten asegurar la validez de un documento firmado electrónicamente, y a su vez, que se gesten procesos donde las administraciones públicas puedan ser más eficientes y eficaces, con un enfoque de modernización del Estado.

A raíz de lo anterior, diversos organismos ligados al derecho y las TIC comenzaron a discutir estas materias a partir de 1995, registrándose avances importantes en los marcos jurídicos respectivos. Uno de los organismos internacionales más importantes para el desarrollo de la firma electrónica es la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL), que ha propiciado una estructura legal marco.

La estructura legal de la UNCITRAL ha dado relevancia a los aspectos mínimos que debe incluir una legislación sobre firma electrónica, la neutralidad tecnológica, la equivalencia funcional que consiste en que los documentos firmados electrónicamente, como los

equivalentes en papel, poseen igual valor y la autonomía de la voluntad; sin dejar de lado la soberanía de la que gozan todas las partes interesadas, para la correcta y homogénea adopción a nivel mundial, en las legislaciones que las caracterizan.

La implementación histórica de la regulación de la firma electrónica provee una perspectiva de las legislaciones de esta firma en el mundo. Como un punto de inflexión en la forma de hacer las cosas, desde 1997, se inicia la agilización de los procesos comerciales, y se adoptan las firmas electrónicas como una necesidad de los nuevos tiempos; en la creciente implementación de gobiernos y comercio digitales, ver el cuadro siguiente:

Cuadro 2. Implementación histórica de la regulación de la firma electrónica 1997-2003

PAISES	AÑO	MES
Italia	1997	Mayo
Alemania	1997	Noviembre
Puerto Rico	1998	Agosto
Singapur	1999	Febrero
Austria	1999	Mayo
Colombia	1999	Agosto
España	1999	Septiembre
Estados Unidos	2000	Enero
Inglaterra	2000	Febrero
Francia	2000	Marzo
Japón	2000	Abril
México	2000	Mayo
Australia	2000	Junio
Perú	2000	Junio
Bélgica	2000	Julio
Ecuador	2001	Febrero
Canadá	2001	Marzo
Venezuela	2001	Marzo
Panamá	2001	Junio
Brasil	2001	Agosto
Argentina	2001	Diciembre
Finlandia	2003	Enero

Fuente: elaboración propia, datos obtenidos en el Ministerio Secretaría de la Presidencia, Modelos de firma electrónica simple para la Administración Pública, Santiago de Chile, Unidad de Proyectos de Reforma y Modernización del Estado de Chile, 2004.

Los gobiernos y las empresas han recurrido al uso de la firma electrónica, desde la década de los noventa. Así, en septiembre del año 2000, el presidente de los Estados Unidos, Bill Clinton, junto con el primer ministro irlandés Bertie Ahern, utilizaron, por primera vez en la historia, una firma electrónica para suscribir un tratado en materia de comercio electrónico entre ambos países. En la misma línea, las demás regiones del mundo comienzan sus propios procesos hacia la modernización del Estado. (FUSADES, 2015, p. 5)

1.1 La firma electrónica como un medio de modernización del Estado

En Latinoamérica todavía existe una gran distancia entre las diferentes administraciones públicas, donde los documentos en soporte de papel proliferan en las organizaciones gubernamentales, y lo que podría ser la gestión documental digital, los sistemas híbridos están más cerca de la realidad, sin perjuicio de avanzar en el uso de los documentos electrónicos.

Las condiciones particulares de cada país, permiten crear y adoptar la infraestructura tecnológica, física y de seguridad apropiadas para desarrollar la gestión documental por medios electrónicos; algunos países cuenta con el marco regulatorio jurídico necesario para la implementación de la firma electrónica; cada vez surgen innovaciones informáticas que resuelven los escollos detectados para mejorar los accesos a los servicios que brindan las instituciones del Estado, la seguridad en la obtención de la información, entre otros, situación que contribuye a la modernización del Estado.

Respecto de la autenticidad y la conservación prolongada de los documentos digitales continúan como temas polémicos, además, de riesgosos para la gestión documental en las administraciones públicas, con la eliminación de los papeles, aunque no se deja de reconocer las grandes ventajas de la gestión por estos medios digitales para los múltiples servicios que el Estado está obligado a ofrecer al ciudadano.

Situación que hace necesario estudiar los diferentes procesos de modernización del Estado que han existido en América Latina, según las normativas más relevantes para cada gobierno en la búsqueda de ser más eficientes y digitales, como se muestra en el siguiente cuadro

:

Cuadro 3. Normativas sobre firmas electrónicas en Argentina, Brasil, México, Colombia y Costa Rica

País	Ley o Norma de Firma Electrónica
Argentina	Ley 25506 del 2001 – Ley de Firma Digital, reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.
Brasil	Decreto Ley 3.996 de 2001 y Decreto Ley 4.414, de 2002. Regula la prestación del servicio de certificación digital de firma electrónica. Se ha intentado promover proyectos en materia de Ley de Comercio Electrónico, pero el país considera suficiente la normativa existente en otras normas que han habilitado el uso de firma electrónica, además de contar ya con decretos en materia específica que regulan dicha prestación de servicio. Brasil es un país de la región que se reconoce por la masificación efectiva del uso de firma electrónica avanzada, exigiendo su uso en materia tributaria.
México	Ley de Firma Electrónica Avanzada de 2012. Corresponde a una nueva Ley de Comercio Electrónico que incluye modificaciones al Código Civil y otras leyes que le dan marco jurídico a la firma electrónica. Regula el uso de la firma electrónica avanzada en los actos previstos en la Ley y la expedición de certificados digitales, servicios relacionados con la firma electrónica avanzada y su homologación.
Colombia	Ley 527 de 1999. Ley de Validez Jurídica y Probatoria de los mensajes de datos. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones. Colombia ha desarrollado infinidad de habilitantes normativos que han permitido ir abonando un camino hacia la masificación.
Costa Rica	Ley 8454 de 2005 - Ley de Certificados, Firmas Digitales y Documentos Electrónicos Establece el marco jurídico general para la utilización segura de los documentos electrónicos y la firma digital en las entidades públicas y privadas

Fuente: Secretaría Permanente del Sistema Económico Latinoamericano y del Caribe, Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe, Caracas, SELA, 2012.

Los países de Argentina, Brasil y México se tomarán en cuenta a continuación, en este trabajo, por considerarlos referentes de la modernización del Estado en América Latina en la puesta en práctica de la firma electrónica:

1.1.1 Argentina

En Argentina la *Ley N° 11.672, Complementaria Permanente de Presupuesto,* emitida

en 1995, fue sustituida en su Art. 49, por el Art. 30 de la Ley 24.624 Presupuesto de la Administración Nacional del mismo año. Esta última, legisló sobre el uso de los medios informáticos para la documentación financiera y demás documentación relacionada con el accionar de la administración, como contratos y convenios, inclusive los formatos indirectos en copia.

La documentación sujeta al funcionamiento del Estado Nacional, permite la generación de un valor agregado en el manejo y control de la información en formato digital, inclusive, la información proveniente de las relaciones comerciales. La normativa complementaria exige que se garantice la estabilidad y la perdurabilidad; asimismo, la uniformidad e integridad de la información digital.

Los documentos originales de primera generación digital u óptico indeleble, y los reproducidos con las mismas características, serán considerados originales con valor probatorio, de acuerdo con el Art. 995 del *Código Civil*. Asimismo, este señala que los documentos originales redactados o producidos en primera generación en cualquier medio de soporte, una vez reproducidos, pierden su valor jurídico y podrán ser destruidos, previa anulación. La norma incluye documentos que sustentan derechos y obligaciones a ser conservados solo por medios digitales.

La *Ley 25.506, de Firmas Digitales,* del 12 de noviembre del 2001, estableció el uso de la firma digital y la firma electrónica. El *Reglamento de la Ley, Decreto 2628/2002,* del 19 de diciembre de 2002, en su Art. 4°, normas técnicas, determinó que el Gabinete de Ministros va a definir la normativa aplicable a los procesos técnicos para la generación, comunicación y archivo de los documentos digitales.

Se podrán obtener copias auténticas, a partir de los originales firmados digitalmente. La certificación de autenticidad se hará de conformidad con el Art. 41, del Reglamento donde se incide en la necesidad de que la Jefatura de Gabinete de Ministros promoviera el uso masivo de la firma digital, para el trámite de expedientes y establecer los períodos de uso para la totalidad de la infraestructura digital (Mendoza, 2010, pp. 12-14).

1.1.2 Brasil

El *Decreto No. 3.505/2000, Política de seguridad de la información en las instituciones que comprenden la Administración Pública Federal*, que tiene como supuestos básicos concienciar a la administración pública sobre la importancia de la información digital y los riesgos que conlleva, el Art. 3°, legisla sobre las garantías para la información, asegurando la confidencialidad, integridad, autenticidad, no repudio y disponibilidad de los datos e información, promueve la modernización del Estado encaminados a la nueva implementación sobre gobierno electrónico en los aspectos del manejo y vida útil, así como de la calidad de la información y la transparencia.

El *Decreto No. 3.996 Prestación de servicios de certificación digital en el ámbito de la Administración Pública Federal*, del 31 de octubre del 2001, norma en el Art. 3°, la tramitación de documentos electrónicos en los que sea necesario usar certificados digitales.

La *Medida Provisoria N° 2.202-2 Infraestructura de claves públicas*, del 24 de agosto del 2001, regula el uso del certificado electrónico y la firma digital, confiriendo autenticidad, integridad y validez jurídica de los documentos electrónicos (Mendoza, 2010, pp. 14-15).

1.1.3 México

El *Decreto del 8 de abril de 2003*, reformó el *Código de Comercio* en materia de firma electrónica. El Art. 89, incluye a la firma electrónica y la firma avanzada que permiten en procesos jurídicos, los mismos efectos que la firma autógrafa, son admisibles como prueba en juicio, y la avanzada agrega una posibilidad de control exclusivo del firmante y que sea posible detectar cualquier alteración de la firma. En el *Código Federal de Procedimientos Civiles* se adicionó el Art. 210-A, que a partir de su segundo párrafo, demanda la fiabilidad del método en que se generó la información para gozar de fuerza probatoria, además debe ser accesible para posterior consulta siempre que se mantenga íntegra.

Algunas instituciones comenzaron con un proceso de digitalización en los procesos administrativos y de prestación de bienes y servicios, enfocados en una gestión de documentos electrónicos en la administración pública hacia un gobierno electrónico, dentro de esas instituciones se encuentran: las Secretarías de Contraloría y Desarrollo Administrativo, Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación, Salud, Trabajo y Previsión Social, la Administración Pública Estatal y Municipal (Mendoza, 2010, pp. 24-25).

