**UNIVERSIDAD DE CIENCIAS COMERCIALES**

**UCC – MANAGUA**

**COORDINACIÓN DE CIENCIAS ECONÓMICAS EMPRESARIALES**

**Curso de Culminación en Proyecto de Investigación para optar al Título de grado en Licenciatura en Derecho.**

# TEMA: LA FIRMA ELECTRÓNICA EN MANAGUA, NICARAGUA EN EL AÑO 2023.


**ELABORADO POR:**

Br. Dayana Isamar Aguilar.

**TUTORA TÉCNICA:** Michelle Geraldine Bonilla Martínez.

**TUTORA METODOLÓGICA:** Michelle Geraldine Bonilla Martínez.


**Managua, Nicaragua 30 de junio del año 2024**

**UNIVERSIDAD DE CIENCIAS COMERCIALES**

**UCC – MANAGUA**

**COORDINACIÓN DE CIENCIAS ECONÓMICAS EMPRESARIALES**

**Curso de Culminación en Proyecto de Investigación para optar al Título de grado en Licenciatura en Derecho.**

## AVAL DE TUTOR

Msc. Michelle Geraldine Bonilla, tiene a bien:

**CERTIFICAR**

**Que:** La monografía con el título: **"LA FIRMA ELECTRÓNICA EN MANAGUA, NICARAGUA EN EL AÑO 2023"**, elaborado por la estudiante, **Dayana Isamar Aguilar**, ha sido dirigida por los suscritos.

Al haber cumplido con los requisitos académicos y metodológicos del trabajo monográfico damos de conformidad a la presentación de dicho trabajo de culminación de estudios para proceder a su lectura y defensa, de acuerdo con la normativa vigente del Reglamento de Régimen Académico Estudiantil y Reglamento de Investigación, Innovación y Transferencia.

Para que conste donde proceda, se firma la presente en UCC Managua/Campus a 30 días del mes de junio de 2024.

_____

**Fdo.: Michelle Geraldine Bonilla**
**Tutora Técnica y Metodológica.**

# DEDICATORIA

Este trabajo monográfico, titulado "La Firma Electrónica en Managua, Nicaragua en el Año 2023", es un testimonio de la importancia de la educación y la perseverancia en la lucha por alcanzar nuestros sueños, y está dedicado con todo mi amor y gratitud a quienes han sido pilares fundamentales en mi vida y en mi formación académica.

A mi madre, Nidia Aguilar González, por su amor incondicional, su constante apoyo y sus sabios consejos a lo largo de todo este proceso; por ser mi ejemplo a seguir; por motivarme siempre a ser mejor y a luchar hasta hacer realidad mis sueños. Su fe en mí ha sido una fuente inagotable de motivación y esperanza. Su apoyo y sacrificio han sido la fuerza impulsora detrás de mis logros.

A mi mejor amigo y guía, Carlos Fonseca Terán, por su apoyo incondicional, sus consejos y por guiarme siempre por el camino correcto; por creer en mí y por estar presente en cada paso de este camino.

## AGRADECIMIENTO

Quiero agradecer a Dios por haberme dado la fortaleza, sabiduría y perseverancia necesarias para llevar a cabo y concluir este proyecto monográfico.

Agradezco al Gobierno de Nicaragua por haberme otorgado la oportunidad de cursar mis estudios superiores, como parte de su compromiso con el acceso general de los ciudadanos nicaragüenses y en especial de los jóvenes, a la educación.

Agradezco a mis maestros, en especial:

A la Licenciada Michelle Geraldine Bonilla, por su invaluable guía y asesoría. Su conocimiento, paciencia y dedicación fueron fundamentales para el desarrollo y finalización de esta investigación. Su compromiso y profesionalismo son una inspiración constante para mí.

También quiero extender mi agradecimiento a todas las personas y entidades que me brindaron información y apoyo durante la realización de esta monografía. Su colaboración fue esencial para alcanzar los objetivos propuestos y enriquecer el contenido de esta investigación.

A todos ellos, gracias por su valioso apoyo y orientación. Su influencia ha sido esencial en mi desarrollo personal y académico. Mi reconocimiento a todos aquellos que creen en el poder transformador del conocimiento.

Con gratitud y esperanza,

Dayana Isamar Aguilar

## Índice de Contenido

## Índice de Tablas



## Índice de Figuras

## RESUMEN ABSTRACT

La firma electrónica es una herramienta esencial en la era digital, proporcionando una manera segura y eficiente de firmar documentos y realizar transacciones electrónicas. En Nicaragua, la Ley 729 de Firma Electrónica fue aprobada en 2011 con el objetivo de establecer un marco jurídico para su uso. Sin embargo, esta ley no ha sido implementada de manera efectiva, lo que ha impedido su adopción generalizada. Este trabajo monográfico investigó las razones por las cuales la Ley 729 se encuentra en desuso en Managua, Nicaragua en 2023, a pesar de su vigencia.

El análisis revela que la falta de proveedores de servicios de certificación, los altos costos de la infraestructura tecnológica y la ausencia de incentivos gubernamentales son los principales obstáculos. Además, la falta de conocimiento y cultura digital, así como problemas legales y regulatorios, agravan la situación.

Se concluye que es esencial mejorar la infraestructura tecnológica, fomentar la cultura digital y simplificar los procedimientos administrativos para impulsar el uso de la firma electrónica. Como recomendaciones clave se incluyen el desarrollo de proveedores de certificación, la implementación de programas de capacitación y sensibilización, la simplificación de trámites, la modernización de la infraestructura tecnológica y la promoción de la colaboración público-privada. Estas acciones pueden facilitar la adopción de la firma electrónica, mejorando la eficiencia y seguridad de las transacciones electrónicas en Nicaragua, y contribuyendo al desarrollo económico del país.

**Palabras claves:** firma electrónica**,** era digital, transacciones electrónicas**,** ley 729 de Firma Electrónica, Nicaragua, marco jurídico**.**

## ABSTRACT

The electronic signature is an essential tool in the digital age, providing a secure and efficient way to sign documents and conduct electronic transactions. In Nicaragua, Law 729 on Electronic Signature was approved in 2011 with the objective of establishing a legal framework for its use. However, this law has not been effectively implemented, which has prevented its widespread adoption. This monographic work investigated the reasons why Law 729 is in disuse in Managua, Nicaragua in 2023, despite its validity.

The analysis reveals that the lack of certification service providers, the high costs of technological infrastructure and the absence of government incentives are the main obstacles. In addition, the lack of knowledge and digital culture, as well as legal and regulatory problems, aggravate the situation.

It is concluded that it is essential to improve the technological infrastructure, promote digital culture and simplify administrative procedures to promote the use of the electronic signature. Key recommendations include the development of certification providers, the implementation of training and awareness programs, the simplification of procedures, the modernization of technological infrastructure and the promotion of public-private collaboration. These actions can facilitate the adoption of the electronic signature, improving the efficiency and security of electronic transactions in Nicaragua, and contributing to the economic development of the country.

**Keywords:** electronic signature, digital era, electronic transactions, law 729 on Electronic Signature, Nicaragua, legal framework.

# INTRODUCCIÓN

La firma electrónica se ha convertido en una herramienta fundamental en la era digital, permitiendo la firma de documentos y transacciones de manera segura y eficiente a través de medios electrónicos. En Nicaragua, la Ley de Firma Electrónica (Ley N° 729) fue aprobada en el año 2011 con el objetivo de establecer el marco jurídico para la utilización de la firma electrónica en el país. Sin embargo, a pesar de su aprobación hace más de una década, la ley aún no se ha implementado de manera efectiva, lo que ha impedido la adopción generalizada de la firma electrónica en Nicaragua.

Este trabajo monográfico se propone abordar y analizar las razones por las cuales la Ley 729 de Firma Electrónica en Nicaragua se encuentra en desuso a pesar de estar en vigencia desde el 2011, identificando los principales obstáculos que dificultan la implementación efectiva de la ley. Fomentando la adopción generalizada de la firma electrónica para potenciar la eficiencia en operaciones jurídicas, financieras y comerciales entre individuos, así como entre instituciones privadas y estatales para poder proponer soluciones viables y hacer que la Ley 729 sea más accesible a los particulares, empresarios locales e instituciones estatales.

Este trabajo de investigación se ha realizado utilizando leyes internacionales y nacionales, así como entrevistas a especialistas en este ramo, con todo se hizo una investigación con metodología cualitativa hermenéutica, revisión literaria para documentar la existencia de la Firma Electrónica, identificar los principales obstáculos que dificultan la implementación efectiva y proponer diferentes tipos de estrategias y soluciones para la implementación de la Ley 729.

La importancia de este trabajo radica en la posibilidad de promover una mayor comprensión y utilización de la firma electrónica en Nicaragua. La adopción de esta tecnología no solo puede mejorar la eficiencia y seguridad de las transacciones electrónicas, sino que también puede contribuir al desarrollo económico del país al facilitar operaciones comerciales más rápidas y seguras. Además, una

implementación efectiva de la Ley 729 puede fortalecer la confianza en el comercio electrónico y en las interacciones digitales tanto a nivel nacional como internacional.

Su implementación efectiva beneficia tanto al sector privado, al sector estatal, así como para los demás individuos ya que es un paso necesario para que Nicaragua se integre plenamente a la sociedad de la información y aproveche las oportunidades que ofrece la tecnología digital.

Este trabajo se encuentra estructurado en: Capítulo Uno: Planteamiento del Problema, capítulo Dos: Marco Referencial, capítulo Tres: Diseño Metodológico, Capítulo Cuatro: Resultados, Capítulo Cinco: Conclusiones y Capítulo Seis: Recomendaciones, Referencias Bibliográficas y Anexos.

Este trabajo no solo busca ofrecer una visión detallada de los desafíos y oportunidades relacionados con la Ley 729, sino también proponer soluciones concretas para su efectiva implementación, contribuyendo así al desarrollo tecnológico y económico del país.

# CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA:

### 1.1.1.1 Antecedentes históricos.

La Firma Electrónica (FE) ha experimentado un desarrollo acelerado a nivel global. Sus inicios se remontan a la década de 1970 con la criptografía de clave pública, sentando las bases para la creación de sistemas de firma electrónica confiables. En la década de 1990, diversos países comenzaron a promulgar leyes que regulaban la FE, impulsando su adopción en el ámbito comercial y gubernamental. *(Holguín García, 2018)*

**Nuevas Fundamento legal en Chile**

En Latinoamérica, la adopción de la Firma Electrónica ha sido gradual. Algunos países pioneros como Chile el cual en sus primeros pasos a la F.E, comenzó con la Comisión Presidencial de Tecnologías de Información y Comunicación, la cual, en su informe al presidente de la República presentado en el mes de enero del año1999, concluyó en la necesidad de avanzar en el marco jurídico normativo que regulara el comercio electrónico. Dicho marco, señala la propuesta, debía apuntar a reconocer que los documentos electrónicos tengan la misma validez de todos aquellos actos jurídicos que pueden y deben celebrarse por escrito.

El Gobierno asumió los primeros pasos para impulsar la firma electrónica. En junio de 1999, emitió un decreto supremo que legalizó en el ámbito del sector público el documento y la firma digital. Al mismo tiempo, en la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado se presentó una moción parlamentaria de firma digital, cuyo propósito era extender al sector privado la validación del documento y firma digital.

El consenso creciente sobre la necesidad de impulsar el comercio electrónico, se ha traducido también en numerosas propuestas e iniciativas, de expertos y también asociaciones gremiales que presentaron incluso propuestas de proyecto de ley sobre comercio y firma electrónica.

Estas iniciativas son las que inspiran la Ley N.º 19.799 "Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma", publicada el 12 de abril del 2002. Esta ley regula la firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento voluntario de acreditación de prestadores de servicio de certificación, para su uso en actos o contratos celebrados por medio de documentos electrónicos a través de medios electrónicos de comunicación. (*Ministerio de Economía, fomento y Reconstrucción; Subsecretaria de Economía, fomento y reconstrucción*, 2002)

**Fundamento legal en México**

En el caso de México, en el año 2000, el 29 de mayo, se publicó en el Diario Oficial de la Federación, el Decreto por el cual se reformó el Código Civil Federal, el Código Federal de Procedimientos Civiles y el Código de Comercio, para efecto de legislar en materia de Comercio Electrónico y utilización de medios electrónicos y tecnológicos como forma de manifestación de la voluntad de los contratantes, y su consecuente valoración como prueba en juicios del orden común.

El 29 de agosto de 2003, se publicó en el Diario Oficial de la Federación el Decreto por el cual se reforma el Código de Comercio en materia de Firma Electrónica, a través del cual se añadieron reglas claras y detalladas basadas en la Ley Modelo sobre las Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). (*Breve historia de la Firma Electrónica en México, 2021*)

Estos fundamentos se encuentran en distintas áreas jurídicas, regulados por su marco legal nacional:

- **Código Civil Federal:** la regulación se encuentra presente en los artículos 1794, 1796, 1803, 1811, 1834 y 1834 bis;
- **Código de Comercio:** se encuentra reglamentado en los artículos 89, 89 bis, 93, 97 y 1205;

Ley de Firma Electrónica avanzada, se sabe que los artículos reguladores son el 2 y 7;

- **Código Federal de Procedimientos Civiles:** en esta ley se valorará la fuerza probatoria generada o comunicada que conste en medios electrónicos, ópticos o de cualquier otra tecnología, en su artículo 210-A;

**Código Nacional de Procedimientos Penales:** acá establece que los medios electrónicos pueden utilizarse durante todo el proceso penal en su artículo 51. *(La validez jurídica de la firma electrónica en México, 2022).*

**Fundamento legal en Nicaragua**

En Nicaragua, la historia de la Firma Electrónica comienza con el Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA) en el año 2003 y complementada en el 2008. Este reglamento menciona el uso de firmas electrónicas o digitales y exige la transmisión electrónica de información para las operaciones aduaneras. Sin embargo, no fue hasta el año 2010 que se promulgó la Ley 729 de Firma Electrónica, la cual brindó un marco legal integral para el uso de la Firma Electrónica en el país.

La Ley 729 de Nicaragua se inspiró en las Leyes Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), específicamente en la Ley Modelo de Firma Electrónica aprobada en 2001, y esta última está basada en la Ley Modelo del Comercio Electrónico, aprobada en 1996 y complementada en 1998. La Ley Modelo del Comercio Electrónico marca un hito trascendental en la regulación y reconocimiento de las firmas electrónicas a escala global, respondiendo al acelerado ascenso del comercio electrónico y la necesidad apremiante de establecer normativas uniformes que garanticen seguridad y certeza jurídica en este ámbito.

El rápido crecimiento del comercio electrónico hacia finales del siglo XX generó una demanda urgente de marcos legales que respaldaran las transacciones digitales. La ausencia de modelos internacionales en el uso de firmas electrónicas planteaba

incertidumbre y obstáculos legales para su pleno desarrollo. En respuesta a este desafío, la CNUDMI elaboró la Ley Modelo sobre las Firmas Electrónicas, fundamentada en principios esenciales como la equivalencia funcional entre las firmas electrónicas y las manuscritas, la integridad de los datos y la no discriminación por su formato electrónico.

La diversidad de legislaciones nacionales sobre firmas electrónicas complicaba aún más el panorama del comercio electrónico transfronterizo. La Ley Modelo de Firma Electrónica de la CNUDMI surgió como una herramienta para armonizar estas legislaciones y facilitar el intercambio comercial entre países. Su aprobación y adopción por parte de más de 60 países desde entonces ha contribuido significativamente a este propósito, promoviendo la confianza en las transacciones electrónicas y fomentando la interoperabilidad a nivel global.

#### 1.1.1.2 Objetivos:

### 1.1.2 *General:*

- Analizar las razones por la cuales la ley 729 de Firma Electrónica se encuentra en desuso a pesar de estar en vigencia desde el 2011.

### 1.1.3 *Objetivos específicos:*

- Identificar los principales obstáculos que dificultan la implementación efectiva de la Ley 729, Ley de Firma Electrónica en Nicaragua.
- Fomentar la adopción generalizada de la firma electrónica para potenciar la eficiencia en operaciones jurídicas, financieras y comerciales entre individuos, así como entre instituciones privadas y estatales.
- Proponer soluciones viables para hacer que la Ley 729 sea más accesible a los particulares, empresarios locales e instituciones estatales.

#### 1.1.3.1 Descripción del problema y preguntas de investigación

La ley 729, Ley de firma electrónica en Nicaragua, tiene como objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica y los certificados digitales y a toda información intangible en formato electrónico.

