UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Firma Electrónica en El Salvador: retos y oportunidades

PRESENTADO POR

Nelson Douglas Grande Sánchez

Víctor Manuel Guardado Sandoval

ASESOR

Mg. Leonel Maye

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Julio 2023

Índice

Índice de figuras

Índice de Tablas

Abreviaturas

CA: Certification Authority, es español Autoridad de Certificación (AC)

ECPA: Electronic Communications Privacy Act

LFE: Ley de Firma Electrónica

MH: Ministerio de Hacienda

MINEC: Ministerio de Economía

PKI: Public Key Infrastructure, en español Infraestructura de Clave Pública

PSC: Proveedor de Servicios de Certificación

Introducción

Le tecnología es la evolución de los sentidos, el ser humano es una especie que se adapta al cambio y busca la forma de hacer más fáciles las tareas y actividades que realiza de forma cotidiana, por ello de manera constante investiga y desarrolla herramientas que le ayudan a la automatización. Como parte de esto, la eliminación del papel y la sustitución de la firma autógrafa por mecanismos electrónicos está marcando una clara tendencia en el siglo XXI, principalmente posterior a la pandemia por COVID-19, donde el uso de la firma electrónica cobro mayor realce.

Sin embargo, pese a este crecimiento causado por la pandemia y por la Ley de Firma Electrónica vigente en El Salvador desde el año 2015, aún se encuentran oportunidades de mejora para diversificar el uso de la firma electrónica en el país, en ofrecer soluciones que ayuden a automatizar procedimientos de organizaciones públicas y privadas.

Por ello, con la presente investigación se analizan aspectos y elementos claves que merecen ser revisados por los tomadores de decisiones, los cuales pueden contribuir en áreas en particular, donde el uso de la firma electrónica pueda agregar valor en diversos procesos, como por ejemplo cómo se gestiona la identidad de las personas, los tramites que se realizan en el sistema bancario, las solitudes de gestiones administrativas en oficinas del sector público, los pagos de impuestos, los accesos a los servicios médicos, de educación y una cantidad de registros públicos que actualmente son llevados de forma manual y no centralizada, los cuales con una gestión centralizada de firma electrónica autorizada se podrían realizar de una forma oportuna y reduciendo los tiempos de respuesta y los costos asociados a ellos.

Objetivos

Objetivo general

- Elaborar un documento que contenga los avances y retos de la Ley de Firma Electrónica en El Salvador y de todo el potencial que esta representa en la automatización de procesos a nivel de las organizaciones, para brindar la misma validez civil o legal de una firma manuscrita que es utilizada para dar consentimiento o aprobación en un documento.

Objetivos específicos

- Definir conceptos claves de la Firma Electrónica y los diferentes servicios asociados a ella.

- Documentar casos de éxitos de implementación de la Firma Electrónica en El Salvador.

- Proponer mejoras a la Ley de Firma Electrónica, para potenciar su uso y productividad en las organizaciones.

- Exponer los principales factores del poco avance en El Salvador sobre el uso de la Firma Electrónica.

- Proponer mecanismos que promuevan el uso y adopción de la Firma Electrónica.

Capítulo I: Antecedentes y conceptos de Firma Electrónica

1.1 Breve historia de la firma electrónica

La firma electrónica tiene sus antecedentes en la década de 1970, cuando surgieron las primeras tecnologías de criptografía y se desarrollaron los protocolos de red para la transmisión de información digital. Pero fue en la década de 1990 cuando comenzaron a surgir las primeras leyes y regulaciones para el uso de la firma electrónica.

En 1988, se promulgó el Electronic Communications Privacy Act (ECPA) en los Estados Unidos, que estableció que los mensajes electrónicos eran equivalentes a los mensajes en papel. Esta ley permitió el uso de la firma electrónica en contratos y acuerdos legales.

En 1996, la Unión Europea adoptó la Directiva 1999/93/CE sobre firma electrónica, cuya finalidad es facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico.

El 30 de junio del año 2000 se promulgó en Estados Unidos la Ley de Firmas Electrónicas en el Comercio Global y Nacional (E-Sign Act, Public Law EEUU, 106–229, 2000), para facilitar el uso de las firmas electrónicas en el comercio interestatal e internacional. La E-Sign Act establece la validez legal de las firmas electrónicas, los contratos y los registros electrónicos en situaciones donde una ley exige una firma, un contrato o un registro por escrito.

De acuerdo con la E-Sign Act, las firmas electrónicas tienen el mismo valor legal que las firmas manuscritas, y los contratos y registros electrónicos se consideran legalmente ejecutables si cumplen ciertos requisitos, los cuales incluyen:

- Las partes deben haber acordado llevar a cabo la transacción electrónicamente.
- La firma electrónica debe ser atribuible a la persona que la firma.
- La firma electrónica debe ser verificable.
- El registro electrónico debe ser capaz de retenerse y reproducirse con exactitud.