1.1.4 Antecedentes de la firma electrónica en El Salvador

La creciente implementación de tecnologías en las actividades comerciales, para la integración a un mundo globalizado, y específicamente en la vía de comercio electrónico en El Salvador, es uno de los factores que ha impulsado la creación de la *Ley de firma electrónica,* debido a que es un mecanismo importante en el comercio nacional y exterior en la actualidad.

“En 1999 en El Salvador se desarrolló un sistema de teledespacho que permitía transmitir electrónicamente cualquier documento requerido para realizar operaciones de comercio exterior” (FUSADES, 2015, p. 5)

El Ministerio de Hacienda (MH) desarrolló el sistema junto con la Cámara de Comercio e Industria de El Salvador, a través de la Dirección Estratégica de Comercio Electrónico (DIESCO), esta era la encargada de ejecutar la parte técnica y de autenticar la persona remitente de la información.

No obstante, *la Ley de simplificación aduanera* requiere que esta información se presente y conserve el documento en original; en el año 2001, existió la necesidad de reformar dicha Ley, para establecer, que los documentos contenidos en un soporte magnético, digital o electrónico produjeran los mismos efectos jurídicos que los escritos en un soporte de papel.

Además, para poder garantizar la autenticidad e integridad de los documentos electrónicos, fue necesario incorporar el reconocimiento y validez legal de la firma

electrónica. En octubre de 2015, la Asamblea Legislativa aprobó la *Ley de firma electrónica*, la cual establece como objetivo principal en el Art. 1, otorgar el mismo valor jurídico de la firma autógrafa a la firma electrónica simple y a la firma electrónica certificada (Asamblea Legislativa de El Salvador, 2015).

CAPÍTULO II

Acciones y dinámicas para hacer funcional la firma electrónica en el CNR

2.1 Preámbulo necesario de la firma electrónica en el CNR

En el siglo XXI, se vive una era de amplias relaciones económicas, financieras y comerciales globales, donde las personas ya no se limitan a efectuar sus actividades y transacciones en su espacio físico, ni en su territorio.

A cada instante se realizan cientos o miles de acuerdos comerciales a través de la internet, que según lo cita Nóres González, 2002 en *La Firma Digital y Administraciones públicas*, “es un canal de comunicaciones que incluye a múltiples redes, interconectadas entre sí, que facilita la difusión de información, la extensión del comercio electrónico, así como la prestación de servicios públicos a ciudadanos y empresas por parte de la Administración”. Esta tendencia del uso de la tecnología lleva a muchas personas naturales y jurídicas, a aprovechar las ventajas de los medios electrónicos, por ser medios más agiles, eficientes, cómodos, diversos y adaptables a las necesidades de cada persona.

El CNR, teniendo en cuenta que el desarrollo de las tecnologías de información y comunicación se han convertido en un factor estratégico para mejorar la eficiencia, fomentar la competitividad y el crecimiento económico del país, así como para elevar la calidad de vida de los ciudadanos, ha iniciado un proceso de análisis interno y externo para fortalecer su capacidad instalada, así como preparar las condiciones necesarias para acreditarse como prestador de servicios de certificados de firma electrónica,

regulado en el Art. 43 y siguientes de la *Ley de firma electrónica*, y/o como prestador de servicios de almacenamiento de documentos electrónicos, contenido en el Art. 52 y siguientes de la referida Ley, en el marco del *Decreto Legislativo N° 133*, aprobado por la Asamblea Legislativa y publicado en el *Diario Oficial* N° 196, Tomo N° 409, con fecha 26 de octubre de 2015.

La evidencia histórica e internacional dice que este tipo de emprendimientos infraestructurales no pueden ni deben ser carentes de planeación en su despliegue. Son articulaciones de capital financiero y regulatorios que deben aprovechar la "visibilidad tecnológica" de la que hoy se goza para su optimización productiva y social.

Una de las cuestiones más específicas que toda organización debe tener en cuenta a la hora de operar en Internet, es que para que el comercio electrónico pueda desarrollarse plenamente, es necesario que las transacciones electrónicas ofrezcan el mismo nivel de seguridad y confianza que las relaciones tradicionales. Es decir que se requiere, crear la seguridad necesaria en las relaciones que surgen entre dos partes que operan a través de Internet.

Para poder asimilar los efectos de firmar manuscritamente con los de firmar digitalmente, se deben obtener las garantías que ofrece el hecho de firmar de forma manuscrita, es decir, que deberá garantizarse, principalmente, la autenticidad, integridad y confidencialidad de los mensajes que circulan por la Red, para que ni el remitente pueda negar haber enviado un determinado mensaje después de hacerlo, ni el destinatario pueda negar haberlo recibido, cuando tal recepción se haya producido (Lomascolo, 2003, p. 58).

La firma es la prueba de la manifestación de la voluntad que permite atribuir la autoría e identificar al firmante de un instrumento. La firma electrónica es un método o símbolo, que se basa en medios electrónicos, utilizado o adoptado por una persona con la intención de vincularse o autenticar un documento (Irigoitia, 2016, p.35). Es una forma de manifestar la voluntad, a través de un conjunto de datos asociados a un documento en medios o formatos electrónicos que permiten lo siguiente:

- La identificación de la persona que lo “firma” (en el concepto tradicional del término de forma manuscrita), pero en un ámbito digital y, además, se identifica de manera inequívoca.

- Asegurar la integridad del documento que ha sido firmado, es decir, que es el mismo que el autor firmó en su momento y este no ha sido alterado de ninguna manera (supongamos una solicitud de un servicio firmada por una persona, se debe garantizar que lo que se lee, es lo que la persona aceptó al firmar digitalmente el documento).

- Garantizar el “no repudio” del documento firmado. Es decir, como la firma solo puede ser emitida por el usuario autorizado, no es posible negar que se ha firmado el documento si realmente se ha hecho.

Un certificado de firma electrónica, es un documento electrónico expedido por una entidad autorizada para proveer de una certificación que identifica a una persona (física o jurídica) con un par de claves, la pública y la privada, estas tienen como misión validar y certificar que una firma electrónica se corresponde con la persona o entidad concreta, este es el servicio que el CNR, aspira a proveer al ciudadano, como una contribución a la modernización del Estado.

Una firma digitalizada, se trata de una simple representación gráfica de la firma manuscrita obtenida a través de un escáner, que puede ser “pegada” en cualquier documento. Esta técnica la empezaron a utilizar masivamente los expertos en *marketing* cuando la publicidad circulaba por correo postal ordinario (*Snail mail*).

En la práctica, la firma que utiliza la mayoría de ciudadanos para la realización de diversos trámites, tanto ante el Ministerio de Hacienda, como en otras instituciones públicas, e incluso, para uso interno de las propias empresas o el correo electrónico seguro, es la firma electrónica simple conocida también con el nombre de firma digital.

Actualmente, existe la posibilidad de obtener lo que se llama una firma digitalizada, mediante el uso de los *pads* o tabletas de firmas.

A la hora de analizar la seguridad de las tabletas de firma, es necesario diferenciar entre las que sólo captan una imagen de la firma (se emplean en algunos negocios) y las que además tienen la capacidad de obtener los datos biométricos (presión, velocidad, coordenadas de la firma). Estas últimas, con la calidad suficiente, permiten la posterior identificación del firmante con las mismas garantías que una firma sobre papel.

Estas soluciones de firma pueden utilizarse para captar una imagen de firma o, acompañadas del *software* adecuado, firmar y almacenar un documento en formato digital protegiendo su integridad y garantizando que se detecte cualquier manipulación posterior del mismo. La seguridad a aplicar dependerá del tipo de documento que se deba firmar y la seguridad que cada institución o cada empresa decida aplicar al proceso.

Por ejemplo, si se requiere la máxima seguridad, los datos biométricos deben transmitirse encriptados a la PC (computadora personal). Las tabletas más avanzadas, como las de *Step Over*, ya incorporan esta característica, fundamental para impedir que en ningún momento los datos biométricos puedan ser capturados en un entorno inseguro.

Se trata de una solución que, correctamente aplicada, presenta ventajas frente a la firma mediante *smartcard*/DNI (Lector de tarjeta inteligente/Documento Nacional de Identidad), por ejemplo, por su universalidad de uso. No requiere que el firmante disponga de un certificado, que lo tenga actualizado o no y, además, lo lleve consigo en el momento de efectuar la firma.

En resumen, la firma electrónica es una alternativa dentro de un contexto de la modernización del Estado, un sistema seguro y que puede ser complementario a la firma reconocida mediante *smartcard* o DNI electrónico, por lo que no necesariamente sustituye o dificulta el uso de esta. En cambio, su sencillez para el usuario puede contribuir y complementar este sistema ayudando a lograr una auténtica oficina que la base sea sin papel. El CNR al tomar la decisión de proveer la firma electrónica debe tomar en cuenta los aspectos tecnológicos antes mencionados.

2.2 Condiciones favorables que contribuyen para que el CNR sea proveedor de Certificados de Firma Electrónica

El Centro Nacional de Registros fue creado por medio del *Decreto Ejecutivo No. 62*, de fecha 5 de diciembre de 1994, publicado en el *Diario Oficial* No. 227, Tomo No. 325, del 7 de diciembre de dicho año; en la actualidad es una entidad descentralizada adscrita al Ministerio de Economía (MINEC), con autonomía administrativa y financiera. Actualmente, la integran los procesos misionales siguientes: Registro de la Propiedad Raíz e Hipotecas, Registro de la Propiedad Intelectual, Registro de Comercio, Registro de Garantías Mobiliarias y el Instituto Geográfico y del Catastro Nacional.

Las estrategias definidas en el Plan Estratégico Institucional por los altos funcionarios del CNR, favorecen a la institución para implementar la firma electrónica en los principales procesos misionales; asimismo, para la creación de una nueva unidad que provea los servicios de firma electrónica.

Las estrategias definidas son las siguientes:

- Fortalecimiento de la transparencia institucional, rendición de cuentas y participación ciudadana.
- Desarrollo integral del recurso humano.
- Renovación de la gestión institucional y de la calidad en el servicio.
- Fortalecimiento del proceso de autosostenibilidad institucional.
- Renovación de los recursos tecnológicos.
- Consolidación de la imagen y posicionamiento institucional.
- Actualización del marco legal aplicable a la Institución

2.2.1 Acciones a considerar para implementar la infraestructura PKI (Public Key Infrastructure)

Este análisis sobre los aspectos técnicos, se basan en una propuesta de Términos de referencia para la contratación de servicios profesionales y de consultoría para el diagnóstico, propuesta de implementación, documentación técnica y capacitación para la implementación de firma electrónica en el CNR, elaborado por el Ministerio de Economía (MINEC) y el Programa de cooperación de Estados Unidos de América- El Salvador a través del Fondo del Milenio, denominado FOMILENIO II, del año 2018.