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son: Identificar al firmante de manera inequívoca. Asegurar la integridad del documento firmado. Este conjunto de datos es significativo hacia la modernización y la facilitación de trámites administrativos y comerciales en el país.

Sin embargo, la ley de firma electrónica no se implementa en su totalidad por razones tales como: falta de proveedores nacionales e internacionales que emitan certificados digitales lo que impide la disponibilidad de este tipo de servicio en nuestra capital, adicional de un incentivo por parte del estado para promover este tipo de proveedores de servicios. Todas estas limitantes afectan el uso efectivo de la firma electrónica en Managua, generando la necesidad de realizar una investigación que dé a conocer estas limitantes y proponga la implementación o la hoja de soluciones para la puesta en marcha de ésta.

La eventual implementación de la Ley 729 de Firma Electrónica en Nicaragua se enfrenta a diversos desafíos que merecen una atención detallada. En este contexto, se plantea la necesidad de abordar preguntas fundamentales que guiarán la investigación sobre los obstáculos y facilitadores de la plena implementación de esta legislación:

¿Cuáles son los principales obstáculos que impiden la implementación total de la Ley 729 de Firma Electrónica en Nicaragua?

¿Qué medidas se han tomado para promover la adopción de la firma electrónica por parte de las entidades públicas y privadas?

¿Existe una cultura de confianza en la firma electrónica por parte de la población nicaragüense?

¿Qué medidas se han tomado para promover la capacitación y el conocimiento sobre la firma electrónica?

¿Cuáles son los beneficios económicos y sociales potenciales de la implementación de la firma electrónica en Nicaragua?

¿Cómo se puede medir el impacto de la firma electrónica en la eficiencia y transparencia de los trámites administrativos y comerciales?

¿Qué medidas se pueden tomar para asegurar que la firma electrónica sea accesible y beneficiosa para todos los sectores de la sociedad?

#### 1.1.3.2 Justificación:

El uso efectivo de la Firma Electrónica en Managua ha enfrentado diversos obstáculos que han limitado su adopción y aplicación desde que entró en vigencia en el 2011.

Uno de los principales desafíos radica en la falta de proveedores de servicios de certificación en el país. Esta carencia impide que los empresarios y ciudadanos puedan aprovechar plenamente los beneficios de la firma electrónica, ya que recurrir a empresas extranjeras conlleva costos elevados.

Además, la imposibilidad legal que tiene el Estado para constituirse él mismo como proveedor de servicio de certificación de firma electrónica, debido a que es la Dirección General de Tecnología (DGTEC) la que autoriza a los proveedores de firma electrónica, por tanto, no sería posible que el Estado se autorice así mismo; lo cual limita las opciones para garantizar la disponibilidad y accesibilidad de la firma electrónica en el ámbito gubernamental y empresarial.

Esta situación ha generado un desconocimiento generalizado de la legislación que respalda la firma electrónica en Nicaragua. La falta de información y la percepción de altos costos han desanimado su adopción y utilización, privando a la población de

aprovechar las ventajas que ofrece esta herramienta en términos de eficiencia, seguridad y agilidad en los procesos comerciales y administrativos.

Por tanto, resulta necesario abordar estos desafíos para promover una mayor conciencia y aplicación de la Firma Electrónica en Nicaragua. Esto no solo beneficiará a los empresarios y ciudadanos al facilitar sus transacciones y trámites, sino que también contribuirá al desarrollo económico y tecnológico del país en un entorno global cada vez más digitalizado.

#### 1.1.3.3 Limitaciones:

- Algunas fuentes de información sobre la firma electrónica en Nicaragua son difíciles de obtener.
- La disponibilidad de trabajos investigativos similares es limitada, lo que dificulta la visualización y comparación.
- La firma electrónica se basa en una tecnología compleja, lo que se dificulta la comprensión del tema por no poseer conocimientos técnicos.
- Existe poca jurisprudencia sobre la firma electrónica en Nicaragua, lo que genera incertidumbre jurídica.

#### 1.1.3.4 Hipótesis:

La carencia de proveedores de certificados digitales, la falta de incentivos estatales, así como la disponibilidad y confiabilidad de los servicios de firma electrónica, obstaculizan su implementación.

#### 1.1.3.5 Variables:

Independientes: Confiabilidad, seguridad jurídica.

Dependientes: Falta de interés del sector comercial en su uso. Falta de instituciones que acrediten la firma electrónica certificada.

## CAPÍTULO II: MARCO REFERENCIAL

### 2.1.1.1 REVISION DE LA LITERATURA

### 2.1.2 *MARCO TEORICO:*

Según la Ley de la CNUDMI (Nations, 2002):

> Durante la preparación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, se examinaron las funciones tradicionales de las firmas manuscritas: identificar a una persona, proporcionar certidumbre en cuanto a su participación personal en el acto de la firma; y vincular a esa persona con el contenido de un documento. Se señaló además que una firma podía cumplir diversas funciones, según cuál fuera la naturaleza del documento firmado. Por ejemplo, una firma podía constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado, de la intención de una persona de respaldar la autoría de un texto (manifestando así su conciencia de que del acto de la firma podrían derivarse consecuencias jurídicas), de la intención de una persona de asociarse al contenido de un documento escrito por otra persona, y del hecho de que una persona estuviera en un lugar determinado en un momento determinado.
>
> Sin embargo, las posibilidades de fraude son considerables debido a la facilidad con que se pueden interceptar y alterar datos en forma electrónica sin posibilidad de detección y a la velocidad con que se procesan operaciones múltiples.
>
> La finalidad de las diversas técnicas que ya están disponibles en el mercado o que se están desarrollando es ofrecer medios técnicos para que algunas o todas las funciones identificadas como características de las firmas manuscritas se puedan cumplir en un entorno electrónico. Estas técnicas se pueden denominar, en general, **“firmas electrónicas”.**

**Firmas numéricas basadas en la criptografía de clave pública**

Ante el creciente empleo de técnicas de firma numérica en diversos países, la siguiente introducción puede ser de utilidad.

### 2.1.2.1 Terminología y conceptos técnicos

#### *2.1.2.1.1 Criptografía*

Las firmas numéricas se crean y verifican utilizando la criptografía, la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original. Las firmas numéricas utilizan lo que se denomina “criptografía de clave pública”, que con frecuencia se basa en el empleo de funciones algorítmicas para generar dos “claves” diferentes, pero matemáticamente relacionadas entre sí (por ejemplo, grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos). Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible, y la otra para verificar una firma numérica o devolver el mensaje a su forma original. El equipo y los programas informáticos que utilizan dos de esas claves se suelen denominar en conjunto “criptosistemas” o, más concretamente, “criptosistemas asimétricos” cuando se basan en el empleo de algoritmos asimétricos.

Si bien el empleo de la criptografía es una de las características principales de las firmas numéricas, el mero hecho de que una firma numérica se utilice para autenticar un mensaje que contiene información en forma numérica, no debe confundirse con el uso más general de la criptografía con fines de confidencialidad. El cifrado con fines de confidencialidad es un método utilizado para codificar una comunicación electrónica de modo que sólo el originador y el destinatario del mensaje puedan leerlo. En algunos países, el empleo de la criptografía con fines de confidencialidad está limitado por ley por razones de orden público que pueden incluir consideraciones de defensa nacional. Ahora

bien, el empleo de la criptografía con fines de autenticación para crear una firma numérica, no implica necesariamente el empleo del cifrado para dar carácter confidencial a la información durante el proceso de comunicación, dado que la firma numérica codificada puede sencillamente añadirse a un mensaje no codificado.

#### *2.1.2.1.2 Claves públicas y privadas*

Las claves complementarias utilizadas para las firmas numéricas se denominan “clave privada”, que se utiliza sólo por el firmante para crear la firma numérica, y “clave pública”, que de ordinario conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado pueda verificar la firma numérica. El usuario de una clave privada debe mantenerla en secreto. Hay que señalar que el usuario individual no necesita conocer la clave privada. Esa clave privada probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o mediante un dispositivo de identificación biométrica, por ejemplo, mediante el reconocimiento de una huella digital. Si es necesario que muchas personas verifiquen firmas numéricas del firmante, la clave pública debe estar a disposición o en poder de todas ellas, por ejemplo, publicándola en una base de datos de acceso electrónico o en cualquier otro directorio público de fácil acceso. Si bien las claves del par están matemáticamente relacionadas entre sí, el diseño y la ejecución en forma segura de un criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan deducir de ella la clave privada. Los algoritmos más comunes para la codificación mediante el empleo de claves públicas y privadas se basan en una característica importante de los grandes números primos: una vez que se multiplican entre sí para obtener un nuevo número, constituye una tarea larga y difícil determinar cuáles fueron los dos números primos que crearon ese nuevo número mayor. De esa forma, aunque muchas personas puedan conocer la clave pública de un firmante determinado y utilizarla para verificar las firmas de

éste, no podrán descubrir la clave privada del firmante y utilizarla para falsificar firmas numéricas.

Cabe señalar, sin embargo, que el concepto de criptografía de clave pública no implica necesariamente el empleo de los algoritmos mencionados anteriormente basados en números primos. En la actualidad se están utilizando o desarrollando otras técnicas matemáticas, como los criptosistemas de curvas elípticas, que se suelen describir como sistemas que ofrecen un alto grado de seguridad mediante el empleo de longitudes de clave notablemente reducidas.

#### *2.1.2.1.3 La función control*

Además de la creación de pares de claves, se utiliza otro proceso fundamental, generalmente conocido con el nombre de “función control”, tanto para crear como para verificar una firma numérica. La función control es un proceso matemático, basado en un algoritmo que crea una representación numérica o forma comprimida del mensaje, a menudo conocida con el nombre de “compendio de mensaje” o “huella digital” del mensaje, en forma de un “valor control” o “resultado control” de una longitud estándar que suele ser mucho menor que la del mensaje, pero que es no obstante esencialmente única con respecto al mismo. Todo cambio en el mensaje produce invariablemente un resultado control diferente cuando se utiliza la misma función control. En el caso de una función control segura, a veces denominada “función control unidireccional”, es virtualmente imposible deducir el mensaje original aun cuando se conozca su valor control. Por tanto, las funciones control hacen posible que el programa de creación de firmas numéricas funcione con cantidades más pequeñas y predecibles de datos, proporcionando no obstante una consistente correlación testimonial con respecto al contenido original del mensaje, y dando garantías efectivas de que el mensaje no ha sido modificado desde que se firmó en forma numérica.

#### *2.1.2.1.4 La firma numérica*

41. Para firmar un documento o cualquier otro material de información, el firmante delimita primero en forma precisa el espacio de lo que se ha de firmar. Seguidamente, mediante la función control del programa informático del firmante se obtiene un resultado control único, a todos los fines prácticos, de la información que se firme. El programa del firmante transforma luego el resultado control en una firma numérica utilizando la clave privada del firmante. La firma numérica resultante es, por lo tanto, exclusiva de la información firmada y de la clave privada utilizada para crearla.

Normalmente, la firma numérica (es decir, el resultado control con firma numérica del mensaje) se adjunta al mensaje y se almacena o transmite junto con éste. Ahora bien, puede también ser enviado o almacenado como un conjunto de datos independiente, siempre que mantenga una vinculación fiable con el mensaje correspondiente. Dado que una firma numérica es exclusiva de un mensaje, resulta inservible si se la desvincula de éste permanentemente.

#### *2.1.2.1.5 Verificación de la firma numérica*

La verificación de la firma numérica es el proceso de comprobar esa firma por remisión al mensaje original y a una clave pública dada, determinando de esa forma si la firma numérica fue creada para ese mismo mensaje utilizando la clave privada que corresponde a la clave pública remitida. La verificación de una firma numérica se logra calculando un nuevo resultado control del mensaje original mediante la misma función control utilizada para crear la firma numérica. Seguidamente, utilizando la clave pública y el nuevo resultado control, el verificador comprueba si la firma numérica fue creada utilizando la clave privada correspondiente y si el nuevo resultado control calculado corresponde al resultado control original que fue transformado en la firma numérica durante el proceso de la firma.

El programa de verificación confirmará la firma numérica como “verificada”: a) si se utilizó la clave privada del firmante para firmar numéricamente el mensaje, lo que ocurre si se utilizó la clave pública del firmante para verificar la firma, dado que esta clave pública sólo verificará una firma numérica creada con la clave privada del firmante; y b) si el mensaje no fue modificado, lo que ocurre si el resultado control calculado por el verificador es idéntico al resultado control extraído de la firma numérica durante el proceso de verificación.

#### *2.1.2.1.6 Infraestructura de clave pública y prestadores de servicios de certificación*

Para verificar una firma numérica, el verificador debe tener acceso a la clave pública del firmante y tener la seguridad de que corresponde a la clave privada de éste. Ahora bien, un par de claves pública y privada no tiene ninguna vinculación intrínseca con ninguna persona; es simplemente un par de números. Se necesita un mecanismo adicional para vincular en forma fiable a una persona o entidad determinada al par de claves. Para que la codificación de la clave pública pueda cumplir su función específica, debe proporcionar un medio para facilitar claves a una gran diversidad de personas, muchas de las cuales no son conocidas del firmante y con las que no ha desarrollado ninguna relación de confianza. A tal efecto, las partes interesadas deben tener cierto grado de confianza en las claves pública y privada que se emitan.

El nivel de confianza requerido puede existir entre partes que confíen unas en otras, que se hayan tratado durante algún tiempo, que se comuniquen mediante sistemas cerrados, que operen dentro de un grupo cerrado, o que puedan regir sus operaciones en base a un contrato, por ejemplo, en un acuerdo de asociación comercial. En una transacción en la que participen sólo dos partes, cada una puede sencillamente comunicar (por un canal relativamente seguro, como un servicio de mensajería o el teléfono, que conlleva el reconocimiento de la voz) la clave pública del par de claves que cada parte utilizará. Ahora bien,

este nivel de confianza puede no existir entre partes que no realicen transacciones con frecuencia, que se comuniquen a través de sistemas abiertos (por ejemplo, Internet), que no formen parte de un grupo cerrado o que no tengan acuerdos de asociación comercial u otros acuerdos que rijan sus relaciones.

Además, dado que la criptografía de clave pública es una tecnología altamente matemática, todos los usuarios deben tener confianza en las aptitudes, los conocimientos y los dispositivos de seguridad de las partes que emitan las claves pública y privada.

Un firmante potencial podría hacer una declaración pública indicando que las firmas verificables por una clave pública determinada deben ser consideradas como procedentes de ese firmante. La forma y la eficacia jurídica de tal declaración se regirían por la ley del Estado promulgante. Por ejemplo, la presunción de que una firma electrónica corresponde a un determinado firmante podría corroborarse con la publicación de la declaración en un boletín oficial o en un documento de “autenticidad” reconocida por las autoridades públicas (véase A/CN.9/484, párr. 36). Ahora bien, puede que otras partes no estén dispuestas a aceptar la declaración, especialmente si no hay ningún contrato previo que establezca con certeza el efecto jurídico de esa declaración publicada. La parte que se base en esa declaración publicada sin ningún respaldo en un sistema abierto corre un gran riesgo de confiar inadvertidamente en un impostor, o de tener que impugnar con buen éxito la negativa falsa de una firma numérica (cuestión a menudo mencionada en el contexto del “repudio negativo” de firmas numéricas) si la operación resulta desfavorable para el supuesto firmante.

Una forma de resolver algunos de estos problemas es el empleo de uno o más terceros para vincular a un firmante identificado o el nombre del firmante a una clave pública determinada. El tercero se conoce en general, en la mayoría de

las normas y directrices técnicas, como “entidad certificadora”, “prestador de servicios de certificación” o “proveedor de servicios de certificación” (en la Ley Modelo, se ha elegido el término de “prestador de servicios de certificación”). En unos cuantos países, esas entidades certificadoras están siendo organizadas en forma jerárquica en lo que suele denominarse una infraestructura de clave pública (ICP). Otras soluciones pueden ser, por ejemplo, los certificados emitidos por terceros que confían en la firma.