La E-Sign Act también establece un marco para la retención de registros electrónicos y requiere que los registros electrónicos se retengan durante el mismo período de tiempo que los registros en papel. La E-Sign Act ha tenido un impacto significativo en la forma en que se realiza el comercio y los negocios en los Estados Unidos y ha creado el camino para la adopción generalizada de las transacciones y la firma electrónica en todo el mundo.

Desde entonces, han surgido numerosas tecnologías y estándares para la implementación de la firma electrónica, como el Estándar de Firma Electrónica Avanzada (XAdES) y el Protocolo de Firma Electrónica (PAdES). En muchos países, la firma

electrónica es ampliamente utilizada en transacciones financieras, contratos legales y comunicaciones gubernamentales, entre otros ámbitos.

En El Salvador, la Asamblea Legislativa aprobó el día 1 de octubre de 2015 el Decreto Legislativo No. 133 que contiene la Ley de Firma Electrónica, el cual fue publicado en el Diario Oficial N° 196 el 26 de octubre de 2015. Esta ley busca brindar seguridad a los usuarios de las comunicaciones electrónicas y en las transacciones autorizadas mediante las aplicaciones de la tecnología o la suscripción electrónica de las mismas, brindando validez jurídica a tales transacciones. Adicionalmente, la ley busca responder al desarrollo de las tecnologías de información y comunicación.

El objeto de la ley es equiparar la firma electrónica simple y firma electrónica certificada con la firma autógrafa. Así también, otorgar y reconocer eficacia y valor jurídico a la firma electrónica certificada y otra información en formato electrónico que se hubiere suscrito con la firma electrónica certificada. La ley, además regula lo pertinente a los Proveedores de Servicios de Certificación Electrónica y de Servicios de Almacenamiento de Documentos Electrónicos, los cuales pueden ser terceros nacionales o extranjeros que estén interesados en vender servicios a personas naturales o jurídicas en el país.

En El Salvador, de acuerdo con la Ley de Firma Electrónica se reconocen 2 tipos firmas (Asamblea Legislativa, 2015-2021):

- **Firma Electrónica Simple:** Son datos en forma electrónica, consignados en un mensaje de datos o documento electrónico, lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante por cualquier medio tecnológico disponible, e indicar que el firmante aprueba la información recogida en el mensaje de datos o documento electrónico.
- **Firma Electrónica Certificada:** Son los datos en forma electrónica, consignados en un mensaje de datos o documento electrónico, lógicamente asociados al mismo, que son generados mediante un dispositivo seguro de creación y permiten vincular de manera exclusiva, la firma con su titular.

1.2 Conceptos relacionados a la firma electrónica

La firma electrónica es una herramienta que permite verificar la identidad de una persona y la autenticidad de un documento o mensaje en el entorno digital. Es utilizada para garantizar la integridad y la no repudiación de la información transmitida. En el presente apartado se mencionan los principales conceptos relacionados a la firma electrónica, los cuales han sido tomados principalmente de la Ley de Firma Electrónica de El Salvador.

- **Firma digital:** consiste en una implementación técnica específica de algunas firmas electrónicas mediante la aplicación de algoritmos criptográficos. Las firmas

digitales, por otro lado, se pueden verificar utilizando un algoritmo de verificación conocido públicamente.

- **Firma biométrica:** es una firma electrónica que se realiza mediante un dispositivo que captura y almacena información biométrica del firmante, como la firma manuscrita, la huella dactilar o la voz.
- **Entidad certificadora:** es una organización que emite certificados digitales y garantiza la autenticidad de estos.
- **Infraestructura de Clave Pública (PKI, por sus siglas en inglés):** es un conjunto de sistemas, protocolos y estándares que permiten la generación, distribución y verificación de claves públicas y certificados digitales necesarios para la firma electrónica y otros servicios de seguridad informática. La PKI se basa en la utilización de claves públicas y privadas, que son generadas por algoritmos de cifrado asimétricos. Las claves públicas se pueden compartir libremente, mientras que las claves privadas se mantienen en secreto. Los certificados digitales se utilizan para vincular una clave pública a una entidad, como una persona, una organización o un sitio web.
- **Sello de tiempo:** Es un servicio de confianza que permite asociar una marca de tiempo a un documento electrónico, garantizando la fecha y hora de su creación, modificación o recepción.
- **Autoridades de Certificación (CA, por sus siglas en inglés):** son entidades responsables de emitir y revocar certificados digitales en una Infraestructura de Clave Pública (PKI). Las CA son confiables porque se consideran una fuente fiable de información sobre los titulares de los certificados. Las CA emiten certificados digitales después de verificar la identidad del titular y garantizar que la clave pública en el certificado pertenece al titular.
- **Acreditación:** es la autorización que otorga la autoridad competente establecida a los proveedores de servicios de certificación, para operar y proporcionar certificados electrónicos, y a los proveedores de servicios de almacenamiento de documentos electrónicos, una vez cumplidos los requisitos y condiciones establecidos.
- **Certificado Electrónico:** documento proporcionado por un proveedor de servicios de certificación que otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con dicha firma (Asamblea Legislativa, 2015-2021, pág. 3).
- **Firma Autógrafa:** marca o signo, que una persona escribe de su propia mano en un instrumento o documento para asegurar o autenticar la identidad de una persona como prueba del consentimiento y verificación de la información contenida en dicho instrumento (Asamblea Legislativa, 2015-2021, pág. 3).