El CNR requiere describir los procedimientos técnicos para la ejecución de las "Ceremonias de Claves", en la cual se producirá la generación del par de claves criptográficas y el correspondiente certificado de Proveedor de Servicios de Certificación, conforme a los siguientes criterios:

1. Alineamiento con lo estipulado en CEN/TS 419 261:2015 –*Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures.*

2. Alineamiento con lo estipulado en EN 319 411-1:2016 – *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.*

3. Alineamiento con los requisitos de política y seguridad definidos por la Unidad de Firma Electrónica del MINEC para las instalaciones donde se alojará la Infraestructura de Clave Pública de los Proveedores de Servicios.

4. Vigencia tecnológica para el momento en que se tome la decisión de implementar la firma electrónica.

2.2.2 Acciones internas para la ejecución de la firma electrónica en el CNR

La unidad organizativa que se encargará de implementar la firma electrónica debe cumplir al menos dos condiciones, primero cumplir con los requisitos para certificarse como proveedor de firma electrónica; segundo, elaborar un plan de negocios, que

permita precisar la estructura, el formato de dirección, el diseño conceptual de los procesos, cómo desarrollar el negocio y hacerlo rentable y de utilidad pública, conforme a los criterios siguientes:

- Particularidades del diseño de la tecnología a implementar, según el mercado y procesos internos de la institución.

- Alinear los requisitos de política y seguridad definidos por la Unidad de Firma Electrónica del Ministerio de Economía para las instalaciones donde se alojará la Infraestructura de clave pública de los proveedores de servicios.

- Realizar un estudio de mercado, descripción de la organización y gestión, los productos y/o servicios, la estrategia de comercialización, las proyecciones financieras básicas: flujo de caja, presupuesto y gastos, y el detalle de la inversión inicial.

- Interoperabilidad, según las prácticas existentes a la fecha de implementación en la región centroamericana.

Las capacidades institucionales indican que el CNR tiene condiciones favorables para convertirse en proveedor de servicios de certificación; pero para tomar la decisión definitiva, es necesario disponer de una evaluación técnica y una formulación metodológica que permita una adecuada implementación de PKI en el CNR. Una vez ejecutado lo anterior, el CNR podrá con mayor seguridad avanzar en la hoja de ruta que se ha trazado.

2.2.3 Acciones de formación del recurso humano en el CNR

Es importante que en la hoja de ruta se considere el desarrollo de un programa de capacitación que deberá estar destinado para el personal y ejecutado por la Escuela de Formación Registral (ESFOR) del Centro Nacional de Registros, debiendo considerar formación en temas técnico-jurídicos en materia de firma electrónica, certificados digitales, infraestructura de clave pública, política de certificación, declaración de práctica

de certificación, almacenamiento de documentos electrónicos, sellos de tiempo y cualquier otro modelo de negocio que se considere pertinente.

El programa de capacitación debe considerar los temas siguientes:

a) Nociones básicas de infraestructuras de Clave Pública

- Componentes principales
- Autoridad de Certificación Raíz
- Autoridad de Certificación Subordinada
- Autoridad de Registro
- Autoridad de validación
- Otros componentes de la infraestructura
- Autoridad de sellado de tiempo
- Sistemas de firma desatendida o masiva
- Dispositivos criptográficos de creación de firma
- Declaración de prácticas de certificación y política de certificación
- Almacenamiento de documentos electrónicos

b) Implementación de la PKI

- Sitio primario
- Sitio alterno
- Arquitectura lógica
- Respaldo sitio primario

- Arquitectura jerárquica
- Perfiles de certificados
- Listas de Revocación de Certificados (CRL)
- Protocolo de Estado de Certificado en Línea (OCSP)

c) Administración del proveedor de servicios de certificación

- Funciones post implementación del proveedor de servicios de certificación
    i. Identificación y autenticación del suscriptor y sujeto
    ii. Ciclo de vida del certificado
    iii. Controles operacionales, de gestión y de las instalaciones: de seguridad física, procedimientos, personal, archivo de registros, cambios de clave, recuperación de desastres, terminación de una autoridad de registro o del proveedor de servicios, etc.
    iv. Controles técnicos de seguridad
    v. Asuntos comerciales y legales: precio del certificado, confidencialidad, privacidad de la información, garantías, limitaciones de responsabilidad legal, indemnizaciones, resolución de disputas, etc.
- Gestión y emisión de certificados de los usuarios finales
- Divulgaciones a los clientes
    i. Definición de los servicios básicos, derechos y responsabilidades de los suscriptores y las partes que confían
- Servicio y soporte del suscriptor

i. Definición de los servicios de soporte al suscriptor

ii. Definición de políticas y procedimientos para servicios de soporte

- Suspensión y revocación de certificados

i. Procedimiento para la revocación o suspensión de un certificado

ii. Definición de políticas para suspensión / revocación de certificados

iii. Definición de problemas de monitoreo de manera oportuna

- Proceso de solicitud a las partes que confían

i. Definición de políticas y procedimientos que minimizan el riesgo para el Proceso de Solicitud de Certificados (PSC) en casos asociados con el procesamiento de solicitudes por parte de terceros con respecto al estado de los certificados individuales

d) Firma electrónica y otros servicios de certificación

- Requerimientos para firmar electrónicamente documentos y transacciones: dispositivos, certificados y aplicaciones

- Funcionamiento de la firma electrónica y su validación: las funciones de hash (algoritmos que aseguran que con la respuesta nunca se podrá saber cuáles han sido los datos insertados), el cifrado asimétrico, la composición de la firma, los perfiles y formatos estándar de firma electrónica (XAdES CAdES y PAdES*: Advanced Electronic Signatures* para ficheros pequeños, grandes y en formatos PDF).

- Escenarios de firma electrónica:

i. Interactiva: PC, dispositivo móvil

ii. Desatendida: firma masiva de procesos y documentos

iii. Otros servicios de certificación

1. Servicios de sellado de tiempo
2. Servicios de digitalización y almacenamiento de documentos electrónicos

e) Experiencias de implementación en otros países

- Casos de éxito y de fracasos, lecciones aprendidas
- Planes de implementación y despliegue que se han realizado
- Modelos de negocio implementados
- Administración de fianzas
- Términos y condiciones

2.3 Análisis comparativo de la implementación de la firma electrónica en Costa Rica y Colombia

2.3.1 Costa Rica

Marco Jurídico

En Costa Rica, *la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley 8454)* es firmada el 22 de agosto de 2005. Esta Ley faculta la posibilidad de vincular jurídicamente a los actores que participan en transacciones electrónicas, lo que permite llevar al mundo virtual transacciones o procesos que anteriormente requerían el uso de documentos físicos para tener validez jurídica, bajo el precepto de presunción de autoría y responsabilidad, además lo anterior sin demérito del cumplimiento de los requisitos de las formalidades legales según negocio jurídico.

En Costa Rica, mediante la *Ley 8454*, establece un marco jurídico para el uso de la firma digital especificando que es “cualquier conjunto de datos adjunto o lógicamente

asociados a un documento electrónico, que permitan verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico". Esta ley establece únicamente el concepto de Firma Digital, por lo que no considera en el contexto legal el uso del término de firma electrónica para efectos legales.

Con el establecimiento de esta ley, se permite a las personas tanto físicas como jurídicas en tener la opción de no trasladarse a las instituciones para la realización de trámites financieros, legales, artísticos, u otros. Así, el uso de la firma digital en documentos electrónicos garantiza:

- Autoría: la información del documento y su firma electrónica que corresponden indudablemente con la persona que ha firmado.
- Integridad: la información contenida en el texto electrónico, no ha sido modificada luego de su firma.
- No repudio: la persona que ha firmado electrónicamente no puede negar la autoría.

La firma digital se basa en el uso de la criptografía, que es la ciencia de cifrar y descifrar información utilizando técnicas matemáticas, para garantizar el intercambio de información segura. Específicamente se utiliza el método asimétrico, el cual consiste en la generación de dos claves o llaves digitales a saber:

- Llave privada: la cual es almacenada por el dueño de la firma digital y no deberá ser compartida a ninguna otra personal.
- Llave pública: la que es conocida y distribuida a las personas que se relacionan con el dueño de esta llave.

Existen varios tipos de firmas digitales:

1. Firma digital simple: incluye un método de identificar al firmante (autenticidad).

2. Firma digital avanzada: además de identificar al firmante (firma digital simple), permite garantizar la integridad del documento a lo largo del tiempo.

3. Firma digital reconocida: es una firma digital avanzada donde se utiliza un dispositivo seguro para su creación y certificados cualificados, se conoce como firma digital segura.

En la actualidad, el uso de firma electrónica puede tener muchas funcionalidades, algunas son:

1. Sellado de tiempo.

2. Firma Web Seguro.

3. Firma PDA.

4. Firma *WebSite*.

5. Evidencias Electrónica.

6. Digitalización Certificada.

7. Establecimiento de conexiones seguras entre personas

8. Establecimiento de conexiones seguras entre dos servidores

Entidades Involucradas

- Dirección de Certificadores de Firma Digital (Ministerio de Ciencia y Tecnología).

- Banco Central de Costa Rica: Autoridad Certificadora para la emisión de certificados de firma digital para personas físicas (CA SINPE - Persona Física) y Autoridad Certificadora para personas jurídicas (CA SINPE- Persona Jurídica).

- Red de agencias bancarias

- Institución homóloga del CNR, el Registro Nacional de Costa Rica ya opera como usuario de firma electrónica, oportunidad para conocer su experiencia.

Desafíos a superar

La Dirección de Certificadores de Firma Digital de Costa Rica, solicitó colaboración al Centro de Informática (CI) de la Universidad de Costa Rica, con el propósito de desarrollar un componente que permita aplicar firma electrónica XADES-XL en documentos ODF (*Open Document Format*), debido a que dentro de la herramienta ofimática LibreOffice u *OpenOffice* no se contaba con un componente de tal alcance, únicamente se tiene firma digital básica, la cual permite firmar un documento electrónico, pero no garantiza el documento a lo largo del tiempo, como sí lo hace la firma electrónica XADES-XL .