#### *2.1.2.1.7 Infraestructura de clave pública*

El establecimiento de una ICP es una forma de ofrecer confianza en que: a) la clave pública del usuario no ha sido alterada y corresponde de hecho a la clave privada del mismo usuario; b) se han utilizado buenas técnicas de codificación. Para poder ofrecer el grado de confianza descrito más arriba, una ICP puede ofrecer diversos servicios, incluidos los siguientes: a) gestión de las claves criptográficas utilizadas para las firmas numéricas; b) certificación de que una clave pública corresponde a una clave privada; c) provisión de claves a usuarios finales; d) publicación de una guía segura de certificados o claves públicas; e) administración de contraseñas personales (por ejemplo, tarjetas inteligentes) que permitan identificar al usuario con información de identificación personal singular o que permitan generar y almacenar claves privadas individuales; f) comprobación de la identificación de los usuarios finales y prestación de servicios a éstos; g) prestación de servicios de marcado cronológico; y h) gestión de las claves de codificación utilizadas con fines de confidencialidad en los casos en que esté autorizado el empleo de esa técnica.

Una ICP se suele basar en diversos niveles jerárquicos de autoridad. Por ejemplo, los modelos considerados en ciertos países para el establecimiento de una posible ICP entrañan referencias a los siguientes niveles: a) una “entidad principal” única que certificaría la tecnología y las prácticas a todas las partes autorizadas a emitir certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves, y llevaría un registro de las entidades de

certificación subordinadas13; b) diversas entidades de certificación, situadas bajo la autoridad “principal” que certificarían que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir que no ha sido alterada); y c) diversas entidades locales de registro, situadas bajo las autoridades de certificación, que reciban de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, y que exijan pruebas de identidad a los posibles usuarios y las verifiquen. En ciertos países, se prevé que los notarios podrían actuar como entidades locales de registro o prestar apoyo a dichas entidades.

Las cuestiones de la ICP quizá no se presten fácilmente a la armonización a nivel internacional. La organización de una ICP puede comprender diversas cuestiones técnicas, así como cuestiones de orden público que es preferible dejar al arbitrio de cada Estado14. A este respecto, quizá sea necesario que cada Estado que contemple el establecimiento de una ICP adopte decisiones, por ejemplo, respecto de: a) la forma y el número de niveles de entidades que se incluirán en una ICP; b) si sólo las entidades certificadoras pertenecientes a la ICP podrán emitir pares de claves criptográficas o si éstos podrían ser emitidos también por los propios usuarios; c) si las entidades certificadoras de la validez de los pares de claves criptográficas deben ser entidades públicas o si también las entidades privadas podrían actuar como entidades certificadoras; d) si el proceso de autorizar a una entidad determinada para actuar como entidad certificadora debería adoptar la forma de una autorización expresa, o “licencia”, por parte del Estado, o si se deberían utilizar otros métodos para controlar la calidad de las operaciones de las entidades certificadoras permitiendo que éstas actúen sin una autorización específica; e) el grado en el que el empleo de la criptografía se debe autorizar para fines de confidencialidad; y f) si las autoridades gubernamentales deben poder tener acceso a la información codificada mediante un mecanismo de “custodia de claves” o de otro tipo. La Ley Modelo no aborda estas cuestiones.

#### *2.1.2.1.8 El prestador de servicios de certificación*

Para vincular un par de claves a un posible firmante, el prestador de servicios de certificación (o entidad certificadora) emite un certificado, un registro electrónico que indica una clave pública junto con el nombre del suscriptor del certificado como “sujeto” del certificado, y puede confirmar que el firmante potencial que figura en el certificado posee la clave privada correspondiente. La función principal del certificado es vincular una clave pública con un titular determinado. El “receptor” del certificado que desee confiar en una firma numérica creada por el tenedor que figura en el certificado puede utilizar la clave pública indicada en ese certificado para verificar si la firma numérica fue creada con la clave privada correspondiente. Si dicha verificación es positiva, se obtiene técnicamente cierta garantía de que la firma numérica fue creada por el firmante y de que la parte del mensaje utilizada en la función de control (y, por lo tanto, el correspondiente mensaje de datos) no han sido modificados desde que fue firmado en forma numérica.

Para asegurar la autenticidad del certificado con respecto tanto a su contenido como a su fuente, la entidad certificadora lo firma en forma numérica. La firma numérica de la entidad certificadora que figura en el certificado se puede verificar utilizando la clave pública de esta última que está recogida en otro certificado de otra entidad certificadora (que puede ser de un nivel jerárquico superior aunque no tiene que serlo necesariamente), y ese otro certificado puede ser a su vez autenticado utilizando la clave pública incluida en un tercer certificado, y así sucesivamente hasta que la persona que confíe en la firma numérica tenga seguridad suficiente de su autenticidad. Entre otros métodos posibles para verificar la firma numérica del prestador de servicios de certificación, esa firma se puede registrar en un certificado emitido por ese mismo prestador de servicios de certificación, que se denomina en ocasiones “certificado raíz”. En todos los casos, el prestador de servicios de certificación que emita el certificado deberá firmarlo en forma numérica durante el período de validez del otro certificado utilizado para verificar la firma numérica del

prestador de servicios de certificación. Para fomentar la confianza en la firma numérica del prestador de servicios de certificación, algunos Estados prevén la publicación en un boletín oficial de la clave pública del prestador de servicios de certificación (véase A/CN.9/484, párr. 41) o de ciertos datos sobre el certificado raíz (como la “huella digital numérica”).

La firma numérica correspondiente a un mensaje, ya sea creada por el tenedor de un par de claves para autenticar un mensaje o por una entidad certificadora para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma numérica fue creada durante el “período de validez” indicado en el certificado, que es una condición para poder verificar una firma numérica.

Para que una clave pública y su correspondencia con un firmante específico se pueda utilizar fácilmente en una verificación, el certificado debe publicarse en un repositorio o difundirse por otros medios. Normalmente, los repositorios son bases de datos electrónicas de certificados y de otro tipo de información a los que se puede acceder y que pueden utilizarse para verificar firmas numéricas.

Una vez emitido, puede que un certificado no sea fiable, por ejemplo, si el titular falsifica su identidad ante la entidad certificadora. En otros casos, un certificado puede ser suficientemente fiable cuando se emite, pero dejar de serlo posteriormente. Si la clave privada ha quedado “en entredicho”, por ejemplo, si el tenedor de la clave ha perdido el control de ésta, el certificado puede dejar de ser fiable y la entidad certificadora (a petición del titular o aun sin el consentimiento de éste, según las circunstancias), puede suspender (interrumpir temporalmente el período de validez) o revocar (invalidar de forma permanente) el certificado. Inmediatamente después de suspender o revocar un certificado, el prestador de servicios de certificación puede hacer pública la revocación o suspensión o notificar este hecho a las personas que soliciten

información o de que se tenga conocimiento de que han recibido una firma numérica verificable por remisión al certificado que carezca de fiabilidad.

Las entidades certificadoras podrán ser entidades públicas o privadas. En algunos países, por razones de orden público, se prevé que sólo las entidades públicas estén autorizadas para actuar como entidades certificadoras. En otros países, se considera que los servicios de certificación deben quedar abiertos a la competencia del sector privado. Independientemente de que las entidades certificadoras sean públicas o privadas y de que deban obtener una autorización, normalmente existe más de una entidad certificadora en la ICP. Plantea especial inquietud la relación entre las diversas entidades certificadoras. Las entidades certificadoras de una ICP pueden establecerse en una estructura jerárquica, en la que algunas de ellas sólo certifican a otras entidades certificadoras, que son las que prestan los servicios directamente a los usuarios. En dicha estructura, las entidades certificadoras están subordinadas a otras entidades certificadoras. En otras posibles estructuras, algunas entidades certificadoras pueden actuar en plano de igualdad con otras entidades certificadoras. En una ICP de gran envergadura, probablemente habría tanto entidades certificadoras subordinadas como superiores. En cualquier caso, si no existe una ICP internacional, pueden surgir una serie de problemas con respecto al reconocimiento de certificados por parte de entidades certificadoras de países extranjeros. El reconocimiento de certificados extranjeros se realiza generalmente mediante un método denominado “certificación cruzada”. En tales casos es necesario que entidades certificadoras sustancialmente equivalentes (o entidades certificadoras dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera más eficaz y con mayor confianza en la fiabilidad de los certificados que se emitan.

Con respecto a la certificación cruzada o a las cadenas de certificados, cuando entran en juego diversas políticas de seguridad se pueden plantear problemas jurídicos, por ejemplo, respecto de la identificación del autor del error que causó una pérdida y de la fuente en que se basó el usuario. Cabe señalar que las normas jurídicas cuya aprobación se está considerando en ciertos países disponen que, cuando los niveles de seguridad y las políticas se pongan en conocimiento de los usuarios y no haya negligencia por parte de las entidades certificadoras, no habrá responsabilidad.

Puede que corresponda al prestador de servicios de certificación o a la entidad principal asegurar que los requisitos de sus políticas se cumplen de forma permanente. Si bien la selección de las entidades certificadoras puede basarse en diversos factores, incluida la solidez de la clave pública utilizada y la identidad del usuario, el grado de fiabilidad del prestador de servicios de certificación puede depender también de la forma en que aplique las normas para emitir certificados y de la fiabilidad de la evaluación que realice de los datos que reciba de los usuarios que solicitan certificados. Es de especial importancia el régimen de responsabilidad que se aplique al prestador de servicios de certificación con respecto al cumplimiento, en todo momento, de la política y los requisitos de seguridad de la entidad principal o de la entidad certificadora superior, o de cualquier otro requisito aplicable. Igual importancia reviste la obligación del prestador de servicios de certificación de actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas, tal como dispone el artículo 9, 1 a) de la nueva Ley Modelo (véase A/CN.9/484, párr. 43).

Al preparar la Ley Modelo, se examinaron los siguientes elementos como posibles factores a tener en cuenta para determinar el grado de fiabilidad de un prestador de servicios de certificación: a) independencia (es decir, ausencia de un interés financiero o de otro tipo en las transacciones subyacentes); b) recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida; c) experiencia en tecnologías de clave pública y familiaridad con

procedimientos de seguridad apropiados; d) longevidad (las entidades certificadoras pueden tener que presentar pruebas de certificaciones o claves de codificación muchos años después de que se hayan concluido las operaciones subyacentes, por ejemplo con motivo de un juicio o de una reivindicación); e) aprobación del equipo y los programas informáticos; f) mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente; g) existencia de un plan para casos de emergencia (por ejemplo, “programas de recuperación en casos de desastre” o depósitos de claves); h) selección y gestión del personal; i) disposiciones para proteger su propia clave privada; j) seguridad interna; k) disposiciones para suspender las operaciones, incluida la notificación a los usuarios; l) garantías y representaciones (otorgadas o excluidas); m) limitación de la responsabilidad; n) seguros; o) capacidad para intercambiar datos con otras entidades certificadoras; y p) procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado en entredicho).

#### *2.1.2.1.9 Sinopsis del proceso de la firma numérica:*

El empleo de las firmas numéricas abarca por lo general los siguientes procesos, realizados por el firmante o por el receptor del mensaje firmado en forma numérica:

a) El usuario genera o recibe un par de claves criptográficas único;

b) El firmante prepara el mensaje (por ejemplo, en forma de mensaje de correo electrónico) en una computadora;

c) El firmante prepara un “compendio del mensaje”, utilizando un algoritmo de control seguro. En la creación de la firma numérica se utiliza un resultado de control derivado del mensaje firmado y de una clave privada determinada, que es exclusivo de éstos;

d) El firmante codifica el compendio del mensaje utilizando la clave privada. La clave privada se aplica al texto del compendio del mensaje utilizando un algoritmo matemático. La firma numérica es el compendio del mensaje codificado;

e) El firmante normalmente adjunta o acompaña su firma numérica al mensaje;
f) El firmante envía en forma electrónica la firma numérica y el mensaje (codificado o no) a la parte que confía en la firma;
g) La parte que confía en la firma utiliza la clave pública del firmante para verificar la firma numérica de éste. Esta verificación con la clave pública del firmante da cierta seguridad técnica de que el mensaje proviene exclusivamente del remitente;
h) La parte que confía en la firma también crea un "compendio del mensaje" utilizando el mismo algoritmo de control seguro;
i) La parte que confía en la firma compara los dos compendios de mensajes. Si son iguales, esa parte sabe que el mensaje no ha sido modificado después de la firma. Aun cuando sólo se haya modificado una parte ínfima del mensaje después de que haya sido firmado en forma numérica, el compendio del mensaje creado por dicha parte será diferente al compendio del mensaje creado por el firmante;
j) La parte que confía en la firma obtiene un certificado del portador de servicios de certificación (o por conducto del firmante o de otro modo), que confirma la firma numérica del firmante del mensaje (véase A/CN.9/484, párr. 44). El certificado contiene la clave pública y el nombre del firmante (y posiblemente otra información), y lleva la firma numérica del prestador de servicios de certificación.

#### *2.1.2.1.10 Para los fines de la Ley Modelo del Comercio Internacional se entenderá:*

a) Por **"mensaje de datos"** la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

b) Por **"intercambio electrónico de datos (EDI)"** se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por **"iniciador"** de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;

d) Por **"destinatario"** de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él;

e) Por **"intermediario",** en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por **"sistema de información"** se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

#### 2.1.2.2 MARCO LEGAL.

### 2.1.3 *CONTEXTO INTERNACIONAL*

#### 2.1.3.1 Canadá

En el año 2004, se promulgó la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), que establece que una firma electrónica puede satisfacer cualquier necesidad de firma exigida por las leyes federales.

PIPEDA define una firma electrónica como una "firma que consta de una o más letras, caracteres, números u otros símbolos en formato digital incorporados, adjuntos o asociados con un documento electrónico".

PIPEDA también diferencia “firmas electrónicas” y “firmas electrónicas seguras”. Una firma electrónica segura es un tipo de firma digital que aplica tecnologías o procesos específicos por regulación, incluido un conjunto de operaciones consecutivas que deben completarse para que la firma califique como segura.

De acuerdo con la Ley de Alberta y Ontario, una firma electrónica es “información electrónica que una persona crea o adopta para firmar un registro y que se encuentra en, adjunta o asociada con el registro”. De manera similar, la Ley de Columbia Británica lo define como “información en formato electrónico que una persona ha creado o adoptado para firmar un registro y que se encuentra en, adjunto o asociado con el registro”.

Además de cumplir con los requisitos legales canadienses, las firmas electrónicas deben cumplir con las siguientes pautas para ser plenamente aplicables:

- Confirme que la persona que está firmando el documento está completamente autenticada
- Mostrar la intención del firmante
- Asegúrese de que el documento esté protegido contra cambios posteriores. *(Guías de Legalidad Canadá, Visión general, s.f.)*

#### 2.1.3.2 Estados Unidos

En 1999, fue desarrollado el proyecto UETA de acuerdo con el que a cada estado de los Estados Unidos se puede conceder la estructura jurídica para usar las firmas electrónicas. UETA fue aceptada por 48 estados, el distrito de Columbia y las Islas Vírgenes de los Estados Unidos.

El 1 de octubre de 2000 en los Estados Unidos entró en vigor la ley federal ESIGN (Ley de firmas electrónicas en las relaciones comerciales internacionales y domésticas). La ESIGN determina la firma electrónica como el “sonido, el símbolo o el proceso electrónico adjunto o relacionado lógicamente con el contrato u otra grabación creada, enviada, transmitida, recibida o almacenada con los medios electrónicos”. Con

esto según ESIGN: “no se puede rechazar en la validez judicial, la efectividad o la fuerza ejecutiva sólo por estar estos en forma electrónica”.

Según ESIGN la parte firmante debe demostrar una intención clara de firmar el convenio en forma electrónica. Una firma puesta por el ratón o estilete, así como pulsando el botón “Yo acepto” tiene el mismo efecto como la firma manuscrita. La ESIGN es el acta jurídica de coordinación, ya que hacia el momento de su aceptación ya en la mayoría de ciertos estados se formó la legislación reguladora correspondiente.

#### 2.1.3.3 México

Existe la Ley de Firma Electrónica Avanzada (LFEA) publicada en el diario oficial de la federación el 11 de enero de 2012. La Secretaría de Economía es la encargada de acreditar a los diferentes de servicios de Firma Electrónica Avanzada.

La LFEA de México establece que la Firma Electrónica Avanzada es el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa, garantiza el contenido del documento firmado y no es repudiable.