Por lo anterior, se da inicio en el año 2013 por el CI, la investigación y desarrollo de un componente de firma avanzada para documentos de formato abierto. Para este desarrollo, la Dirección de Certificadores de Firma Digital de Costa Rica, indica la disponibilidad del código fuente de la plataforma de firma digital del gobierno Belga, el cual se puede tomar como base inicial para la implementación de dicho componente.

Esta plataforma ofrece varios servicios, algunos de ellos son:

1. eID Trust Service: servicio que permite realizar la validación de los certificados emitidos, por la estructura del certificado del gobierno.

2. eID Identity Provide: permite proveer a los ciudadanos del gobierno una herramienta de autenticación de los ciudadanos que tienen firma electrónica.

3. eID Digital Signature Service: le permite a los ciudadanos firmar documentos electrónicos y verificar firmas a documentos electrónicos firmados.

4. eID Middleware: ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas.

Así se da inicio al proyecto de “Implementación de Componente para firma electrónica XADES-XL para Libre Office”, donde reúne a un equipo de profesionales en TIC para la especificación del componente y se contrata a un desarrollador para la implementación del mismo. El objetivo del proyecto fue “desarrollar un componente para firmar documentos con formato *Open Document*”, tales como: documento de texto (.odt), hoja electrónica (.ods), presentación (.odp) y diseño de dibujos (.odg), estableciendo inicialmente los siguientes requerimientos:

1. Multiplataforma: debe ser soportado en los sistemas operativos de mayor uso a saber: Windows, Linux.

2. Lectura de firma: debe permitir hacer lectura de la firma por medio del dispositivo lector instalado en el computador.

3. Lista de firmas: debe permitir mostrar una lista de las firmas que han sido aplicadas al documento que está abierto.

4. Aplicar firma a un documento: debe de aplicar el algoritmo de firma electrónica (XADES-XL) al documento y ser almacenado dentro de este, con un archivo con formato “xml” establecido para almacenar firmas digitales.

5. Verificar las firmas de un documento: Debe realizar el proceso de verificación de una o de varias firmas del documento.

Teniendo definido los requerimientos de funcionalidad del componente, se establecen las siguientes etapas para su implementación, a saber:

1. Componente para Libre Office: se hace una investigación para identificar cómo se crea una extensión para Libre Office u Open Office, donde se genera el documento Creación de extensiones para Libre Office 4.X.

2. Algoritmo de firma de documentos y verificación de documentos: se realiza una extracción del código para firmar ODF de la plataforma belga, generando el código necesario para que sea funcional en un computador.

3. Creación del Componente para Libre Office: se crea la primera versión del componente de Libre Office, el cual es funcional en plataformas MS-Windows y GNU/Linux.

El producto final de esta primera versión es la arquitectura del componente de firma Xa DES-XL para Libre Office.

2.3.2 Colombia

La Ley 527 (e-comerce), por medio de la cual, se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales fue aprobada el 18 de agosto de 1999. Esta norma presenta en su Art. 2, literal c, una definición para firma digital "como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

Por su parte, el *Decreto 2364*, promulgado en el año 2012, por medio del cual se reglamenta el artículo 7° de la *Ley 527,* del año 1999, sobre la firma electrónica y se dictan otras disposiciones, en su Art. 1, define a la firma electrónica como: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permiten identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Mediante el *Decreto 1747,* emitido en el año 2000, se regularon de manera detallada aspectos relacionados con las entidades de certificación, los certificados y las firmas digitales. En la actualidad existen tres entidades de certificación abierta.

Entidades involucradas

La entidad de certificación, expide actos denominados Certificados, los cuales son manifestaciones hechas como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las claves criptográficas y la integridad de un mensaje de datos.

El artículo 365 de la *Constitución Política* hace referencia al tema de los servicios públicos, los cuales pueden ser prestados, tanto por las entidades públicas como las privadas o conjuntamente.

Esta norma permite que este servicio lo presten los particulares, si reúnen los requisitos exigidos por la ley y cuenta con la aprobación de la Superintendencia, organismo rector para todos los efectos.

El proyecto de ley señala que podrán ser entidades de certificación, las Cámaras de Comercio y en general las personas jurídicas, tanto públicas como privadas, autorizadas por la Superintendencia respectiva, que cumplan con los requerimientos y condiciones establecidos por el Gobierno Nacional, con fundamento en el artículo 31 del proyecto.

Una vez las entidades de certificación sean autorizadas, podrán realizar actividades tales como, emitir certificados en relación con las firmas digitales; ofrecer o facilitar los servicios de creación de firmas digitales certificadas; servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos; servicios de archivo y conservación de mensajes de datos, entre otras.

De forma paralela con las actividades definidas anteriormente, estas entidades tendrán deberes que cumplir frente a los involucrados dentro del proceso mercantil, deberes atinentes a cada una de las actividades que pretendan ejercer.

En consecuencia, las entidades de certificación, son las encargadas, entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto grado de confiabilidad, lo que las

hace importantes y merecedoras de un control ejercido por un ente público, control que redunda en beneficio de la seguridad jurídica del comercio electrónico.

La comisión redactora del proyecto de ley, consideró que la Superintendencia de Industria y Comercio debe ser la entidad encargada del control y vigilancia de las entidades de certificación, por cuanto su competencia es afín con estas labores.

La función que actualmente ejercen las Superintendencias y que les fue delegada, le corresponde constitucionalmente al Presidente de la República como Suprema Autoridad Administrativa, cuando señala que una de sus funciones es la de ejercer la inspección y vigilancia de la prestación de los servicios públicos.

En razón a que la naturaleza de las funciones de las entidades de certificación se considera como la prestación de un servicio público, la inspección y vigilancia de los servicios públicos que tienen que ver con la certificación, actividades que ejercerán las entidades de certificación, debe radicarse en cabeza de una Superintendencia como la de Industria y Comercio.

Desafíos a superar

Hay una variedad de tendencias en la innovación digital y el entorno regulador. Las principales conclusiones son las siguientes:

1. Existe un fuerte movimiento hacia un enfoque centrado en el ciudadano o el usuario, ya que los servicios en línea del gobierno electrónico se reconocen como un paso hacia la participación electrónica;

2. El reconocimiento y aplicación de las mejores prácticas es necesario para la mejora futura del gobierno móvil, a través del uso de teléfonos inteligentes como parte del marco del gobierno electrónico;

3. Existe una falta de cooperación efectiva y productiva entre los sistemas de gobierno electrónico central y local. Es urgente la coordinación entre las principales partes interesadas para reducir la duplicación de esfuerzos;

4. Se requiere evaluar las actividades de gobierno electrónico y crear un nuevo modelo de gobierno digital integral para alcanzar los Objetivos de Desarrollo Sostenible de las Naciones Unidas en este sector.

5. El papel del gobierno electrónico en el tratamiento del envejecimiento de la sociedad como cuestión mundial ha comenzado a recibir atención e interés.

6. Calidad del servicio de gobierno electrónico evaluada por un modelo de *marketing*

7. Impacto de la política nacional en el desarrollo del gobierno electrónico local

8. Utilidad del gobierno electrónico como nuevo mecanismo de lucha contra la corrupción

9. Uso de tecnologías emergentes como IOT y *Big Data* en *e-government*

El CNR al tomar la decisión de proveer el servicio de la firma electrónica en sus procesos, debería tomar en consideración la experiencia del Registro Nacional de Costa Rica, en la transformación del ordenamiento jurídico, para darle agilidad a la puesta en práctica de la firma electrónica.

El CNR como proveedor debería tomar en consideración la formación de alianzas con la academia y empresas nacionales de ciencia y tecnología, entre otros, porque se necesita que de forma conjunta se satisfaga las demandas de los usuarios; asimismo mantener una actualización, desarrollo e innovación continua del proceso de firma electrónica, en el contexto de la modernización del Estado.

CAPÍTULO III

Análisis de la Ley y el Reglamento de la Firma Electrónica en El Salvador

Para la elaboración de este capítulo, se consultó un estudio realizado por un equipo de funcionarios del CNR, que llevó a cabo el análisis de la *Ley y el Reglamento de la firma electrónica*, para determinar o identificar las siguientes propuestas de reformas para ambos instrumentos jurídicos que se deben abordar, con el objetivo de garantizar el éxito en la implementación del proyecto.

3.1 Observaciones Generales.

1. Desbalance entre Ley y Reglamento. Un proyecto de Reglamento de 41 artículos busca ser el instrumento que orienta la aplicación de una Ley de 71 artículos. Este desbalance en el contenido de ambos instrumentos jurídicos genera una especie de "déficit reglamentario".

En efecto, el *Reglamento*, de acuerdo a lo regulado en el Art. 68 de la Ley de Firma Electrónica, es de carácter aplicativo, por lo que el contenido de este debe desarrollar de manera amplia los principios regulados en la referida ley.

A la luz del contenido del Reglamento, se considera que a este le faltan algunos aspectos que de acuerdo a la Ley, deben de ser contemplados en el mismo, por lo que se sugiere agregar más disposiciones que faciliten su aplicación.

2. Técnica jurídica con posibilidad de mejora. El Reglamento tiene 41 artículos integrados en VIII Títulos, la mayoría de los cuales no tiene Capítulos, por lo anterior se recomienda una estructuración con base a Capítulos.

Además, se recomienda ordenar los contenidos del Reglamento de la siguiente manera:

- **Parte sustantiva:**
    a. Disposiciones generales respecto al Reglamento y la Ley;
    b. Disposiciones específicas respecto al servicio;
    c. Disposiciones específicas respecto a los proveedores;
    d. Disposiciones específicas respecto a los usuarios del servicio; e,
    e. Institucionalidad.
- **Parte procedimental:**
    a. Procedimientos de acreditación;
    b. Procedimientos de certificación;
    c. Procedimientos de atención a los usuarios;
    d. Procedimientos de reclamos;
    e. Procedimientos sancionatorios;
    f. Recursos; y,
    g. Disposiciones finales.

3. Garantizar reglamentación complementaria simultánea. El Art. 68 de la Ley, señala que además del Reglamento de Aplicación que emitió el presidente de la República, en un plazo no mayor a ciento ochenta días contados a partir de la vigencia de la Ley, la Unidad de Firma Electrónica tendría que haber emitido las normas y reglamentos técnicos necesarios y a la fecha esto no se ha cumplido.

En el texto del Art. 5 del Reglamento, no queda claro que la Unidad elaborará en el referido plazo, las normas y los reglamentos técnicos necesarios en coordinación con el Organismo Salvadoreño de Reglamentación Técnica (OSARTEC) y el Organismo Salvadoreño de Normalización (OSN).