#### 2.1.3.4 Guatemala

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Decreto 47-2008), fue publicada en el diario oficial el 23 de septiembre de 2008. El Ministerio de Economía de ese país tiene bajo su responsabilidad el regular este tema, y abrió en el mes de junio de 2009 el Registro de Prestadores de Servicios de Certificación, publicando su sitio web con copia de la ley e información importante sobre el tema. Existen dos Prestadores de Servicios de Certificación Digital debidamente autorizado por el Ministerio de Economía de Guatemala, el primero autorizado en 2012 fue la

Cámara de Comercio de Guatemala a través de su instancia Firma-e, en el año 2015 la entidad Prisma Registro Digital.13 y en 2018 5B. Lista oficial

#### 2.1.3.5 Honduras

La ley para certificar cualquier institución como Prestadora de Servicios de Certificación de Firma Electrónica, Ley aprobada mediante Decreto 149-2013 aprobado por el Congreso Nacional en julio de 2013, siendo el Banco Central de

Honduras (BCH) la primera institución del país en ser autorizado como Prestadora de Servicios de Certificación de Firma Electrónica, su Certificado lo recibió de Instituto de la Propiedad (IP).

#### 2.1.3.6 Nicaragua

El 30 de agosto de 2010 en La Gaceta Diario Oficial No. 165, se publicó la Ley No. 729, Ley de Firma Electrónica, siendo la Dirección General de Tecnología (DGTEC), dependencia del Ministerio de Hacienda y Crédito Público (MHCP), la Entidad Rectora del proceso de acreditación de firma electrónica.

El 8 de noviembre de 2011, se publicó en La Gaceta Diario Oficial, el Decreto No. 57-2011, Reglamento de Ley N°729, Ley de Firma Electrónica15.
La legislación nicaragüense, para su país, define dos tipos de firma electrónica:

- Firma Electrónica.
- Firma Electrónica Certificada.

La diferencia se establece en que la Firma Electrónica Certificada está basado en un certificado emitido por un Proveedor de Servicios de Certificación, el cual en cumplimiento de la ley y normativa aplicable fue autorizado por la DGTEC para operar en el país.

#### 2.1.3.7 Costa Rica

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. *(Firma Electrónica, Regulaciones en diferentes países, 2024).*

### 2.1.4 *Marco legal nacional:*

#### 2.1.4.1 Objeto de la Ley.

Artículo 1: La presente Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica y a los certificados digitales y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación.

Art. 2 Ámbito de Aplicación.
Las disposiciones de la presente Ley serán aplicadas dentro del territorio nacional a todos los actos o contratos en que se utilice firma electrónica en el contexto de las actividades no comerciales y comerciales, que garanticen su autenticidad e integridad de los documentos electrónicos.

Art. 12 Así mismo se autoriza el uso de la firma electrónica certificada a las instituciones del Estado, entes desconcentrados, descentralizados y autónomos; para que emitan documentos electrónicos, celebren toda clase de contratos electrónicos en sus relaciones entre sí o con personas naturales o jurídicas.
Se exceptúan aquellos casos mediante el cual la Ley exija la solemnidad que no pueda ser satisfecha por la presente Ley.

Art. 13 De igual manera los actos, contratos y documentos electrónicos de las instituciones y entes referidos en el artículo anterior, suscritos mediante firma electrónica certificada, serán válidos y producirán los mismos efectos que los expedidos por firma manuscrita.

Art. 14 También se autoriza a las Instituciones del Estado a realizar la notificación electrónica a las personas naturales o jurídicas, que sean parte de un proceso judicial o administrativo, en el domicilio del correo electrónico que designen para tal efecto los interesados y bajo su consentimiento.

En el caso de las personas jurídicas, la notificación se hará a su representante legal, abogado, fiscal o procurador designado en las oficinas que estos tuvieren o domicilio del correo electrónico que señalaren. El reglamento a la presente ley establecerá el procedimiento.

#### 2.1.4.2 De La Entidad Rector

Art. 15 Entidad Rectora de Acreditación de Firma Electrónica. Se designa a la Dirección General de Tecnología, conocida en adelante como DGTEC, dependencia del Ministerio de Hacienda y Crédito Público, como el ente rector del proceso de acreditación de firma electrónica.

La DGTEC, además de las potestades establecidas en las leyes de la materia, tendrá las siguientes:

1. Autorizar, inspeccionar y evaluar a los proveedores de servicios de certificación;
2. Cancelar o suspender la autorización otorgada a los proveedores de servicios de certificación;
3. Administrar el registro de proveedores de servicios de certificación, que para tal efecto se conformará dentro de la DGTEC;
4. Gestionar, por medio de la Dirección General de Ingresos, los ingresos provenientes de las tasas y multas establecidas en la presente Ley;

5. Administrar y ejecutar su presupuesto de conformidad con la Ley de la materia;
6. Supervisar la prestación de los servicios que brinden los proveedores de servicios de certificación;
7. Aplicar las sanciones administrativas que correspondan;
8. Seleccionar y contratar al personal técnico administrativo para el desempeño de sus f unciones de conformidad con la ley de la materia;
9. Solicitar la información a los proveedores de servicios de certificación;
10. Realizar auditorías técnicas a los proveedores de servicios de certificación; y
11. Velar por el cumplimiento de la presente Ley y su reglamento.

Procedimiento de Inscripción para ser proveedor de servicios de Certificación (PSC):

En la República de Nicaragua se inicia con una solicitud de parte del proveedor ante la oficina de la DGTEC, la que contendrá su nombre o denominación social, su RUC, (Registro Único de Contribuyente) el nombre y RUC del Representante Legal, su domicilio social, número telefónico, dirección de correo electrónico y llevar los requisitos antes descritos y acompañar el comprobante de pago de los costos de la acreditación, la autoridad competente dispondrá de sesenta (60) días hábiles a partir de la recepción para resolver si no estará en silencio administrativo, lo cual conllevara a ser entendida por aceptada por parte del proveedor ante esta Dirección. Una vez acreditado este proveedor será inscrito en el registro que lleve a cabo esta Dirección. Cabe mencionar que en dichos requisitos no está establecido el valor a pagar por dicha inscripción, la cual se encuentra en el artículo 18 de dicha Ley que establece:

Se establecen las siguientes tasas por los servicios de la DGTEC:

1. Por la acreditación de la prestación de servicios de certificación por un término de cinco (5) años, se cobrará una tasa de unos mil dólares de los Estados Unidos de América (US$ 1,000.00) o su equivalente en córdobas;

2. Por la renovación de la prestación de servicios de certificación, se cobrará una tasa de Quinientos dólares de los Estados Unidos de América (US$ 500.00) o su equivalente en córdobas.

Ahora en cuanto a la Garantía, en el Reglamento no está definido el monto o si es con respecto al riesgo (variable). El reglamento Art. 19, Decreto No. 57-2011 hace referencia al seguro en artículo diecinueve. El PSC (proveedor de servicio de certificación) debe contar con seguros vigentes que cumplan con los siguientes requisitos:
a) Ser expedidos por una entidad aseguradora autorizada para operar en Nicaragua. En caso de no ser posible lo anterior, por una entidad aseguradora del exterior que cuente con la autorización de la Superintendencia de Bancos y Otras Instituciones Financieras, SIBOIF.)

b) Cubrir todos los perjuicios contractuales y extracontractuales de los titulares y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados del PSC en el desarrollo de las actividades para las cuales solicita autorización o cuenta con autorización. Para tal fin se cubrirán los anteriores riesgos por una cuantía 5,000 salarios mínimos mensuales legales del sector financiero asegurada por evento.
El límite de responsabilidad definido en la Declaración de Prácticas de Certificación,

c) cláusula de restitución automática del valor asegurado.

d) Incluir una cláusula que obligue a la entidad aseguradora a informar previamente a la Entidad Rectora, la terminación del contrato o las modificaciones que reduzcan el alcance o monto la cobertura.

El PSC que pretenda otorgar el reconocimiento cruzado de certificados de firma electrónica, deberá acreditar la cobertura de las garantías requeridas en este reglamento para los perjuicios que puedan causar los certificados reconocidos.

Art. 26 Al recibir la solicitud la DGTEC, dispondrá de un plazo de diez (10) días hábiles para la verificación de los requisitos, se podrá subsanar los requisitos en un plazo de cinco (5) días hábiles, de no cumplirse en tiempo y forma se rechazará y se procederá a dictar una resolución en la que rechaza la solicitud de acreditación.

La Entidad Rectora podrá acreditar temporalmente por un plazo máximo de sesenta (60) días calendario al interesado, cuando se subsanen los requisitos que no afecten el funcionamiento del sistema previa autorización de un plan de medidas correctivas, los costos no serán restituidos cuando la acreditación no se conceda por incumplimiento de los requisitos y obligaciones legales y reglamentarias.

Una vez completados los requisitos exigidos se procederá a acreditar definitivamente y cualquier cambio que realice el proveedor deberá notificarlo tres (3) días hábiles a la DGTEC (Dirección General de Tecnología). En cuanto a las modificaciones de las condiciones que permitieron su acreditación.

#### 2.1.4.3 Procedimiento de acreditación de la firma electrónica en Nicaragua.

En Nicaragua los Procedimientos se encuentran dentro de los Requisitos a cumplir establecidos en el artículo 5 y 8 de la Ley No. 729. (REGLAMENTO DE LA LEY n 729, 2011)

Requisitos para la acreditación de la Firma Electrónica Certificada:

El artículo cinco de la Ley de Firma Electrónica expresa: que una firma electrónica certificada es válida si cumple los siguientes requisitos:

1. Que los datos de creación de firma correspondan exclusivamente al titular;
2. Que el certificado reconocido en que se base, haya sido expedido por un proveedor de servicios de certificación acreditado; y

3. Cuando el dispositivo seguro de creación de firma provenga de un proveedor de servicios de certificación acreditado.

Requisitos de Validez de los Certificados de Firma Electrónica:

Así mismo en el artículo ocho de la misma ley expresa que Los certificados de firma electrónica deberán cumplir con los siguientes requisitos de validez mínimos:

1. Indicar que el certificado se expide como certificado electrónico;
2. Identificar al proveedor de servicios de certificación y el país en que se encuentra establecido;
3. Contener el nombre y los apellidos del titular o un seudónimo que conste como tal;
4. Designar un atributo específico del titular, en caso de que fuera significativo en función de la finalidad del certificado;
5. Contener los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del titular;
6. Estipular una indicación relativa al período de validez del certificado;
7. Contener el código identificativo del certificado;
8. Identificar la firma electrónica certificada del proveedor de servicios de certificación que expide el certificado;
9. Determinar los límites de uso del certificado; y
10. Establecer los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

La consignación en el certificado de cualquier otra información relativa al titular requerirá su consentimiento expreso, siempre y cuando no contravenga la presente Ley.

#### 2.1.4.4 Proveedor de servicios de certificación (psc).

Para ser proveedor de servicios de certificación se requiere los siguientes requisitos:

1. Un establecimiento permanente situado en territorio nicaragüense donde resida de forma continua o habitual, así como de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad;

2. Emplear personal que tenga los conocimientos especializados, la experiencia y las calificaciones necesarias correspondientes a los servicios prestados. En particular, el personal deberá poseer competencia en materia de gestión informática. Conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados. Tal personal deberá poner en práctica los procedimientos administrativos y de gestión adecuada y conforme a normas reconocidas internacionalmente;

3. Contar con sistemas y productos fiables que estén protegidos contra toda alteración a fin de garantizar la seguridad jurídica, técnica y criptográfica de los procedimientos con que trabajan; y la confidencialidad de la información;

4. Ser persona jurídica debidamente constituida e inscrita en el registro público mercantil;

5. Disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Ley; en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, según valoración de la entidad rectora; y

6. Contratar a uno o varios notaros públicos con cinco años de experiencia profesional, a fin de que pueda dar fe pública sobre el cumplimiento de las obligaciones del proveedor de servicios en el momento del libramiento del certificado al titular.

Acreditación de los Proveedores de Servicios de Certificación.

La acreditación es el acto mediante el cual el proveedor de servicios de certificación es autorizado a funcionar como tal por la DGTEC (Dirección General de Tecnología), habiendo demostrado su capacidad técnica, infraestructura, recursos humanos y económicos, así como programas informáticos necesarios para otorgar los certificados

en el plazo establecido en la presente Ley y en su reglamento, permitiendo su inscripción en el registro que para tal efecto se constituya.

Procedimiento de Acreditación de los Proveedores de Servicios de Certificación:

El procedimiento de acreditación se llevará a cabo por medio de solicitud ante la DGTEC (Dirección General de Tecnología), la que adjuntará los requisitos establecidos en la presente Ley.
Esta, resolverá sobre dicha solicitud en un plazo de sesenta días hábiles a partir de la recepción de la solicitud del interesado. Si pasado el término establecido la DGTEC (Dirección General de Tecnología no se pronunciare, la solicitud se entenderá aceptada.
En tal caso, el proceso de registro operará de mero derecho conforme a la solicitud con acuse de recibo en manos del interesado.
A si mismo otorgada la acreditación, el proveedor de servicios de certificación será inscrito en el Registro que se lleve para tal efecto por la DGTEC. El proveedor de servicios de certificación está obligado a informar a la DGTEC, en un plazo no mayor de tres días hábiles, de cualquier modificación de las condiciones que permitieron su acreditación.

Con respecto al Reglamento, Decreto No. 57-2011, para ser PSC (proveedor de servicios de certificación) establece lo siguiente:
Quienes pretendan realizar las actividades propias de los Proveedores de Servicios de Certificación deberán particularizarlas y acreditar ante la Entidad Rectora:
1. Personería jurídica.
Cuando se trate de una entidad extranjera, se deberá acreditar el cumplimiento de los requisitos contemplados en el Código de Comercio para las sociedades extranjeras que pretendan ejecutar negocios permanentes en territorio nicaragüense.

2. Que los administradores y representantes legales no tengan prohibido el ejercicio del comercio.

3. Declaración de Practicas de Certificación satisfactoria, de acuerdo con los requisitos establecidos por la Entidad Rectora.

4. Patrimonio mínimo de 800 salarios mínimos mensuales del sector financiero legales vigentes al momento de la solicitud de autorización, esto en caso de que las actividades a desarrollar por el PSC sean las de una Autoridad de Registro (AR). En el caso en que las actividades que desarrolle el PSC incluyan también las de una Autoridad de Certificación (AC), el patrimonio mínimo que deberá evidenciar será de al menos el mismo monto mínimo que el PSC debe asegurar de acuerdo a los señalado en el artículo 19 inciso (b).

5. Constitución de las garantías previstas en este Reglamento.

6. Infraestructura y recursos por lo menos en la forma exigida en el artículo 20 de este Reglamento.

7. Informe inicial de Inspección satisfactoria juicio de la misma Entidad Rectora.

8. Un mecanismo de ejecución inmediata revocar los certificados de firma electrónica expedidos a los titulares, a petición de estos o cuando se tenga indicios de que ha ocurrido algunos de los eventos de revocación previstos en la ley, en este Reglamento o en la Declaración de Practicas de Certificación.

9. En caso de tratarse de proveedores de servicios de certificación que requieran o utilicen infraestructura o servicios tecnológicos prestados desde el extranjero, la inspección o auditoría podrá ser realizada por una persona o entidad facultada para realizar este tipo de inspecciones o auditorías en el lugar donde se encuentra la infraestructura, siempre y cuando permita constatar el cumplimiento de lo señalado en el presente Reglamento.

Como se establece en el Decreto No. 57-2011 de Nicaragua (2011):
La Entidad Rectora tendrá la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente. Si se solicita autorización para certificaciones cruzadas, se deberán acreditar adicionalmente la entidad o prestador de servicios de certificación reconocida, los certificados reconocidos y el tipo de certificados al cual se remite, la vigencia y los términos del reconocimiento. (Art. 12, Decreto No. 57-2011, Nicaragua, 2011)

Según lo estipulado en el Decreto No. 57-2011 de Nicaragua (2011):
El procedimiento de acreditación de los proveedores de servicios de certificación se iniciará por medio de una solicitud presentada a la Entidad Rectora, acompañada del comprobante de pago de los costos de la acreditación y de los antecedentes que permitan verificar el cumplimiento de los requisitos de acreditación.
En la solicitud que presente el interesado deberá individualizarse debidamente y para ello señalará su nombre o denominación social, su Registro Único de Contribuyente, el nombre y Registro Único de Contribuyente del Representante Legal, su domicilio social, número telefónico y dirección de correo electrónico, aceptando expresamente dicho medio electrónico como forma de comunicación. (Art. 25, Decreto No. 57-2011, Nicaragua, 2011)

El Decreto No. 57-2011 de Nicaragua (2011) indica que:
Recibida la solicitud, la Entidad Rectora procederá a conocer la admisibilidad de la misma, mediante la verificación de los antecedentes requeridos, dentro del plazo de diez días hábiles.