Para la comprensión y uso de la firma electrónica se hace necesario la emisión de las normas y reglamentos técnicos para facilitar la operativización de la firma electrónica.

4. Riesgo en la seguridad jurídica. Es básico que un Reglamento de aplicación desarrolle aspectos centrales sobre la recepción y resolución de denuncias, sin embargo, el Art. 7 del Reglamento solo señala que la Unidad establecerá procedimiento para atención de denuncias, lo que puede dar espacio para discrecionalidades y hasta a posibles riesgos de inconstitucionalidad por presunta falta de seguridad jurídica.

5. Imprecisión técnica en algunas disposiciones. Por ejemplo, el Art. 8 del Reglamento establece que la fianza será 5% del activo del prestador del servicio; si eso aplicara al CNR como proveedor de servicios de firma electrónica, que posee un activo de $79.3 millones dólares (US) al 31 de diciembre del año 2018, la fianza a aplicar sería de $3.9 millones de dólares. El mismo artículo establece que en ningún caso la fianza no podrá ser mayor a 2000 salarios mínimos del sector comercio y servicio.

3.2 Observaciones Específicas.

En las Disposiciones Generales debería reglamentarse puntos contenidos en la Ley que requieren mayor desarrollo, por ejemplo, los temas de “Neutralidad tecnológica y equivalencia funcional” haciendo referencia a organismos internacionales o modelo de estandarización a implementar, así como sobre las “Reglas para el tratamiento de datos personales”, entre otros.

Art. 2: El catálogo de las definiciones es muy escueto y en algunos casos con conceptos diferentes a los que están en la Ley, por lo que se sugiere ampliar y armonizar contenidos.

Es conveniente utilizar un mismo término para los prestadores o proveedores de servicios, ya que en algunos artículos del Reglamento se hace referencia a ellos como “Proveedores de Servicios de Certificación” y otras disposiciones lo mencionan como “Prestadores de Servicios”, por lo que se sugiere unificar el concepto a “Proveedores”, tal como lo menciona la Ley.

Art. 3: Se propone que el ámbito de aplicación debe separar en artículos diferentes lo relativo a los sujetos, el alcance de los marcos normativos y reglamentos técnicos y las atribuciones del ente regulador.

Para el inc. 2 se propone modificar la redacción de la siguiente manera: “Las normas técnicas, los reglamentos técnicos y lineamientos que se emitan por la Unidad para la aplicación del presente Reglamento y de la Ley, son de obligatorio cumplimiento para los proveedores de servicios acreditados de conformidad con la Ley de Firma Electrónica”.

Art. 4: El acápite se refiere a “Requisitos para el Encargado de la Unidad de Firma Electrónica”, pero en el desarrollo del artículo y el inc. 6 del Art. 10 se menciona el puesto de Director, por lo que hay que hacer la corrección para que toda la redacción esté unificada con el término de encargado.

Respecto a los requisitos, se sugiere que se armonicen con los requisitos para Directores del MINEC. También se propone incluir aspectos más objetivos entorno a las capacidades, por ejemplo experiencia mínima en algún área determinada.

Asimismo, se sugiere ampliar las incompatibilidades e inhabilitaciones para ejercer el cargo de encargado de la Unidad de Firma Electrónica.

Art. 6: En el inc. 2do se sugiere establecer que la inspección ordinaria se realizará a través de una visita anual como mínimo y un requerimiento semestral de información; asimismo, referir que la auditoría es una inspección extraordinaria.

También se sugiere regular los procedimientos y formalidades a cumplir en las inspecciones, por ejemplo: actas, modo de acreditar a los inspectores, regularidad de las inspecciones, etc., así como aclarar más los términos aplicables para la realización de inspecciones y auditorías.

Art. 7: Sugerimos que el Reglamento como mínimo debería desarrollar el tema del procedimiento de atención de denuncias y regular los recursos.

Art. 9: Se considera que los requisitos de la fianza son muy generales y podrían detallarse más en el Reglamento.

Título III: En primer lugar se recomienda que este Título, ordene y separe los requisitos para la acreditación y de los procedimientos, así como establecer las posibilidades de resolución y modos de proceder, en caso de observaciones e inconformidades a las resoluciones de sustanciación y de las que ponen fin al proceso.

Art. 14: Sugerimos que el Reglamento no solo relacione los requisitos para la acreditación establecidos en la Ley, sino que debería detallarlos más, ya que por ejemplo, queda la duda de cuáles serían las normas técnicas aplicables.

Art. 15: En el inciso 1º. menciona que la solicitud podrá ser presentada a la Unidad de forma física o digital; sin embargo, al no tener autorizada aún la firma electrónica, el Proveedor sólo podría presentarla en formato físico; por lo que deberá eliminarse la presentación digital en ese primer momento.

En el literal b) se exige certificación que muestre conformidad con estándares internacionales reconocidos y eso implicaría contratar a un especialista internacional que certifique eso, lo que encarecería el servicio a prestar. Además, cabe preguntarse quién será el organismo que valorará la idoneidad de los prestadores de servicios de certificaciones con estándares internacionales y las prácticas a las que deberá someterse para su obtención.

Es importante conocer qué tipo de certificaciones deben obtenerse para los servicios y para los dispositivos y saber si ofrece la posibilidad de hacer uso de infraestructura o servicios tecnológicos prestados desde el extranjero.

Art. 16: En caso que el dictamen de la Unidad de Firma Electrónica sea desfavorable al proveedor, cabe las preguntas: ¿Se puede recurrir?, ¿A qué instancia? Sugerimos reglamentar sobre este tema.

Art. 22: Sobre la Declaración de prácticas de certificación, se requiere claridad para la preparación de *software, hardware*, políticas de certificación o de emisión y aplicativos.

Art. 25: La redacción no es muy clara. Se sugiere ampliar los mecanismos de protección de datos en caso de cierre o liquidación de las empresas proveedoras o en caso de incumplimientos a los usuarios, estableciendo criterios para la determinación de la responsabilidad.

También recomendamos incorporar una redacción similar para proveedores de servicios de almacenamiento.

Se observa que ni en el Título IV ni en el Título V se encuentran desarrollados los efectos jurídicos del cierre de un proveedor de servicios, aunque la Ley sí tiene regulaciones al respecto, sugerimos reglamentar este tema.

Art. 23, numeral 13, en este artículo se utiliza el término "Revocación"; considerando que la Ley, en los artículos 60 y 61, hace referencia a la palabra "Cancelación", se sugiere armonizar conceptos y causales de la cancelación, siguiendo y desarrollando la disposición contenida en la Ley.

Al relacionar este artículo con el Art. 23 numeral 10 del Reglamento, se deduce que viabiliza gestionar la solicitud de suspensión y/o cancelación de un certificado digital por la vía telefónica. Por ello, se sugiere definir el procedimiento de atención de dichas solicitudes con el objetivo de prevenir que personas distintas al titular sean quienes hagan la gestión actuando en contra de la voluntad del titular.

Consideramos que sería conveniente que la llamada telefónica sea para prevención o alerta y no para suspensión; se podrían dar 24 o 48 horas para que se presente solicitud de suspensión por escrito.

Art. 31: Sugerimos incluir en el inciso último los requisitos y procedimientos para la conservación de documentos electrónicos.

Art.39: Se propone revisar y aclarar la redacción de este artículo, debido a que puede entenderse de formas diferentes:

- Que los certificados electrónicos que serán utilizados por funcionarios y empleados públicos deberán de contener la fecha y hora de emisión del documento (¿A cuál documento se refiere?) y los límites establecidos según el cargo a desempeñar; o,

- Que los documentos que funcionarios y empleados públicos firmen electrónicamente contengan la fecha y hora en que los documentos fueron emitidos y los límites establecidos del firmante.

Si la segunda interpretación es la correcta, entonces hay que agregar que para incorporar información adicional a los documentos habrá que contemplar que no todos los formatos de archivos electrónicos permiten incorporar información adicional (metadata), por lo que el reglamento técnico de la ley debería de especificar los formatos de archivos electrónicos que deberán de utilizarse, señalando que podrá ampliarse a otros formatos en actualizaciones de los reglamentos técnicos.

Este análisis jurídico le permite al CNR conocer los vacíos y riesgos de la Ley y el Reglamento que se deben superar para tomar la decisión de convertirse o no en proveedor de servicios de firma electrónica; asimismo, si continúa las gestiones para la obtención del financiamiento que se requiere para la implementación del proyecto de la firma electrónica. Es condición *sine quanon* considerar superar los vacíos y tomar en cuenta las observaciones realizadas.

CAPÍTULO IV

Registro de Servicios de Firma Electrónica en el CNR

4.1 Elementos de la administración del CNR que favorecen la prestación de los servicios de firma electrónica.

Los constantes cambios en el entorno, obligan a los miembros de las organizaciones, tanto públicas como privadas a reflexionar y definir acerca de cuál es el papel que representan o quieran desempeñar en su entorno. Asimismo, se ven obligados a analizar hacia dónde se dirigen, es decir tener claridad del presente y del futuro, para definir cómo cumplir su misión y visión acorde a las exigencias de los nuevos tiempos.

Para instituciones como el Centro Nacional de Registros, generar un pensamiento estratégico le ha garantizado, a medida que avanza el tiempo, lograr la consolidación de unas bases fuertes en sus procesos administrativos, operativos y financieros, cimentados en los análisis que conlleva todo proceso de planificación estratégica y que contribuye a decidir, si el proyecto que se propone desarrollar es válido o no, si se justifican sus procedimientos y si el camino es el acertado para reducir la incertidumbre, minimizar los riesgos y maximizar las oportunidades (Román, 2010, p.27).

Para una institución como el CNR, adquiere mucha importancia el pensamiento estratégico, porque le permite, entre otros, los tres estadios siguientes:

1. Identificar los factores de éxito, para implementar políticas, programas y servicios asociados con el cumplimiento de su misión y visión, a partir de la focalización de los recursos para satisfacer las demandas de los usuarios; la determinación de los

recursos que deberá prever para la consecución de sus objetivos (eficacia) y de los recursos que serán necesarios para lograr impacto (eficiencia).

2. El aprovechamiento de las experiencias y redes, que facilita sus áreas de actuación, respecto a los servicios registrales que el CNR brinda a los ciudadanos, aprovechando las relaciones intergubernamentales que se generan de la gestión en red, que forman parte de su entorno.

3. La búsqueda de nuevas líneas de acción, ya que, ante el intento de alcanzar una ventaja competitiva ante las demandas y exigencias de los servicios, surge la innovación como una alternativa para lograr una mayor legitimidad. Para el CNR, la definición de las estrategias que requiere para ser una institución exitosa, conducen a adaptar y aprovechar la mejor combinación de los recursos existentes. Mediante la reflexión estratégica, a las instituciones públicas se les facilita “identificar y experimentar nuevas ideas, gracias a la innovación” (Román, 2010, p.24).