De ser inadmisible la solicitud, se procederá a comunicar al interesado tal situación, el que podrá completar los antecedentes dentro del plazo de cinco días hábiles, bajo apercibimiento de ser rechazada la solicitud de no cumplirse en tiempo y forma con los requisitos y obligaciones establecidos. Admitida a trámite la solicitud, la Entidad Rectora procederá a un examen sobre el cumplimiento de los requisitos y obligaciones

exigidas por la Ley, este Reglamento y las normas técnicas para obtener la acreditación. (Art. 26, Decreto No. 57-2011).

Conforme a lo dispuesto en el Decreto No. 57-2011 de Nicaragua (2011):

En caso que la Entidad Rectora determine que el proveedor de servicios de certificación no cumple con las normas técnicas fijadas para el desarrollo de la actividad señalará si los incumplimientos son subsanables, y si no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica certificada o para los servicios adicionales de certificación electrónica definidas en este reglamento.

En caso que los incumplimientos no sean subsanables, la Entidad Rectora procederá a dictar una resolución en la que rechaza la solicitud de acreditación.

Si los incumplimientos son subsanables y no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley y su Reglamento para la firma electrónica certificada, la Entidad Rectora podrá acreditar temporalmente por un plazo máximo de sesenta días calendario al interesado, previa autorización de un plan de medidas correctivas.

Una vez completados los requisitos exigidos la Entidad Rectora procederá a acreditar definitivamente al interesado. (Art. 27, Decreto No. 57-2011)

Durante todo el proceso de acreditación, la Entidad Rectora podrá solicitar documentación adicional o realizar visitas a las instalaciones del interesado, por intermedio de sus funcionarios o por expertos especialmente Contratados para dichos fines. (Art. 28, Decreto No. 57-2011)

En el marco del Decreto No. 57-2011 de Nicaragua (2011), se señala:

Los costos de acreditación serán pagados por el proveedor de servicios de certificación que solicite acreditarse, los que no serán restituidos en el evento de que la acreditación no se conceda por incumplimiento de los requisitos y obligaciones legales y reglamentarias exigidas para el desarrollo de la actividad de certificación como acreditado. (Art. 29, Decreto No. 57-2011).

### 2.1.5 *Marco conceptual:*

Para abordar la Firma Electrónica o digital es necesario definir algunos términos que servirán para la realización y comprensión de este trabajo. Los que se encuentran en el artículo 3 de la LEY NO. 729, LEY DE FIRMA ELECTRÓNICA, DE NICARAGUA, APROBADA EL 01 DE JULIO DEL 2010. Para los fines de la presente Ley se entiende:

#### 2.1.5.1 Firma electrónica

Son datos electrónicos integrados en un mensaje de datos o lógicamente asociados a otros datos electrónicos, que puedan ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de datos.

#### 2.1.5.2 Firma electrónica certificada

Es la que permite identificar al titular y ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que vinculada al mismo y a los datos a los que se refiere, permite que sea detectable cualquier modificación ulterior a estos.

Ejemplos:

**Imagen 1: Seleccionar el archivo PDF para firmar**

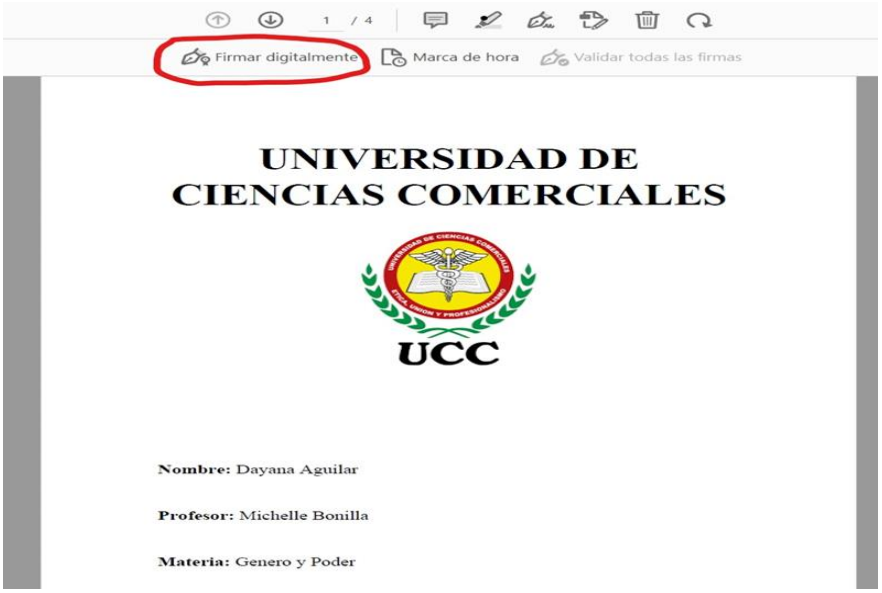


**Imagen 2: Firmar con un Id electrónico Certificado**

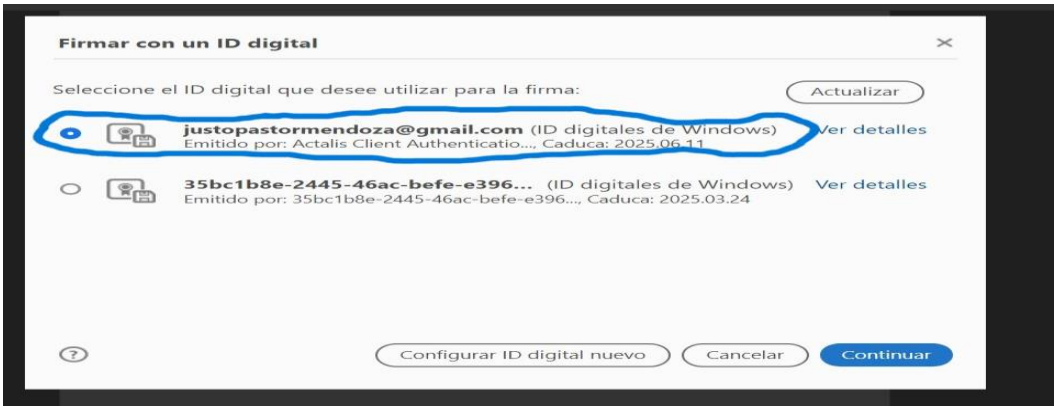



**Imagen 3: Delimitación del espacio del archivo a firmar**

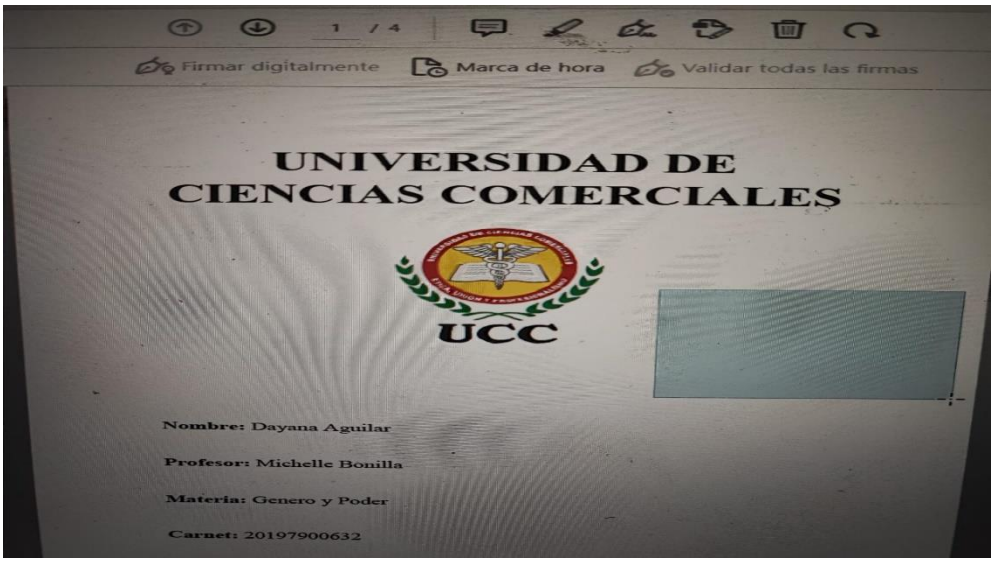



**Imagen 4: Visión de cómo quedará aplicada la firma en el documento**

**Imagen 5: Resumen del certificado de firma electrónica antes de firmar**

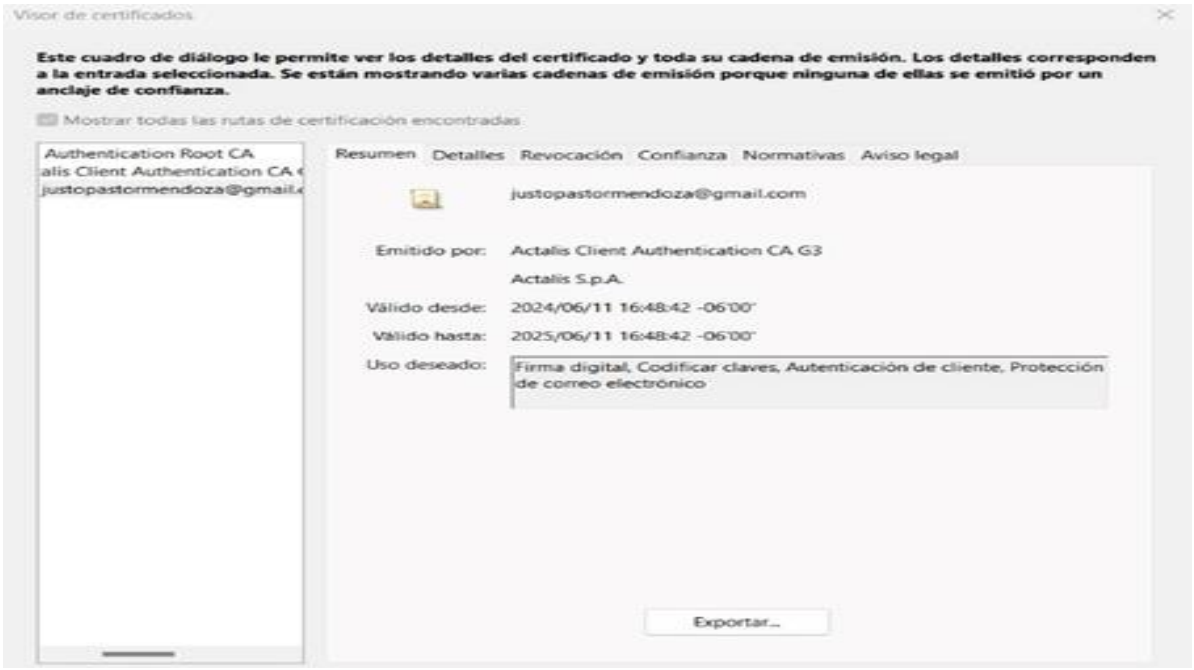



**Imagen 6: Detalles del Certificado de Firma electrónica**

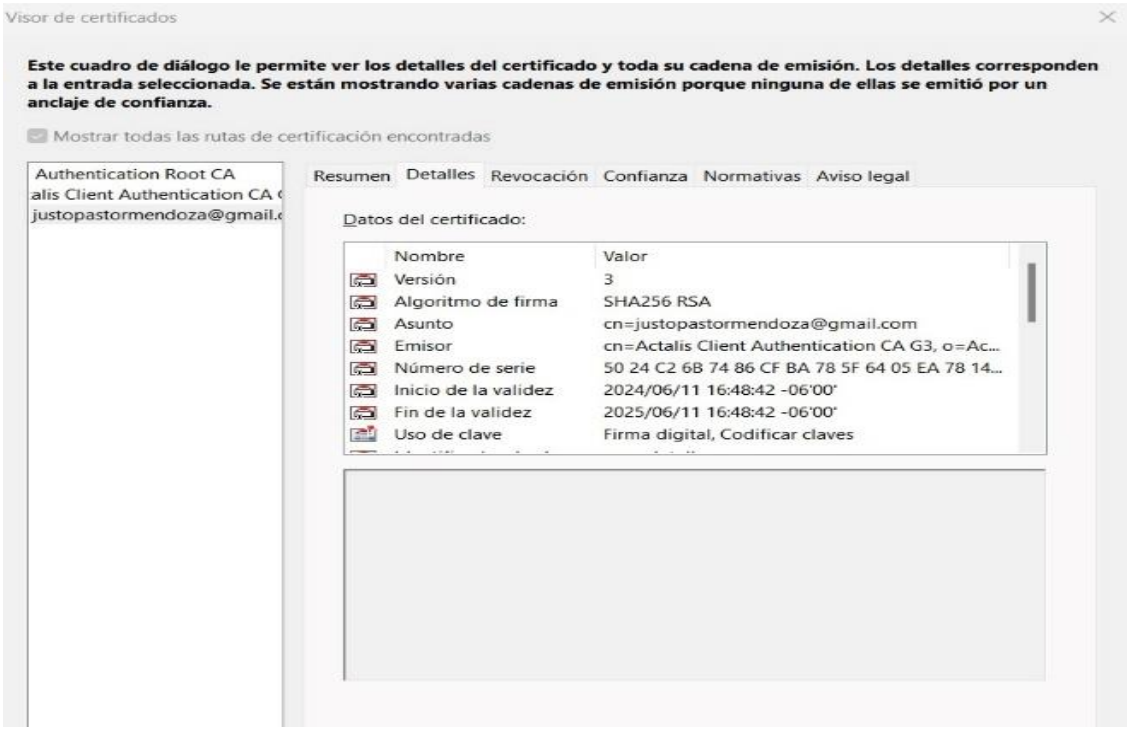
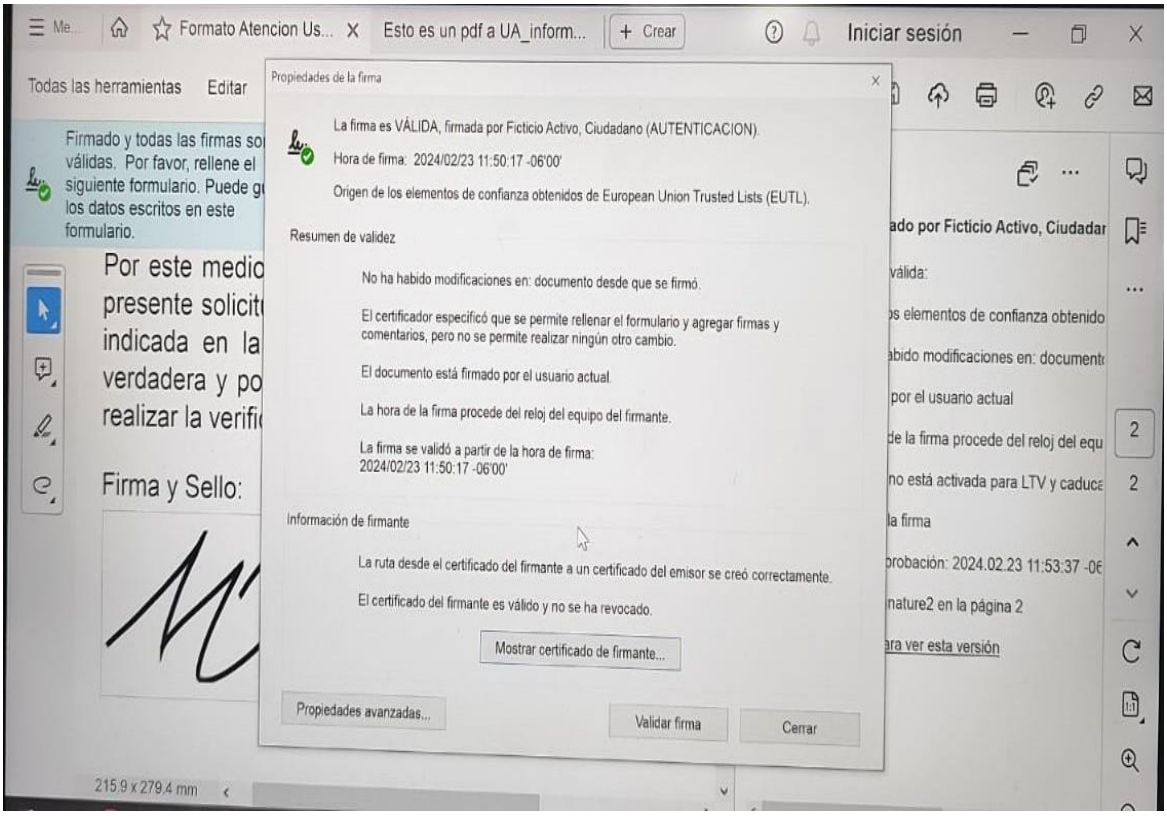


**Imagen 7: Confianza del Certificado de Firma electrónica**


**Imagen 8: Firmar**

**Imagen 9: Firma electrónica aplicado en el Documento.**


**Imagen 10: Verificación del certificado después de firmar**



#### 2.1.5.3 La Acreditación voluntaria

Es la autorización otorgada por el organismo público encargado de su acreditación y supervisión, a petición del proveedor al que se beneficie, y que establece los derechos y obligaciones específicas para la prestación de servicios.

#### 2.1.5.4 El Certificado

Es la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta.

#### 2.1.5.5 El Certificado de firma electrónica

Es el documento electrónico firmado electrónicamente cuyos datos son vinculados a su titular, y suministrado por un proveedor de servicios de certificación.

#### 2.1.5.6 El Certificado digital

Es la certificación electrónica que da fe sobre los datos que identifican a quien posee la clave pública de un criptograma.

#### 2.1.5.7 El Certificador

Es la Entidad proveedora de servicios de certificación de firma electrónica.

#### 2.1.5.8 Clave criptográfica

Es aquella que se utiliza en un criptosistema asimétrico para acceder a un documento con firma electrónica.

#### 2.1.5.9 El Criptosistema asimétrico

Es el algoritmo que utiliza un par de claves, una clave privada para firmar electrónicamente y su correspondiente clave pública para verificar dicha firma electrónica.

#### 2.1.5.10 Los Datos de creación de firma

Son los datos únicos, códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

#### 2.1.5.11 Los Dispositivos de creación de firma

Es un mecanismo que sirve para aplicar los datos de creación de firma.

#### 2.1.5.12 Datos de verificación de firma

Son los datos, códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

#### 2.1.5.13 Dispositivo de verificación de firma

Es un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de firma.

#### 2.1.5.14 Documento electrónico

Toda información generada, transferida, comunicada o archivada, por medios electrónicos, ópticos u otros análogos.

#### 2.1.5.15 Encriptar

Es el acto de utilizar una clave única antes de intercambiar información.

#### 2.1.5.16 Mensaje de datos

Es la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

#### 2.1.5.17 El Producto de firma electrónica certificada

Es el programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas.

#### 2.1.5.18 Los Proveedor de servicios de certificación

Son las Entidades que otorgan, registran, mantienen y publican los certificados de firma electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas que pueden prestar otros servicios relacionados con la firma electrónica.

#### 2.1.5.19 El Titular

Es la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona que representa.

### 2.1.6 *Causas y consecuencias del uso y desuso de la ley 729.*

#### 2.1.6.1 Causas del uso:

**Agilidad y eficiencia en los trámites:** La firma electrónica permite la automatización de procesos, reduciendo el tiempo y los costos asociados a la gestión tradicional de documentos en papel.

**Reducción del uso de papel:** La firma electrónica contribuye a la protección del medio ambiente al disminuir la necesidad de imprimir, firmar y enviar documentos físicos.

**Mayor seguridad y confiabilidad:** La firma electrónica utiliza mecanismos criptográficos que garantizan la integridad y autenticidad de los documentos, previniendo fraudes y falsificaciones.

**Accesibilidad y comodidad:** La firma electrónica permite a las personas firmar documentos desde cualquier lugar y en cualquier momento, sin necesidad de desplazarse o estar presente físicamente.

**Falta de conocimiento y cultura digital:** Existe un desconocimiento general sobre las ventajas y beneficios de la firma electrónica, lo que limita su adopción por parte de la población.

**Brecha digital:** La falta de acceso a internet y a dispositivos electrónicos por parte de algunos sectores de la población limita la utilización de la firma electrónica.

**Costos de implementación:** La implementación de la firma electrónica puede ser costosa para algunas empresas e instituciones, especialmente para las pymes.

#### 2.1.6.2 Consecuencias del desuso:

**Pérdida de competitividad:** Las empresas e instituciones que no adopten la firma electrónica pueden perder competitividad frente a las que sí lo hacen.

**Retraso en la modernización del Estado:** El desuso de la firma electrónica puede retrasar la modernización del Estado y la eficiencia de la administración pública.

**Limitación del acceso a servicios:** Las personas que no puedan utilizar la firma electrónica pueden verse limitadas en el acceso a ciertos servicios públicos y privados.

**Mayor riesgo de fraudes:** El uso de documentos en papel aumenta el riesgo de fraudes y falsificaciones.

## CAPÍTULO III: DISEÑO METODOLÓGICO

#### 3.1.1.1 Tipo de Estudio:

El presente estudio se enmarca en el enfoque cualitativo- hermenéutico, una metodología de investigación que busca comprender y describir la figura legal de la firma electrónica en Nicaragua mediante la recopilación y el análisis de información documental y de fuentes relacionadas con el tema. Este enfoque se centra en la interpretación de datos y en la comprensión profunda del

contexto, permitiendo así la generación de conclusiones basadas en la información obtenida a través de entrevistas, análisis de documentos legales y otras fuentes cualitativas. A diferencia de los estudios cuantitativos, este enfoque no se basa en la medición de variables específicas ni en la objetividad estricta, sino en la exploración detallada y la interpretación de la información para proporcionar una visión comprensiva del fenómeno estudiado.

#### 3.1.1.2 Área de Estudio:

La investigación se desarrollará en el departamento de Managua, con un enfoque particular en el Distrito número 1. Se pondrá especial atención en tres instituciones clave: la Dirección General de Tecnología (DGTEC). 2. BANPRO, Institución financiera de gran prestigio Nacional. 3. UNAN Managua, Institución de Educación Superior con presencia nacional. Estas instituciones representan sectores fundamentales en los cuales el uso de la firma electrónica podría tener un impacto significativo.

**Imagen 11: DGTEC-MHCP**

**Imagen 12: Banco de la Producción**

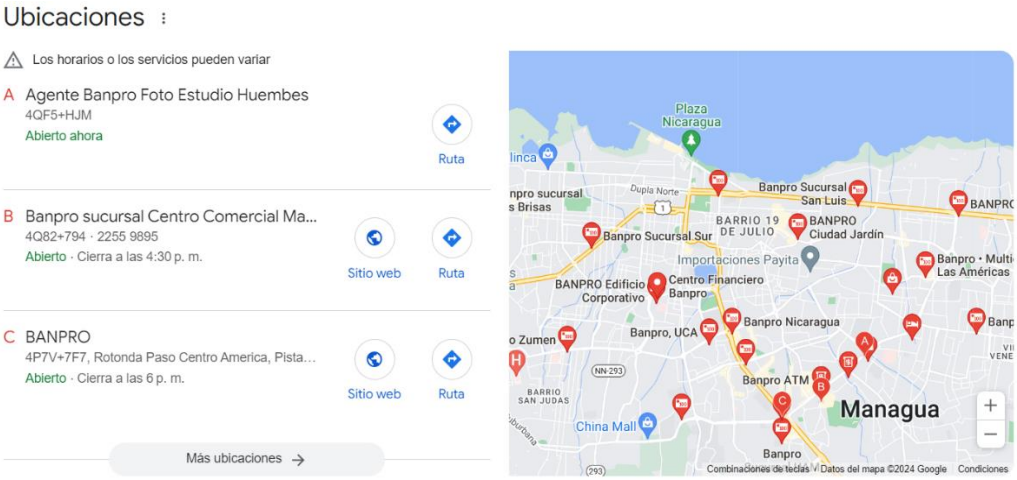



**Imagen 13: Universidad Nacional Autónoma de Nicaragua**


### 3.1.1.3 **Unidad** de **Análisis:**

La población es la ciudadanía del Departamento de Managua que es de 1,374,025 habitantes, con una densidad poblacional de 306 habitantes por kilómetro cuadrado. La muestra de estudio será de 3 expertos, la Dirección General de Tecnología (DGTEC), director de la Firma Electrónica, Asesora Legal Financiera y un abogado docente Investigador de la UNAN.

### 3.1.2 *Muestreo*

El método de muestreo empleado será no probabilístico a conveniencia y se aplicarán entrevistas.

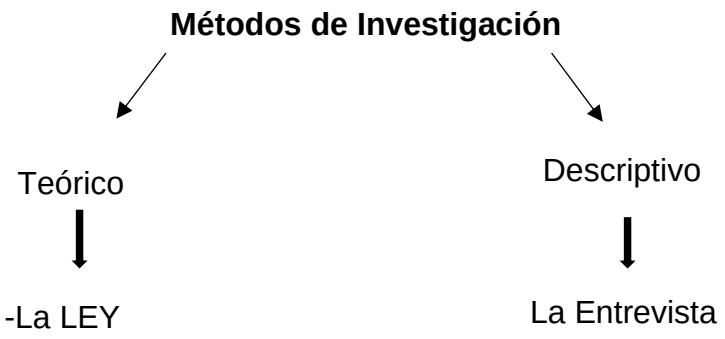
Bajo los criterios de inclusión:

1- Posean un conocimiento especializado y relevante en el tema de estudio.
2- Trabajan en áreas relacionadas a la firma electrónica.
3- Sean abogados de profesión.

#### 3.1.2.1 Métodos e Instrumentos utilizados:

En el marco de la investigación sobre la Firma Electrónica en Nicaragua, se ha adoptado un enfoque cualitativo debido a la necesidad de entender en profundidad las percepciones, experiencias y conocimientos de los actores involucrados en el uso y la regulación de la firma electrónica. A continuación, se describe el diseño metodológico y los instrumentos utilizados:

**Imagen 14: Métodos de Investigación**




1- Se desarrolló un análisis teórico bibliográfico siendo las referencias bibliográficas proporcionadas la Ley de Firma Electrónica y su Reglamento, emitidos en el año 2010 y 2011 respectivamente, por las autoridades legislativas de la República de Nicaragua. Además, se ha consultado la Ley Modelo de la Comisión de las Naciones Unidas para

el Derecho Mercantil Internacional (CNUDMI) sobre Firmas Electrónicas, junto con su Guía para la incorporación al Derecho Interno del año 2001. Estas fuentes legislativas proporcionan un marco legal y regulatorio que establece los criterios y requisitos para la validez y la seguridad de las transacciones electrónicas, incluyendo la recolección y autenticación de datos en entornos digitales. El análisis detallado de estas leyes y guías permite entender mejor las implicaciones legales y técnicas que pueden influir en el diseño y la implementación de los métodos e instrumentos de recolección de datos en este estudio.

2- Se ha aplicado entrevistas a las autoridades y expertos con el fin de generar información de campo, que nos permita gestionar de una mejor manera la utilización de la firma electrónica certificada en el contexto nacional.

**Estudio con enfoque Cualitativo:** El estudio se clasifica como teórico-hermenéutico y cualitativo, ya que se centra en la recopilación, análisis e interpretación de información detallada proveniente de fuentes primarias y secundarias. El objetivo es desarrollar una comprensión integral del tema, a través de técnicas cualitativas y análisis de variables, sobre: Firma electrónica, obstáculos en la firma, fomento de firma, y propuestas de aplicación, mediante la gestión de entrevistas a expertos.

**Técnicas de investigación:**

1. Entrevistas a Expertos:
    - Director de firma electrónico DGTEC
    - Asesora Legal Financiera
    - Catedrático de UNAN Managua

2. Estudio documental de los siguientes archivos:
    - Ley 729 y su reglamento
    - Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre Firmas Electrónicas

La información obtenida de inicio fue a través de entrevistas que realicé a las siguientes personas: al director de la Firma Electrónica, a una Asesora Legal Financiera y al Catedrático de UNAN Managua, quienes tienen el conocimiento sobre esta Ley. La entrevista dirigida al director de la Firma Electrónica constaba de 9 preguntas, la entrevista a la Asesora Legal Financiera constaba de 5 preguntas y, por último, la entrevista dirigida al Catedrático de UNAN Managua constaba de 8 preguntas, todas estas entrevistas eran únicas para cada persona, las cuales fueron escritas y grabadas al mismo tiempo. Logré obtener estas entrevistas mediante mi iniciativa de buscar los correos electrónicos de los expertos antes mencionados y escribirles solicitando formalmente que me brindaran un espacio de su valioso tiempo para hacerles una entrevista sobre la Ley 729.

#### 3.1.2.2 Confiabilidad y Validez de los Instrumentos:

La validación de instrumentos es un proceso crucial para garantizar su fiabilidad y validez en la medición de lo que se pretende evaluar. En el caso de la escala del 1 al 5, donde 1 y 2 indican una calificación baja, 3 es considerado aceptable, y 4 y 5 reflejan una calificación alta o excelente, la validación implica asegurarse de que las preguntas o ítems de la escala realmente capturan la información deseada y que la escala en sí misma es consistente a las diferencias en la variable medida. Esto implica revisión por parte de expertos en el campo para garantizar que los resultados sean válidos y confiables, en este caso calificaron las preguntas La Dirección de Investigación, la Coordinación de Carrera y un abogado de experiencia, aprobando el instrumento para darle validez.

**TABLA 1 Validación de Instrumento**

Se calificó el instrumento a través de una tabla de valor, que va del 1 al 5, donde 1 y 2 indican una calificación baja, 3 es considerado aceptable, y 4 y 5 reflejan una calificación alta o excelente.

| Pregunta | Coordinadora de la carrera de Derecho: Giselle Vázquez | Director de Investigación: Fernando Monge | Licenciado en Derecho: Franklin Jarquín | Promedio |
|---|---|---|---|---|
| ¿Qué ocasionó o influyó para crear la Ley 729 en nuestro país? ¿Hay alguna ley similar anterior a esta? | **5** | **4** | **5** | **5** |
| ¿Cuál es la diferencia entre firma electrónica, firma digital y firma electrónica certificada? | **5** | **4** | **5** | **5** |
| ¿Se está cumpliendo lo que dice la ley 729 y su reglamento con el uso de la Firma Electrónica Certificada en las instituciones públicas y privadas? | **5** | **5** | **5** | **5** |
| ¿Cuál sería el motivo por el cual no hay Proveedores de Servicios de certificación de Firma Electrónica en nuestro país? | **5** | **5** | **5** | **5** |
| ¿La firma Certificada tiene que ser obligatoriamente la misma que está en el documento de identidad de la persona, o es otra? | **5** | **5** | **5** | **5** |
| ¿Las Firmas Electrónicas Certificadas solo se pueden utilizar por medio de dispositivos inteligentes, o se puede en papel físico? | **4** | **4** | **5** | **4** |
| Siendo titular de una F.E.C, ¿cómo me puedo dar cuenta si los Proveedores de Servicio de | **5** | **5** | **5** | **5** |

| | | | | |
|---|---|---|---|---|
| Certificación hicieron mal uso de mis datos, y ante quién hago el reclamo? | | | | |
| ¿Existe algún proyecto de parte del Estado en conjunto con la Empresa Privada para promover en los Bancos y en el comercio mismo el uso de la Firma Electrónica Certificada? | **5** | **5** | **5** | **5** |
| ¿En qué beneficia la Firma Electrónica al Estado y a los particulares? | **5** | **5** | **5** | **5** |
| | | | | **5** |

| **Pregunta** | **Coordinadora de la carrera de Derecho: Giselle Vázquez** | **Director de Investigación: Fernando Monge** | **Licenciado en Derecho: Franklin Jarquín** | **Promedio** |
|---|---|---|---|---|
| ¿Cuál es su opinión sobre la adopción de la Ley 729 de Firma Electrónica en Nicaragua y su implementación en el país hasta la fecha? | **5** | **5** | **4** | **5** |
| ¿Cuáles son las diferencias clave entre la Firma Electrónica y la Firma Electrónica Certificada, y por qué es importante esta distinción en el marco legal nicaragüense? | **4** | **5** | **5** | **5** |

| | | | | |
|---|---|---|---|---|
| ¿Cuáles considera que son los principales obstáculos o desafíos que han impedido el uso de la Firma Electrónica en el país? | **5** | **5** | **5** | **5** |
| ¿Qué medidas considera necesarias para fomentar la confianza y la adopción de la Firma Electrónica Certificada por parte de las instituciones públicas y privadas en Nicaragua? | **5** | **4** | **4** | **4** |
| ¿Qué papel desempeña la capacitación y la concienciación sobre la Firma Electrónica Certificada en la promoción de su uso entre los profesionales del derecho y otros actores relevantes? | **4** | **5** | **5** | **5** |
| ¿Considera que se necesitan reformas adicionales en la legislación nicaragüense o en las políticas gubernamentales para facilitar la implementación y el uso de la Firma Electrónica Certificada? En caso afirmativo, ¿cuáles serían esas reformas? | **5** | **5** | **5** | **5** |
| ¿Cuál es su visión sobre el futuro de la Firma Electrónica Certificada en Nicaragua y cómo podría influir en la eficiencia y la modernización de los procesos legales y comerciales en el país? | **5** | **4** | **3** | **4** |
| ¿En qué beneficia la Firma Electrónica a los Profesionales del Derecho? | **5** | **5** | **4** | **4** |
| | | | | **5** |

| Pregunta | Coordinadora de la carrera de Derecho: Giselle Vázquez | Director de Investigación: Fernando Monge | Licenciado en Derecho: Franklin Jarquín | Promedio |
|---|---|---|---|---|
| ¿Cuáles considera que son los principales beneficios que la implementación de la Firma Electrónica Certificada podría ofrecer tanto a los bancos como al país en general? | **5** | **5** | **5** | **5** |
| ¿Qué medidas o estrategia considera que deberían implementar los bancos para promover y facilitar el uso de la Firma Electrónica Certificada entre sus clientes o dentro de sus procesos internos? | **5** | **5** | **5** | **5** |
| ¿Cómo cree que la Firma Electrónica Certificada podría contribuir a la eficiencia y la modernización del sector legal y empresarial en Nicaragua? | **5** | **5** | **5** | **5** |
| ¿Cree que la adopción de la Firma Electrónica podría aumentar la eficiencia y agilidad de los procesos en el sector financiero en Nicaragua? ¿Por qué? | **5** | **5** | **5** | **5** |
| ¿Qué recomendaciones tendría usted para mejorar la confianza y la aceptación del uso de la Firma Electrónica Certificada tanto a nivel institucional como a nivel nacional? | **5** | **4** | **4** | **4** |
| | | | | **5** |