Para el CNR proyectarse como un proveedor de servicios de certificación de firma electrónica, constituye una línea de oportunidad, ya que es una institución sólida que ofrece sus servicios en los 14 departamentos del país: San Salvador, La Libertad, Santa Ana, Ahuachapán, Sonsonate, Chalatenango, San Vicente, La Paz, Cuscatlán, Cabañas, Morazán, Usulután, San Miguel y La Unión.

El CNR cuenta con los recursos siguientes:

- Una planta de personal de 1,824 plazas autorizadas por el Ministerio de Hacienda.
- En lo financiero se percibe un ingreso anual promedio de 45.7 millones de dólares.
- El patrimonio del CNR tiene un valor de 50.3 millones de dólares.
- Un activo total de 79,3 millones de dólares, según el Balance General y Estados de resultados al 31 de diciembre de 2018 de la Unidad Financiera del CNR.

La administración de las instituciones constituye el modo de lograr que las cosas se realicen de la mejor manera posible, para ello se requiere optimizar los recursos

disponibles que permitan alcanzar los objetivos previstos. La administración, de acuerdo a (Chiavenato, 1994, p. 90) debe coordinar los recursos organizacionales, como los humanos, materiales o físicos, financieros, mercadológicos y administrativos para lograr los objetivos institucionales.

4.2 Propuesta para la creación del Registro de Servicios de Firma Electrónica (RESEFE) en el CNR

De acuerdo con los requisitos establecidos en el Art.43 de la *Ley de Firma Electrónica de El Salvador*, para que el CNR implemente la firma electrónica como proveedor de servicios de certificación, se presenta a continuación, una propuesta para la creación del Registro de Servicios de Firma Electrónica que será responsable de proveer servicios de certificados de firma electrónica.

La propuesta incluye, entre otros, las herramientas gerenciales para su funcionamiento, según se detalla a continuación:

a. Pensamiento Estratégico de Registro de Servicios de Firma Electrónica
b. Mercado potencial
c. Variables de la mezcla de mercado
d. Perfiles y cargos del Registro
e. Estructura organizativa del Registro
f. Proceso para la prestación de servicios de Certificados de Firma Electrónica.

a. Pensamiento Estratégico de Registro de Servicios de Firma Electrónica

En el marco de la propuesta de la creación del Registro responsable de brindar el servicio de firma electrónica, la definición del pensamiento estratégico se vuelve de capital importancia, debido a que le permite definir con claridad su razón de ser, hacia dónde se proyecta, por qué lo hace, así como los valores que orientarán su accionar. El enfoque

estratégico permite “aproximarse a la visualización y construcción de su futuro, para determinar sus mayores propósitos y las estrategias que orientarán la adquisición, uso y control de los recursos, para lograr sus objetivos” (Ramírez, 2009, p. 54).

Tomando en cuenta lo antes expuesto, se propone la misión, visión y valores del Registro de Servicios de Firma Electrónica, que se presentan a continuación:

Misión

Proveer bienes y servicios de firma electrónica a personas naturales o jurídicas, con la infraestructura tecnológica que cumpla con los estándares internacionales de seguridad, que satisfagan las necesidades de los clientes y usuarios, con eficiencia.

Visión

Ser el proveedor líder en la prestación de servicios de firma electrónica en El Salvador.

Valores

- Excelencia en la prestación del servicio
- Innovación tecnológica
- Confianza jurídica y en la prestación de los servicios
- Seguridad en todos los procesos

b. Mercado potencial

Los clientes potenciales a los que se les ofrecerá los servicios de certificados de firma electrónica son las instituciones del Estado y sus funcionarios:

- Poder Ejecutivo
- Poder Legislativo
- Poder Judicial

c. Variables de la mezcla de mercado

La Unidad deberá tomar en cuenta para la distribución, promoción y comercialización de los servicios que brindará, las variables de mercadeo que se detallan a continuación:

- Producto

Estrategia: Producto nuevo – Certificados de firma electrónica

Objetivo: Identificar la firma electrónica certificada como un producto original, así como identificar a la institución como el primer proveedor de servicios de certificación.

Táctica: Establecer la marca y características de la firma electrónica.

- Precio

Estrategia: Precio accesible para la masificación del uso del certificado de firma electrónica.

Objetivo: Definir un precio que contribuya al desarrollo económico y social del país.

Táctica: Establecer el precio que incentive a la población a adquirir el servicio del certificado de firma electrónica para realizar sus transacciones comerciales, financieras y diferentes trámites en las instituciones del Estado.

- Plaza

Estrategia: El CNR será el principal proveedor de servicio de certificados de firma electrónica para las instituciones del Estado orientado a los siguientes segmentos del mercado: Poder Ejecutivo, Poder Legislativo y Poder Judicial.

Objetivo: Definir los canales de distribución, promoción y comercialización de los productos y servicios.

Táctica: Establecer un canal directo: entre el CNR, el sector académico y las empresas de asesoría y proveedores de tecnología que permitan conocer las necesidades de las instituciones de los segmentos que requiere el mercado meta.

- Promoción

Estrategia: Las herramientas a utilizar en la mezcla de mercado permitirán el posicionamiento de la marca como proveedores del servicio.

Objetivo: Conocer a los clientes potenciales del servicio que ofrece la Institución para que se sensibilicen y concienticen de las bondades que tiene ser un usuario de los certificados de firma electrónica.

Táctica: Utilizar las herramientas promocionales: publicidad, promoción de ventas, relaciones públicas, *marketing* directo y venta personal, para sensibilizar al cliente sobre los beneficios de utilizar el certificado de la firma electrónica.

- Personal

Estrategia: Funcionarios de los segmentos identificados, así como usuarios internos del CNR.

Objetivo: Establecer la estructura organizativa y perfiles de puestos de la Unidad del Registro de Servicios de Firma Electrónica.

Táctica: Definir una estructura organizativa y desarrollar programas de sensibilización y capacitación dirigidos al personal técnico-operativo de la unidad y a los usuarios.

- Procesos

Estrategia: Conjunto de procedimientos establecidos para obtener el Certificado de firma electrónica.

Objetivo: Elaborar un diagrama del proceso, mediante el cual el personal que se desempeñe en la unidad proporcionará el Certificado de firma electrónica al cliente-usuario que cumpla con los requisitos y requiera el servicio.

Táctica: Definir el diagrama del proceso que permitirá la emisión, renovación y revocación del Certificado de firma electrónica.

- Evidencia Física

Estrategia: El diseño de las instalaciones físicas de la Unidad.

Objetivo: Generar un impacto positivo y confiable en la primera impresión que perciban los usuarios que visiten las instalaciones donde se brinde el servicio.

Táctica: Tomar en cuenta aspectos como la imagen, condiciones de las instalaciones, el mobiliario de interiores, el equipo, identificación de las áreas, los materiales impresos y otras señales visibles que ofrecen evidencia tangible y de confiabilidad del servicio ofertado.

d. Perfiles y cargos del Registro

La Unidad requerirá personal que posea una formación académica, experiencia y competencias específicas para la ocupación y desempeño de los puestos que se proponen. El perfil para cada puesto es el siguiente:

1. Ejecutivo del Registro de Servicios de Firma Electrónica

- Formación académica: Licenciatura en Administración de Empresas con Maestría en Dirección de Empresas, Finanzas y/o Gerencia Social.
- Experiencia: Con 5 años de experiencia en cargos de dirección y 3 años en temas de firma electrónica.
- Competencias: Habilidades para Comunicación, Negociación y manejo de conflictos, Planificación y administración, Administración de proyectos, Desarrollo del equipo, manejo de relaciones interpersonales, manejo de medios de comunicación social.

2. Jefe/a de la unidad de Mercadeo de Servicios de Firma Electrónica

- Formación académica: Licenciatura en Mercadeo o en Administración de Empresas.
- Experiencia: Con 3 años de experiencia en temas de mercadeo de servicios.
- Competencias: Trabajo en equipo, Identificación y compromiso, Orientación a la calidad, Orientación al cliente, Orientación a resultados, Innovación, Planificación y administración.

3. Jefe/a de Servicios Legales y Administrativos

- Formación académica: Licenciatura en Ciencias Jurídicas, Abogado y Notario, con postgrado en Administración y Gerencia Pública.
- Experiencia: Con 3 años de experiencia como Abogado y Notario.
- Competencias: Trabajo en equipo, Identificación y compromiso, Orientación a la calidad, Orientación al cliente, orientación a resultados, habilidad para relacionarse, Negociación, manejo y resolución de conflictos.

4. Jefe/a de Soporte Técnico

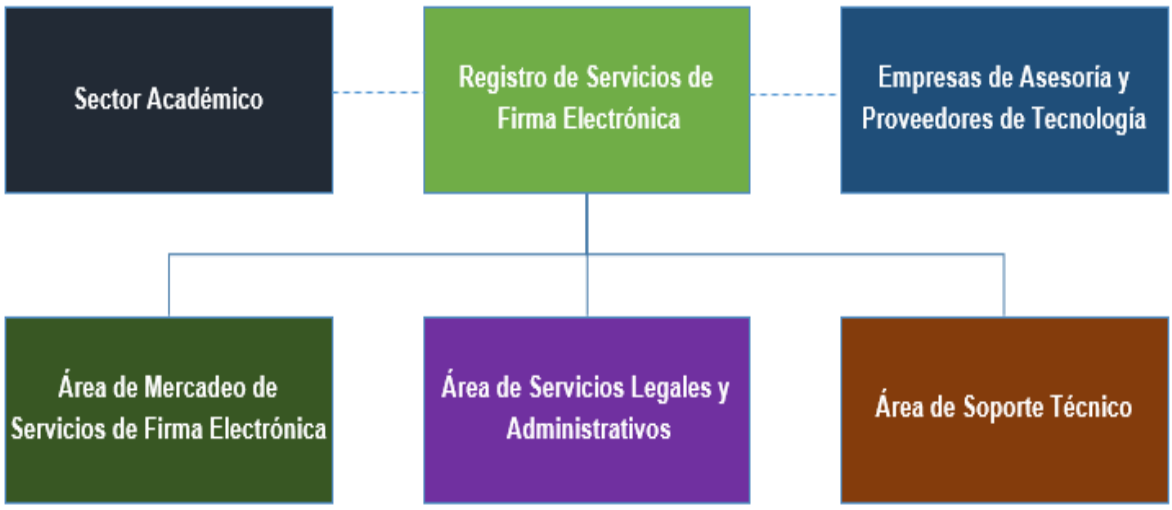
- Formación académica: Ingeniería en Tecnologías de la Información y Comunicación.
- Experiencia: Con 3 años de experiencia en aplicaciones PKI y Seguridad Informática.
- Competencia: Trabajo en equipo, Identificación y compromiso, Orientación a la calidad, Orientación al cliente, Orientación a resultados, Innovación, Seguridad informática, Planificación y administración.

e. Estructura organizativa del Registro de Servicios de Firma Electrónica del CNR

Todas las organizaciones deben poseer una estructura organizacional, según las tareas o actividades que pretendan realizar, mediante una adecuada estructura que le permita establecer sus funciones y áreas, con el propósito de generar productos o servicios, que

faciliten la consecución de sus objetivos y metas. El Registro estará conformado por áreas, cuyas funciones específicas estarán orientadas a alcanzar los objetivos y metas relacionados con el servicio de certificados de firma electrónica. A continuación, se muestra la representación gráfica de la estructura del Registro, en la que se establecen las relaciones entre las áreas que la conforman, así como los aliados con los que establecerá sinergias para lograr la misión:

Figura 2. Organigrama del Registro de Servicios de Firma Electrónica (RESEFE).