Fuente: Elaboración Propia

**TABLA 2 OPERACIONALIZACIÓN DE LA VARIABLE:**

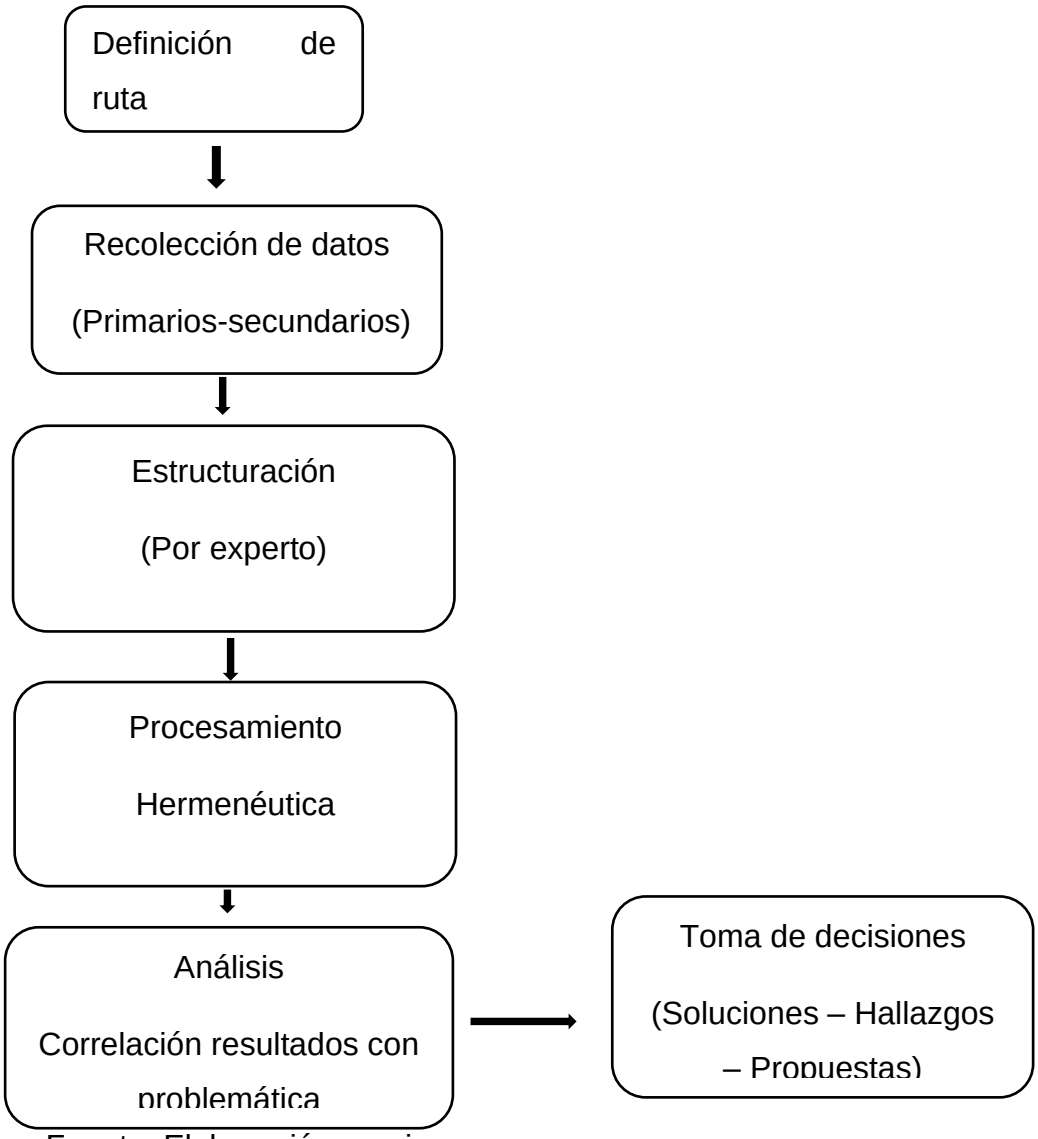
| Objetivo | Variable | Tipo de Variable | Definición Conceptual | Dimensión Operacional | Técnicas e Instrumentos de Recolección de datos |
|---|---|---|---|---|---|
| •Identificar los principales obstáculos que dificultan la implementación efectiva de la Ley 729, Ley de Firma Electrónica en Nicaragua. | Falta de instituciones que acrediten la firma electrónica certificada. | Dependiente | Ausencia o insuficiencia de organismos, entidades o autoridades que tienen la capacidad y autorización legal para verificar y certificar la autenticidad y validez de firmas electrónicas. | No existe tracto jurídico y comercial con el uso de este tipo de instrumento. | Entrevistas |
| | Falta de interés del sector comercial en su uso. | Dependiente | Desinterés mostrado por las empresas y entidades comerciales hacia la adopción, implementación o promoción de la ley. | Nula Adopción o implementación de la ley de F.E. | |
| •Fomentar la adopción generalizada de la firma | Confiabilidad. | Independiente | Es la capacidad de considerar algo creíble | | Entrevistas |

| | | | | | |
|---|---|---|---|---|---|
| electrónica para potenciar la eficiencia en operaciones jurídicas, financieras y comerciales entre individuos, así como entre instituciones privadas y estatales. | | | y veraz. Implica la integridad de la información presentada, así como la credibilidad y la imparcialidad de las fuentes de donde proviene. | 1. Adopción y efectividad de la Firma Electrónica.<br>2. Identificación de Áreas de Mejora. | |
| •Proponer soluciones viables para hacer que la Ley 729 sea más accesible a los particulares, empresarios locales e instituciones estatales. | Seguridad Jurídica | Independiente | Se refiere a la certeza y estabilidad que proporciona el ordenamiento jurídico a los individuos y a la sociedad en general | 1. Aumento de la Confianza de los Usuarios.<br>2. Claridad y Previsibilidad.<br>3. Protección Contra el Fraude y el Abuso.<br>4. Reconocimiento Internacional | Entrevistas |

### 3.1.2.3 Procesamiento y Plan de Análisis de la Información:

El procesamiento de los datos a partir de los instrumentos que se propone para el desarrollo de esta investigación se efectuará siguiendo todo el proceso desde la recolección de datos, hasta la presentación de los mismos en forma resumida. Tiene básicamente tres etapas: 1- recolección 2- entrada, 3- procesamiento y presentación. Se presenta de forma resumida como se llevará a cabo el procedimiento de la información.

**Imagen 15: Procesamiento de los datos**




Fuente: Elaboración propia.

Para el análisis de la información obtenida, se realizó una lectura exhaustiva de la Ley 729, Ley de Firma Electrónica en Nicaragua, para entender el marco legal vigente. Además, se llevaron a cabo entrevistas con expertos en el tema, incluyendo a Hans Espinoza Acuña, director de la Firma Electrónica, Odair Márquez, docente de Derecho, y Kenia Montoya Chavarría, Asesora Legal Financiera. Estas entrevistas permitieron correlacionar los resultados con la problemática planteada, proporcionando una visión integral y detallada del estado actual y las posibles mejoras en la implementación de la firma electrónica en el país.

# CAPÍTULO IV: ANÁLISIS Y RESULTADOS

## 1. Entrevista al director de la DGTEC:

El director de la Dirección General de Tecnología (DGTEC), respeto a la pregunta sobre la creación de la Ley 729, destacó que el origen de la firma electrónica en Nicaragua se remonta al Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA) en 2003, posteriormente complementado en 2008. La Ley 729 de Firma Electrónica, promulgada en 2011, se basó en las Leyes Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), específicamente en la Ley Modelo de Firma Electrónica y la Ley Modelo del Comercio Electrónico. Esta ley proporciona un marco legal integral para el uso de la firma electrónica en Nicaragua. Cabe agregar a lo que externo el entrevistado, que la Ley 729 se fundamenta en estándares internacionales, lo que subraya un esfuerzo por alinearse con prácticas globales. Sin embargo, la adopción de tales marcos puede enfrentar desafíos locales en infraestructura y recursos, lo que puede explicar algunos de los problemas en su implementación.

Según el director de la DGTEC, la Ley 729 no se cumple adecuadamente debido a la ausencia de proveedores de servicios de certificación. La infraestructura necesaria es costosa y los bancos y el sector privado no cuentan con centros de datos seguros ni medidas de seguridad adecuadas.

Respecto a los Proveedores de Servicios de Certificación, respondió que la percepción de altos costos y la falta de infraestructura tecnológica y capital para gestionar riesgos potenciales son las principales razones detrás de la ausencia de proveedores de servicios de certificación.

El director explicó las diferencias entre la firma electrónica (un archivo con usuario y contraseña), la firma digital (incluye certificados digitales y datos biométricos) y la firma

electrónica certificada (FEC), que integra ambos y es emitida por un proveedor de servicios de certificación.

Compartió que no existen proyectos conjuntos entre el Estado y la empresa privada para promover el uso de la ley 729, de la firma electrónica certificada en el sector bancario y el comercio. Enfatizó que las firmas electrónicas certificadas solo pueden ser utilizadas por medios electrónicos.

Explicó que la FEC se genera cuando un USB, microchip o tarjeta inteligente creada y respaldada por un proveedor de servicio de certificación con los datos del titular, se conecta al dispositivo donde se firmará el documento. Este dispositivo convierte los datos en códigos únicos y el certificado emitido refleja en forma resumida los detalles del documento firmado.
Este proceso asegura la autenticidad y la integridad del documento firmado. Sin embargo, la dependencia de hardware específico (USB o microchip) puede ser una barrera si no está ampliamente disponible o es costoso.

Finalmente expresó que la FEC beneficia tanto al Estado y a los individuos, al primero le permite enviar notificaciones oficiales electrónicamente, eliminando la necesidad de envío postal, también mejora la eficiencia operativa facilitando la colaboración y el intercambio de documentos entre departamentos gubernamentales; y al último, le facilita la gestión remota de documentos ya que le permite firmar contratos, formularios y otros documentos sin necesidad de desplazarse físicamente. Además, es accesible para personas con discapacidades, lo que proporciona una solución práctica para los que tienen dificultades en firmar documentos físicamente.

### 2. Entrevista al Maestro de Derecho:

El maestro de derecho considera la Ley 729 como un instrumento valioso para modernizar la gestión pública y privada. Sin embargo, requiere un esfuerzo conjunto para su plena implementación, incluyendo la promoción, simplificación de

procedimientos para certificados digitales, fomento de nuevas entidades certificadoras y actualización de la normativa.

Para el Maestro de Derecho la firma electrónica (FE) tiene un menor nivel de seguridad en comparación con la firma electrónica certificada (FEC), que requiere un certificado emitido por una entidad acreditada y tiene el mismo valor jurídico que una firma manuscrita.

Agregó que los obstáculos principales para la implementación de la ley 729, son la falta de conocimiento y cultura digital, infraestructura tecnológica deficiente, barreras legales y regulatorias, déficit de capacitación y desconfianza en los sistemas electrónicos.

Mencionó que la capacitación y concienciación es crucial para actualizar conocimientos y habilidades, y fomentar la confianza en la FEC entre abogados y notarios; y que también ayuda a reducir la brecha digital y promover la aceptación e innovación entre otros actores. Así mismo, sugiere reformas para simplificar trámites, establecer costos subvencionados, fortalecer la infraestructura tecnológica y promover la cultura digital mediante programas educativos y de sensibilización.

Finalizó con que unos de los principales beneficios para los abogados es la reducción de costos, el acceso remoto ya que permite a los abogados firmar y enviar documentos desde cualquier lugar y en cualquier momento, simplifica procesos como la firma de poderes y mandatos y también gestiona y archiva electrónicamente, optimizando la administración de expedientes judiciales.

### 3. Entrevista a la Asesora Legal Financiera:

Para la Asesora legal financiera, la ley de FEC, proporciona varios beneficios, como: agilizar trámites, reducir la documentación física y mejorar la seguridad de las

transacciones bancarias. También promueve un entorno más seguro para negocios, mejora la eficiencia administrativa y contribuye a reducir el fraude y la corrupción. Y para poder gozar de esos beneficios ella recomienda que se deben aplicar algunas medidas para promover la FEC, por ejemplo: realizar campañas publicitarias, talleres, materiales educativos, ofrecer precios accesibles, simplificar procesos, proporcionar soporte técnico, desarrollar aplicaciones y servicios que aprovechen la FEC, compartir casos de éxito y promover la interoperabilidad.

Mencionó también que la FEC contribuye a la modernización, ya que facilita la celebración de contratos y acuerdos de manera remota, mejora la trazabilidad y transparencia en transacciones, y reduce el papeleo, contribuyendo a un entorno de negocios más eficiente, especialmente en un entorno empresarial globalizado

La asesora legal destacó que la FEC aumenta la eficiencia en el sector financiero, al permitir procesar transacciones más rápidamente, reducir tiempos de espera y fortalecer la seguridad de las operaciones; generando beneficios económicos sustanciales y una mayor competitividad para las instituciones financieras que adopten esta tecnología.

Finalizó que es esencial continuar con campañas de educación y sensibilización, actualizar constantemente la infraestructura y las normativas, y fomentar la colaboración entre el sector público y privado para crear un marco regulatorio robusto y una cultura de confianza en la tecnología.

Después de obtener los resultados de las entrevistas a los tres expertos en el tema de la ley 729, de firma electrónica, se ha llevado a cabo un análisis detallado de las respuestas obtenidas. A continuación, se presenta el análisis sobre los beneficios que la firma electrónica ofrece a distintos sectores clave, como el Estado, los individuos, los abogados y el sector bancario. Este análisis refleja una síntesis de las perspectivas de los expertos, y de la interpretación de la autora, de cómo esta tecnología impacta

positivamente en la eficiencia y accesibilidad de los procesos en cada uno de estos sectores.

Beneficios de la Firma Electrónica:

- Para el Estado

En primer lugar, permite al Estado enviar notificaciones oficiales a los ciudadanos, como multas de tráfico y avisos fiscales, de manera electrónica, lo que resulta en un considerable ahorro de tiempo y recursos al eliminar la necesidad del envío postal. Además, la firma electrónica habilita la prestación de diversos servicios públicos en línea, facilitando la obtención de certificados, licencias y permisos, lo que mejora notablemente la accesibilidad para los ciudadanos.

De igual manera, las plataformas gubernamentales ofrecen la posibilidad a los ciudadanos de firmar electrónicamente para realizar trámites como el registro de vehículos o la solicitud de pasaportes, entre otros, simplificando así los procedimientos administrativos.

Por último, la firma electrónica facilita la colaboración y el intercambio de documentos entre los distintos departamentos y organismos gubernamentales, mejorando la eficiencia operativa del Estado. Esta tecnología no solo optimiza los procesos internos, sino que también contribuye a un servicio más eficiente y accesible para la ciudadanía.

- Para los Individuos

Facilita la gestión de documentos y procesos de manera remota. Por ejemplo, en el ámbito laboral, permite a los trabajadores firmar contratos, formularios de nómina y otros documentos de recursos humanos sin necesidad de desplazarse físicamente a la oficina, ahorrando tiempo y mejorando la eficiencia.

Además, en el ámbito educativo y administrativo, es posible firmar electrónicamente formularios de inscripción, permisos y acuerdos de uso de servicios escolares. Esto

agiliza los trámites y elimina la necesidad de gestionar documentos en papel. En el ámbito de la salud, los pacientes pueden firmar formularios médicos, consentimientos y registros de seguro médico desde cualquier lugar, lo cual es particularmente beneficioso para aquellos con movilidad limitada.

En el contexto de la compra de vivienda, la firma electrónica permite a los compradores y vendedores firmar contratos de compra-venta, hipotecas y otros documentos necesarios de manera remota. Esto no solo simplifica el proceso, sino que también reduce los costos y el tiempo asociados con el manejo de documentos físicos. De manera similar, los inquilinos y propietarios pueden firmar contratos de arrendamiento electrónicamente, lo que facilita el proceso de alquiler.

Un aspecto importante de la firma electrónica es su accesibilidad. Las personas con discapacidades que pueden tener dificultades para firmar documentos físicamente encuentran en la firma electrónica una solución práctica y conveniente. Además, al reducir la necesidad de imprimir documentos, se contribuye a la sostenibilidad y protección del medio ambiente, disminuyendo el uso de papel y los residuos asociados.

- Para los Abogados

La capacidad de presentar documentos electrónicamente elimina la necesidad de desplazamientos físicos, reduciendo tanto el tiempo de espera como los costos operativos. Las notificaciones judiciales también se agilizan, permitiendo una comunicación instantánea y segura entre las partes involucradas.

Uno de los principales beneficios es la reducción de costos. La disminución del uso de papel implica menores gastos en impresión, transporte y almacenamiento de documentos físicos. Además, el acceso remoto permite a los abogados firmar y enviar documentos desde cualquier lugar y en cualquier momento, lo que facilita una práctica jurídica más flexible y adaptada a la era digital. Esta tecnología también facilita la

colaboración internacional, permitiendo la firma de documentos en transacciones legales sin importar las barreras geográficas.

En cuanto al cumplimiento legal, las firmas electrónicas están respaldadas por normativas y estándares que aseguran su validez y reconocimiento legal, como es el caso de la Ley de Firma Electrónica. Esto permite a los abogados redactar, enviar y recibir contratos de forma electrónica, acelerando el cierre de acuerdos y evitando los retrasos del correo tradicional. Los trámites administrativos, como la presentación de pruebas y mociones, también se benefician, ya que se pueden gestionar y archivar electrónicamente, optimizando la administración de expedientes judiciales.

La firma electrónica simplifica procesos como la firma de poderes y mandatos, facilitando la representación de clientes en juicios o transacciones y reduciendo el riesgo de falsificaciones.

- Para el Sector Bancario

La digitalización en el sector bancario transformaría significativamente la forma en que los clientes interactúan con los servicios financieros. Un aspecto crucial de esta transformación es la apertura de cuentas bancarias en línea, eliminando la necesidad de acudir a una sucursal física. Este cambio no solo agiliza el proceso de apertura de cuentas, sino que también reduce considerablemente el tiempo de espera para los clientes.

Otro beneficio destacado de la digitalización es la rapidez en la solicitud y aprobación de préstamos. La posibilidad de firmar y enviar documentos electrónicamente elimina el retraso asociado al papeleo físico, lo que acelera todo el proceso de aprobación. Además, la ausencia de necesidad de presencia física y de envío de documentos reduce los costos de mensajería y transporte para los bancos y sus clientes.

La firma electrónica, es una pieza clave en este ecosistema digital, aportando una mayor seguridad al proceso, garantizando la autenticidad del firmante y la integridad

de los documentos. Los registros electrónicos permiten verificar quién firmó y cuándo, lo cual es esencial para mitigar el riesgo de fraude. Estas firmas electrónicas no solo cumplen con diversas regulaciones legales y estándares internacionales, proporcionando un marco legal seguro para las transacciones, sino que también se integran fácilmente con otros sistemas bancarios, como los sistemas de gestión de relaciones con clientes y los sistemas de gestión documental.

Además, los documentos firmados electrónicamente se almacenan en formato digital, lo que facilita su búsqueda y recuperación. Esto no solo mejora la gestión documental, sino que también permite un acceso más rápido y eficiente a la información necesaria.

La digitalización en el sector bancario, impulsada por la adopción de firmas electrónicas y la gestión electrónica de documentos, optimizaría significativamente los procesos bancarios en el país, ofreciendo mayor rapidez, seguridad y eficiencia, tanto para las instituciones financieras como para sus clientes.

En resumen, basado en las entrevistas, se ha logrado identificar que coinciden en la importancia de la ley 729 de firma electrónica para modernizar los procesos en diversos sectores de Nicaragua, incluyendo el Estado, los individuos, los abogados y el sector bancario.

Se destaca el potencial de la firma electrónica para agilizar trámites, reducir costos, mejorar la seguridad y la transparencia, y promover la eficiencia en diferentes áreas.

Las tres fuentes coinciden en que la firma electrónica certificada (FEC) ofrece el más alto nivel de seguridad y tiene el mismo valor jurídico que una firma manuscrita.

## CAPÍTULO V: CONCLUSIONES

La investigación sobre la Ley 729 de Firma Electrónica en Nicaragua muestra que, aunque está en vigor desde 2011, su aplicación efectiva sigue siendo un gran reto. Los obstáculos son la escasez de proveedores de certificados digitales, los altos costos de la infraestructura requerida y la falta de un entorno tecnológico adecuado. Además, la falta de conocimiento y cultura digital, junto con obstáculos legales y regulatorios, agravan estos desafíos. La insuficiente capacitación y la desconfianza en los sistemas electrónicos también han contribuido a la baja adopción de la firma electrónica.

La firma FEC tiene el potencial de agilizar trámites, reducir la necesidad de documentación física y mejorar la seguridad en las transacciones, lo que puede llevar a un entorno empresarial más eficiente y seguro, disminuyendo el fraude y la corrupción a nivel nacional. La adopción se fomentó a través de la divulgación de estos datos con expertos de instituciones de alto prestigio en la recapitulación teórica y propuesta de soluciones a ser compartidas a través de la extensión del estudio.

Los resultados indican que es crucial mejorar la infraestructura tecnológica, fomentar la cultura digital, simplificar los procedimientos, promover la colaboración entre el sector público y privado para crear un marco regulatorio robusto e impulsar el uso de la firma electrónica a nivel nacional.

Con el uso de la firma electrónica, la difusión del comercio electrónico en Nicaragua mejorará la competitividad de nuestra economía y, al mismo tiempo, favorecerá el nivel y la calidad de vida de los nicaragüenses mediante la creación de nuevos empleos mejor remunerados. Las pequeñas y medianas empresas se beneficiarán de las oportunidades emergentes para vender sus productos en los mercados locales, regionales y mundiales y los consumidores, por su parte, se beneficiarán de una creciente variedad de bienes y servicios a precios menores.

## CAPÍTULO VI: RECOMENDACIONES, REFERENCIAS BIBLIOGRÁFICAS Y ANEXOS.

- Es esencial incentivar el desarrollo de proveedores de servicios de certificación y del uso de la firma por parte de los individuos y sector privado mediante subsidios y estímulos gubernamentales, por ejemplo: Ofrecer exoneraciones fiscales temporales para los P.S.C que operen en el país, facilitar préstamos con tasas de interés reducidas para empresas que desean adoptar la firma electrónica, ofrecer descuentos en servicios gubernamentales o privados para usuarios que utilicen la firma electrónica, implementar programas de recompensas para los ciudadanos que realicen trámites electrónicos utilizando la firma electrónica y establecer premios y reconocimientos para las empresas y organizaciones que lideren en la adopción de la firma electrónica.

- Implementar programas continuos de capacitación para abogados, notarios y otros actores relevantes mediante el Consejo General del Poder Judicial o escuela judicial para mantener sus conocimientos actualizados. Al mismo tiempo, se deben llevar a cabo campañas de sensibilización para reducir la brecha digital y aumentar la aceptación de la firma electrónica por medio del Centro Nacional de Innovación y Tecnología.

- Simplificar los trámites administrativos y establecer costos accesibles para obtener y usar firmas electrónicas. Esto incluye crear procedimientos más simples y menos burocráticos.

- Invertir en la modernización y actualización de la infraestructura tecnológica. Esto incluye asegurar una conexión a internet estable y de alta velocidad en todo el país.

- Realizar campañas publicitarias efectivas y organizar talleres prácticos para educar al público sobre la seguridad y beneficios de la firma electrónica, destacando casos de éxito y buenas prácticas.

- Integrar cursos sobre firma electrónica en los programas educativos de universidades y centros de formación técnica.

- Desarrollar plataformas y herramientas accesibles y fáciles de usar para la firma electrónica, promoviendo su integración en los sistemas existentes de las empresas y bancos.

- Promover la colaboración entre el sector público y privado para crear un marco regulatorio robusto y una cultura de confianza en la tecnología. Primero, establecer mesas de diálogo y comités conjuntos que incluyan representantes clave de ambos sectores, asegurando que todos los actores relevantes tengan voz en el proceso. Segundo, desarrollar acuerdos de cooperación y alianzas estratégicas que definan roles y responsabilidades claras, así como objetivos comunes. Tercero, organizar foros, seminarios y talleres donde se compartan conocimientos y experiencias sobre la implementación y uso de la firma electrónica, fomentando la educación y la confianza en la tecnología. Finalmente, se debe establecer un sistema de seguimiento y evaluación continua para asegurar que la colaboración sea efectiva y que se alcancen los objetivos propuestos.

- Mantener las normativas actualizadas para adaptarse a los avances tecnológicos y a las necesidades del mercado. Esto incluye la revisión periódica de la Ley 729 y sus regulaciones complementarias.

Implementar estas recomendaciones puede ayudar a superar los obstáculos actuales y fomentar la adopción generalizada de la firma electrónica en Nicaragua, potenciando así la eficiencia en las operaciones jurídicas, financieras y comerciales en todo el país.

## REFERENCIAS BIBLIOGRÁFICAS

*Holguín García F., Y (2018). Análisis de la firma digital con base en la infraestructura de clave pública. Hamut´ay, vol. 5, Número.2.* https://revistas.uap.edu.pe/ojs/index.php/HAMUT/article/view/1622/1517

*MINISTERIO DE ECONOMIA, FOMENTO Y RECONSTRUCCION; SUBSECRETARIA DE ECONOMIA, FOMENTO Y RECONSTRUCCION (2002) Historia de la Ley Nº19.799. Ley N. ª 19799. Recuperado de* https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/567/1/hdl-19799.pdf

*Daniel, (10 de febrero del 2021). Historia de la Firma Electrónica en México. Recuperado de* https://blog.digitafirma.com/firma-electronica-avanzada/

*Publicado el 20 de septiembre de 2019. Actualizado el 29 de septiembre de 2022. Docusign. La validez jurídica de la firma electrónica en México. Recuperado de* https://www.docusign.com/es-mx/blog/validez-juridica-de-la-firma-electronica-en-mexico

*Nations, U. (2002). Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al Derecho Interno 2001.*

*Nitro Software, Inc., 2023. Canadá. Guías de Legalidad Canadá. Sobre la Legislación de Firmas Electrónicas en Canadá. Recuperado de* https://www.gonitro.com/es/sign/legality-guide/canada#

*Licencia Creative Commons Atribución-CompartirIgual 4.0. (22 de mayo del 2024) Firma Electrónica. Regulaciones en diferentes países. Recuperado de* https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica

*LEY DE FIRMA ELECTRÓNICA*. (2010). http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/4f3839183e874782062577e60050674d?OpenDocument

*REGLAMENTO DE LA LEY 729, LEY DE FIRMA ELECTRÓNICA*. (2011). http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/1ceea41dc1bdc53d06257951005bbc04?OpenDocument

# ANEXOS

## Anexo 1

INSTRUMENTO / CUESTIONARIO APLICADO EN LAS ENTREVISTAS:

UCC

Derecho con Mención en Gerencia Empresarial

Nombre: Hans Humberto Espinoza Acuña

Puesto: director de Firma Electrónica

Años de experiencia: 14

**1)** Entrevista dirigida al director de Firma Electrónica.

¿Qué ocasionó o influyó para crear la Ley 729 en nuestro país? ¿Hay alguna ley similar anterior a esta?

¿Cuál es la diferencia entre firma electrónica, firma digital y firma electrónica certificada?

¿Se está cumpliendo lo que dice la ley 729 y su reglamento con el uso de la Firma Electrónica Certificada en las instituciones públicas y privadas?

¿Cuál sería el motivo por el cual no hay Proveedores de Servicios de certificación de Firma Electrónica en nuestro país?

¿La firma Certificada tiene que ser obligatoriamente la misma que está en el documento de identidad de la persona, o es otra?

¿Las Firmas Electrónicas Certificadas solo se pueden utilizar por medio de dispositivos inteligentes, o se puede en papel físico?

Siendo titular de una F.E.C, ¿cómo me puedo dar cuenta si los Proveedores de Servicio de Certificación hicieron mal uso de mis datos, y ante quién hago el reclamo?

¿Existe algún proyecto de parte del Estado en conjunto con la Empresa Privada para promover en los Bancos y en el comercio mismo el uso de la Firma Electrónica Certificada?

¿En qué beneficia la Firma Electrónica al Estado y a los particulares?

**Anexo 2**

Entrevista dirigida a Abogado, docente de la UNAN.

INSTRUMENTO / CUESTIONARIO APLICADO EN LAS ENTREVISTAS:

UCC

Derecho con Mención en Gerencia Empresarial

Nombre: Odair Marcelo Morales Márquez

Puesto: Docente

Años de experiencia: 10

¿Cuál es su opinión sobre la adopción de la Ley 729 de Firma Electrónica en Nicaragua y su implementación en el país hasta la fecha?

¿Cuáles son las diferencias clave entre la Firma Electrónica y la Firma Electrónica Certificada, y por qué es importante esta distinción en el marco legal nicaragüense?

¿Cuáles considera que son los principales obstáculos o desafíos que han impedido el uso de la Firma Electrónica en el país?

¿Qué medidas considera necesarias para fomentar la confianza y la adopción de la Firma Electrónica Certificada por parte de las instituciones públicas y privadas en Nicaragua?

¿Qué papel desempeña la capacitación y la concienciación sobre la Firma Electrónica Certificada en la promoción de su uso entre los profesionales del derecho y otros actores relevantes?

¿Considera que se necesitan reformas adicionales en la legislación nicaragüense o en las políticas gubernamentales para facilitar la implementación y el uso de la Firma Electrónica Certificada? En caso afirmativo, ¿cuáles serían esas reformas?

¿Cuál es su visión sobre el futuro de la Firma Electrónica Certificada en Nicaragua y cómo podría influir en la eficiencia y la modernización de los procesos legales y comerciales en el país?

¿En qué beneficia la Firma Electrónica a los Profesionales del Derecho?

**Anexo 3**

Entrevista dirigida a Asesora Legal Financiera.

INSTRUMENTO / CUESTIONARIO APLICADO EN LAS ENTREVISTAS:

UCC

Derecho con Mención en Gerencia Empresarial

Nombre: Kenia Montoya Chavarría
Puesto: Asesora Legal Financiera
Años de experiencia: 12

¿Cuáles considera que son los principales beneficios que la implementación de la Firma Electrónica Certificada podría ofrecer tanto a los bancos como al país en general?

¿Qué medidas o estrategia considera que deberían de implementar los bancos para promover y facilitar el uso de la Firma Electrónica Certificada entre sus clientes o dentro de sus procesos internos?

¿Cómo cree que la Firma Electrónica Certificada podría contribuir a la eficiencia y la modernización del sector legal y empresarial en Nicaragua?

¿Cree que la adopción de la Firma Electrónica podría aumentar la eficiencia y agilidad de los procesos en el sector financiero en Nicaragua? ¿Por qué?

¿Qué recomendaciones tendría usted para mejorar la confianza y la aceptación del uso de la Firma Electrónica Certificada tanto a nivel institucional como a nivel nacional?