Fuente: elaboración propia.

f. **Proceso para la prestación de servicios de Certificados de Firma Electrónica**.

El servicio que brindará el Registro, se circunscribirá a las actividades que se describen a continuación:

1. Trámite de solicitud de un Certificado:

Consiste en que el cliente potencial completa un formato de solicitud que permitirá contar con información del solicitante que opta a la compra de un certificado de firma electrónica para su respectiva calificación.

Aceptación o denegación de una solicitud de certificado de firma electrónica: La aprobación o denegación de un certificado de firma electrónica, será responsabilidad de la unidad proveedora del servicio, para ello se validará el cumplimiento de las condiciones siguientes:

- Que el cliente haya efectuado el pago.
- El informe emitido por el Analista de la solicitud de firma electrónica.
- El tipo de certificado solicitado y gestionado ante el área de Mercadeo de Servicios de Firma Electrónica.
- Una vez verificados y cumplidos a satisfacción los pasos señalados, se procederá a generar el certificado electrónico.

Plazo para la tramitación de un certificado: El plazo para la tramitación y proceso de compra del certificado de firma electrónica solicitado, dependerá en gran medida de la información suministrada por el mismo cliente y de su asistencia a la entrevista de validación. Como resultado de la entrevista se determina que el cliente cumple los requisitos establecidos, procede a la firma del contrato y emisión del certificado electrónico.

El lapso establecido para la aprobación y firma de los certificados, será de ocho (8) días hábiles; luego de la entrevista de validación de identidad y datos, se generará y firmará el certificado de firma electrónica dentro del referido lapso y notificará al cliente, para que este proceda a la descarga e instalación del certificado de firma electrónica. (Alta Dirección, 2018, pp.16-17)

2. Emisión del Certificado de Firma Electrónica.

Acciones para la emisión de un certificado: Posterior a la aprobación de la solicitud, se procede a la aceptación de los términos del contrato y aprobación para la emisión del certificado de firma electrónica; es en este momento donde el cliente solicita la clave pública del certificado.

Notificación de emisión de un certificado: El proveedor comunicará a la Unidad de Firma Electrónica del Ministerio de economía (MINEC) que se ha emitido un certificado, la información del cliente, así como la clave del usuario.

Uso del par de claves y del certificado: La entrega del par de claves a los clientes se suministra con una clave genérica inicial, ya que cada cliente generará su propio par de claves (pública y privada). El titular solo puede utilizar la clave privada y el certificado para usos autorizados de acuerdo a la Política para la emisión de certificado de firma electrónica. El cliente es el único responsable de la custodia y cuido de su clave privada, acerca del compromiso de la clave privada del cliente, sin menoscabo de responder personalmente por las acciones y consecuencias derivadas del uso indebido de sus firmas o certificados electrónicos por parte de terceras personas. (Alta Dirección, 2018, pp.17-18)

3. Renovación del certificado con cambio de clave.

Causas para la renovación de un certificado: Todo certificado de firma electrónica generado por el proveedor podrá ser renovado, siempre y cuando sean cumplidas las condiciones siguientes:

- Que se haya cumplido el término de vigencia del certificado de firma electrónica del cual es propietario.
- Que el certificado de firma electrónica no haya sido revocado por el proveedor por razones de uso ilícito del mismo, según corresponda.

- Que el solicitante cumpla con los requisitos establecidos para la renovación y validación.

Procedimiento para la solicitud de renovación de un certificado: Los clientes interesados en renovar un certificado de firma electrónica emitido por el proveedor, deberán ingresar a la página web del proveedor y acceder al vínculo “compra o renovación de certificado y seguir los pasos establecidos.

Publicación del certificado renovado por la Unidad de Firma Electrónica del MINEC: Esta Unidad poseerá un repositorio de todos los certificados emitidos y renovados. El acceso al repositorio de los certificados emitidos será público y podrá ser revisado por los clientes, proveedores o partes interesadas a través de la página web del proveedor, accediendo al vínculo de “Certificados Emitidos” e ingresando los datos correspondientes al certificado de firma electrónica y el nombre o apellido del cliente propietario del dicho certificado.

Modificación de certificados: Los certificados de firma electrónica generados por el proveedor deben mantener su integridad, durante el período de vigencia que se establezca y no podrá ser objeto de modificación o cambio alguno. (Alta Dirección, 2018, pp.18-19)

4. Revocación y suspensión de un certificado

Inicia con una solicitud por parte del cliente, en la que explicará los motivos por los cuales requiere la revocación del certificado. Esta pasará a un análisis jurídico, que determinará si procede y las condiciones sobre las cuales se acepta o deniega.

Frecuencia de emisión de Lista de Certificados Revocados: El proveedor deberá generar la lista de certificados revocados que incluya una serie de indicadores, por uso indebido del certificado, por causa imputable al cliente o por cese de operación del proveedor. Lista que será publicada cada veinticuatro (24) horas en la página web del proveedor.

Requisitos de comprobación *on-line* de revocación: El cliente podrá acceder en línea a la verificación del estado de un certificado con el fin de constatar, si se encuentra

suspendido o revocado. El cliente podrá ingresar en la página *web* del proveedor y acceder al módulo “CERT-FIRMA” seguidamente buscar la opción publicación de los certificados revocados y seleccionar la opción de “Comprobación”.

Otras formas de divulgación de información de revocación disponible: El proveedor comunicará vía correo electrónico al cliente que corresponda, acerca de la suspensión o revocación de su certificado.

Finalización de la suscripción: Llegado a término el período de vigencia del certificado, el cliente podrá optar al proceso de renovación y nueva emisión. Si el cliente no opta por la renovación o nueva emisión, tendrá la información a su disponibilidad en los archivos digitales por un lapso de diez (10) años. (Alta Dirección, 2018, pp.19-20)

5. Soporte postventa

El proveedor mantiene disponibles los servicios del certificado de firma electrónica y acceso a través de su página *web*. El proveedor mantiene en operación su portal *web*, las 24 horas del día ininterrumpidamente para brindar asesorías respecto a: consultas, problemas que pudiera tener en la conectividad, alguna dificultad que se experimente al realizar una transacción, pérdida, cambio de claves, revocación y asesoría comercial y legal entre otros.

Figura 3. Diagrama del proceso del Registro de Servicios de Firma Electrónica (RESEFE) en el CNR

.

Fuente: elaboración propia.

Conclusiones

La hipótesis planteada en el presente trabajo se aprueba, porque la investigación demostró a través de datos y evidencias que el CNR dispone de condiciones para proveer el servicio de certificados de firma electrónica, dado que en lo financiero, dispone de un patrimonio de 50.3 millones de dólares; un activo de 79,3 millones de dólares e ingresos anuales promedio de 45.7 millones de dólares; en lo técnico cuenta con una planta de personal de 1,824 plazas autorizadas por el Ministerio de Hacienda y aprobadas por la Asamblea Legislativa; así como 14 oficinas en las cabeceras departamentales; en lo jurídico cuenta con su propio marco legal que le brinda autonomía administrativa y financiera para la utilización de sus recursos y prestación de servicios.

El análisis histórico de la firma electrónica que se llevó a cabo ha permitido, conocer las experiencias de la aplicación de la misma, al tomar en cuenta principalmente las particularidades de países como Colombia y Costa Rica, para enfrentar los desafíos y solución de problemas, así como los avances científicos y tecnológicos en la prestación de los servicios públicos y privados; asimismo, conocer la aplicación de las nuevas tecnologías de información y comunicación que contribuyen a la modernización del Estado y a la participación electrónica de los ciudadanos que favorecen a la gobernabilidad democrática.

La digitalización de los procesos es uno de los elementos indispensables para la funcionalidad estatal, vuelve más efectiva y eficiente la administración del Estado; la implementación de la firma electrónica es una necesidad para los Estados, ya que permite brindarle al ciudadano un servicio efectivo, ágil y de calidad.

La modernización del Estado y sus diversos instrumentos de aplicación teórica y práctica permite profundizar el sistema político y democrático; asimismo, incidir en el crecimiento

económico y en el desarrollo social del país, lo que coadyuva a lograr un bienestar ciudadano.

La implementación de la firma electrónica en El Salvador, requiere el cumplimento de ciertas condiciones indispensables en el ámbito jurídico, financiero, económico y técnico; asimismo, realizar al interior del CNR, cambios en su estructura administrativa, tecnológica y de infraestructura, que contribuirá a mejorar los procesos y dinámicas institucionales, con el propósito de brindar un servicio de firma electrónica satisfactorio a la ciudadanía y que esté al nivel de los estándares internacionales.

La implementación de la firma electrónica, no solamente requiere cumplir con las condiciones indispensables antes mencionadas, si no que resulta ineludible reformar la Ley y su respectivo Reglamento, para situarlo al nivel de los actuales estándares internacionales y de los nuevos desafíos que plantea la realidad tecnológica, económica y financiera. Las reformas a los dos instrumentos jurídicos deben realizarse acorde a las nuevas realidades del istmo centroamericano, continentales e internacionales. De no efectuarse, llevarán al fracaso la implementación de la firma electrónica y será un atentado a la seguridad jurídica de los titulares de derecho que hagan uso de los certificados de la firma electrónica.

En este mismo contexto, se hace necesario que el Ministerio de Economía emita la Norma Técnica que esté acorde con los actuales avances tecnológicos y científicos. Para que la provisión del servicio de certificación de la firma electrónica del CNR sea exitosa, entre otros, se hace indispensable que exista una articulación entre la Ley, el Reglamento y la Norma Técnica de firma electrónica.

El proceso de implementación de firma electrónica en el CNR, se percibe en dos dimensiones: Una está orientada a la comercialización de los servicios de certificados de firma electrónica enfocada al segmento de mercado de los tres poderes del Estado (Ejecutivo, Legislativo y Judicial) y a otras personas naturales y jurídicas; y la otra es para la adecuación de los procesos sustantivos y administrativos del CNR para brindar los servicios registrales que demanden los ciudadanos.

Para el primer caso, se concluye que el principal aporte de esta investigación, lo constituye la propuesta que se ha elaborado para la creación del Registro de Servicio de Firma Electrónica en el CNR, que será el responsable de proveer los servicios mediante la emisión, renovación, revocatoria y asesoría técnica o postventa de los certificados; y para la segunda, se considera que la Dirección de Tecnología de la Información en coordinación con la Gerencia de Planificación del CNR, tendrán que adecuar los procesos para ser atendidos por medio de esta plataforma tecnológica.

Bibliografía

Aliaga, T. (2015). El rol del RENIEC en el ámbito del gobierno electrónico. En *Identidad digital, la identificación desde los registros parroquiales al DNI electrónico* (p. 500). Recuperado de https://www.iidh.ed.cr/capel/media/1479/indentidad-digital-la-identificaci%C3%B3n-desde-los-registros-parroquiales-al-dni-electr%C3%B3nico.pdf

Alta Dirección. (2018). *Política de certificado de firma electrónica para representante de empresas privadas*. Recuperado de https://www.procert.net.ve/documentos/AC-D-0008.pdf

Asamblea Legislativa de la República de Costa Rica. (2005). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos*. Recuperado de https://www.mifirmadigital.go.cr/wp-content/uploads/2016/03/DCFD-Ley-de-Certificados-Firmas-Digitales-y-Documentos-Electr.pdf

-------. (2005b). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos*. Recuperado de http://unpan1.un.org/intradoc/groups/public/documents/icap/unpan034006.pdf

Asamblea Legislativa de la República de El Salvador. (1994). *Ley de Creación del Centro Nacional de Registro y su Régimen Administrativo*. Recuperado de https://www.transparencia.gob.sv/institutions/cnr/documents/2549/download

-------. (2015). *Ley de Firma Electrónica de El Salvador*. Recuperado de http://www.informatica-juridica.com/ley/decreto-no-133-ley-de-firma-electronica-de-el-salvador/

Barajas, J. (2013). Las Instituciones Sociales. Recuperado el 10 de abril de 2019, de Sociología divertida website: http://sociologiadivertida.blogspot.com/2013/11/las-instituciones-sociales.html

BID. (2003). *Modernización del Estado Documento de Estrategia*. Recuperado de https://www.aciamericas.coop/Modernizacion-del-Estado-Documento

Bravo, V., & Araujo, A. (2012). SAFET: sistema para la generación de aplicaciones de firma electrónica. *Puente Revista Científica, 6*(1), 43–51.

Casa Presidencial de El Salvador. (2016). *Reglamento de Ley de Firma Electrónica de El Salvador*. Recuperado de http://firmaelectronica.minec.gob.sv/wp-content/uploads/2016/11/reglamento_lfe_2016.pdf

Chiavenato, I. (1994). *Administración de recursos humanos* (2a ed.). Santa Fe de Bogotá: Mc Graw Hill.

Congreso de la Nación de Argentina. (1996). *Ley N° 24.624, Presupuesto General de la Administración Nacional*. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=31692

Congreso de la República de Colombia. (1999). *ley N° 527, Ley de acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales*. Recuperado de https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/L-527-99.htm

De Luca, J. (2015). *La implementación de la firma digital en el sector público: mejoras en la gestión y en los procesos para lograr óptimos resultados* (Universidad de Buenos Aire s). Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0390_DeLucaJC.pdf

Durkheim, E. (1928). *La división del trabajo social*. Buenos Aires: Ediciones LEA.

El Senado y Cámara de Diputados de la Nación Argentina. (2001). *Ley N° 25.506, Firma Digital*. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Escobar, A. (2004). Participación ciudadana y políticas Públicas. Una problematización acerca de la relación Estado y sociedad civil en América Latina en la última década. *Revista Austral de Ciencias Sociales*, *8*, 97–108.

Foucault, M. (1980). *Microfísica del poder* (2a ed.). Recuperado de http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina39453.pdf

FUSADES. (2015). *Análisis legal e institucional* (Núm. 176; p. 12). Recuperado de Fundación Salvadoreña para el Desarrollo Económico y Social website: http://fusades.org/sites/default/files/investigaciones/Ley%20de%20Firma%20Electr%C3%B3nica%20seguirdad%20jur%C3%ADdica%20en%20el%20ambito%20electr%C3%B3nico.pdf

Gerencia de Planificación del CNR. (2014). *Plan Estratégico Institucional 2014-2019*. Recuperado de https://www.transparencia.gob.sv/institutions/cnr/documents/89258/download

Gil, V., & Manero, R. (2012). Algunos referentes teóricos sobre el concepto de institución. *Área 3. Cuaderno de temas grupales e institucionales*, *16*, 13.

González, N. (2003). Marco en el que se desenvuelve la firma electrónica en la administración general del Estado. En *Firma Digital y Administraciones Públicas*

(p. 146). Recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=3908

Holloway, J. (1982). *Fundamentos teóricos para una crítica Marxista de la Administración Pública*. Recuperado de https://www.academia.edu/4823212/Fundamentos_Te%C3%B3ricos_para_una_Cr%C3%ADtica_Marxista_de_la_Administraci%C3%B3n_P%C3%BAblica

Humberstone, J. (2016). Firma Electrónica en El Salvador. *Realidad y Reflexión*, *43*, 64–72.

Irigoitia, M. (2016). *Análisis, Diseño e Implantación de Firma Digital en Documentos Electrónicos* (Instituto Universitario Aeronáutico.). Recuperado de https://rdu.iua.edu.ar/bitstream/123456789/1144/1/Proyecto%20de%20Grado_Maria%20Laura%20Irigoitia.pdf

Lomascolo, R. (2003a). Aspectos técnicos de la firma electrónica. En *Firma Digital y Administraciones Públicas*. Recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=3908

--------. (2003b). Aspectos técnicos de la firma electrónica. En *Firma digital y administraciones públicas* (p. 146). Recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=3908

López, S. (2007). *La firma electrónica, tecnología del Siglo XXI en la legislación salvadoreña* (Universidad de El Salvador). Recuperado de http://ri.ues.edu.sv/id/eprint/5017/1/LA%20FIRMA%20ELECTRONICA%2C%20TECNOLOG%C3%8DA%20DEL%20SIGLO%20XXI%20EN%20LA%20LEGISLACI%C3%93N%20SALVADORE%C3%91A.pdf

Mendoza, A. (2010). *La Realidad Latinoamericana en gestión de documentos electrónicos*. Recuperado de https://ria.asturias.es/RIA/bitstream/123456789/63/1/Archivo.pdf

Ministerio Secretaría de la Presidencia. (2004). *Modelos de firma electrónica simple para la administración Pública*. Recuperado de https://unov.tind.io/record/7979?ln=en

Moro, A. (2017). La interoperabilidad como necesidad. En *La reforma de la administración electrónica: una oportunidad para la innovación desde el derecho* (p. 553). Recuperado de https://www.inap.es/alfresco/alfresco?pathInfo...reforma-de-la-Administracion...

Nores, C. (2003). Marco en el que se desenvuelve la firma electrónica en la administración general del Estado. En *Firma Digital y Administraciones Públicas* (p. 146). Recuperado de https://dialnet.unirioja.es/servlet/libro?codigo=3908

Poder Ejecutivo. (2000). *Decreto N° 3.505, Política de Seguridad de la Información en*

los órganos y entidades de la Administración Pública Federal. Recuperado de https://www2.camara.leg.br/legin/fed/decret/2000/decreto-3505-13-junho-2000-368759-norma-pe.html

Presidencia de la República. (2001). *Decreto N° 3.996, Prestación de Servicios de Certificación Digital en el Ámbito de la Administración Pública Federal*. Recuperado de https://presrepublica.jusbrasil.com.br/legislacao/100496/decreto-3996-01

Presidencia de la República. (2012). *Código Federal de Procedimientos Civiles de los Estados Unidos Mexicanos*. Recuperado de https://www.profeco.gob.mx/juridico/word/c_f_proc_civ.doc

--------. (2014). *Código de Comercio de los Estados Unidos Mexicanos*. Recuperado de https://www.profeco.gob.mx/juridico/pdf/c_comercio.pdf

Ramírez, J. (2009). Procedimiento para la elaboración de un análisis FODA como una herramienta de planeación estratégica en las empresas. *Ciencia Administrativa*, *2*, 53–61.

Reyes, A. (2002). *La firma electrónica y las entidades de certificación* (Universidad Panamericana). Recuperado de http://www.cervantesvirtual.com/obra/la-firma-electronica-y-las-entidades-de-certificacion--0/

Román, O. (2010). El pensamiento estratégico una integración de los sentidos con la razón. *Revista Científica Guillermo de Ockham*, *8*(2), 23–63.

SELA. (2012). *Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe*. Recuperado de http://www.sela.org/media/265546/t023600005189-0-di_16-fundamentos_firma_digital_estado_del_arte_america_latina_caribe.pdf

SGE. (2017). *Sistema de gestión documental Quipux. Manual de usuario ciudadano con firma electrónica*. Recuperado de https://www.academia.edu/36702243/SISTEMA_DE_GESTI%C3%93N_DOCUMENTAL_QUIPUX_MANUAL_DE_USUARIO_CIUDADANO_CON_FIRMA_ELECTR%C3%93NICA

SNAP. (2014). *Plan Nacional de Gobierno Electrónico 2014 -2017*. Recuperado de https://ec.okfn.org/files/2014/12/PlanGobiernoElectronicoV1.pdf

Valenzuela, R., & Gil-García, R. (2019). Gobierno abierto para la modernización del Estado. *Nóesis. Revista de Ciencias Sociales y Humanidades*, *28*(56), 1–2.

Villacorta, A. (2016). *Escuela Nacional de Formación Pública (ENAFOR)*. Recuperado de http://www.secretariatecnica.gob.sv/am_event/iv-foro-de-la-funcion-publica/