- **hash:** es una función matemática que convierte un conjunto de datos en una cadena de caracteres de longitud fija, utilizada en criptografía para garantizar la integridad de los datos.
- **Criptografía:** es el conjunto de técnicas y métodos utilizados para proteger la confidencialidad, autenticidad e integridad de los datos y las comunicaciones electrónicas.
- **Firmante:** la persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona que representa (Asamblea Legislativa, 2015-2021, pág. 3).
- **Proveedor de Servicios de Certificación:** persona jurídica autorizada por la autoridad competente, dedicada a emitir certificados electrónicos y demás actividades previstas en esta Ley de Firma Electrónica (Ley de Firma Electrónica, 2015, p.3).
- **Proveedor de Servicios de Almacenamiento de Documentos Electrónicos:** persona jurídica autorizada por la autoridad competente que, por la naturaleza de su negocio, brinda servicios de almacenamiento de documentos electrónicos (Ley de Firma Electrónica, 2015, p.3).
- **Signatario:** persona que posee un dispositivo de creación de firma electrónica certificada y que actúa en nombre propio o a nombre de una persona natural o jurídica que representa. (Ley de Firma Electrónica, 2015, p.4).

1.3 Diferencia entre firma digital y firma electrónica

La firma electrónica y la firma digital generalmente son usados para referirse a lo mismo, pero técnica tienen significado distintos, la firma electrónica es un concepto más amplio y se refiere a cualquier método que se utiliza para firmar documentos electrónicos; ya que el fin principal es identificar la fuente del documento y su autor, pero no ofrece garantías de seguridad para validar la integridad y manipulación del documento, puede estar representada por medio de imagen de una firma manuscrita escaneada o una marca o código generado por una computadora, que tiene por fin identificar al firmante e indicar la intención de aceptar el contenido del documento, mas no ofrece el mecanismo para validar dicha forma.

En cambio, la firma digital su fin es proteger un documento y evitar que sea modificado, y en caso de que así sea poder evidenciarlo, ya que contiene una serie de mecanismos de seguridad, los cuales proporcionan integridad y autenticidad. Una firma digital es verificable, debido que está autorizada por un tercero de confianza conocido como autoridad de certificación.

En resumen, la principal diferencia entre la firma electrónica y la firma digital es que la firma electrónica es un término más general que puede incluir cualquier tipo de marca o código que se utiliza para identificar al firmante y su intención, mientras que la firma digital es un tipo específico de firma electrónica que utiliza criptografía para garantizar la autenticidad, la integridad y la no repudiación de un documento.

1.4 Características que debe poseer la firma electrónica

De acuerdo con el proveedor de servicios de firma electrónica Docusing, se distingue la firma electrónica ya que cumple con los siguientes requisitos para ser considerada válida y confiable:

1. **Integridad:** utiliza medios tecnológicos para determinar si el contenido del mensaje de datos ha sido alterado.
2. **Autenticidad:** se puede comprobar la identidad del firmante y garantizar la fiabilidad de esta.
3. **Confidencialidad:** solo el firmante está autorizado para descifrar el contenido de un documento.
4. **No repudio:** el emisor no puede negar la autoría del contenido firmado.
5. **Funcionalidad:** satisface el requisito de la firma autógrafa y pertenece exclusivamente al firmante

Estas características son esenciales para garantizar la autenticidad y la integridad de los documentos electrónicos y asegurar la confianza en las transacciones electrónicas. Las regulaciones y estándares internacionales establecen los requisitos específicos para las firmas electrónicas y los procedimientos para su implementación y verificación.

1.5 PKI como servicio

Llamado Public Key Infrastructure (PKI) as a Service, o PKI as-a-Service (PKIaaS), consiste en una solución que es ofrecida por un tercero que se encarga de gestionar la Infraestructura de Clave Pública de una organización, de esta forma no es necesario implementar y mantener una infraestructura propia de PKI, para lo cual se buscan proveedores que se encargan de administrar y proteger los certificados digitales que se poseen.

Entre las principales funciones que puede proporcionar un proveedor de PKI como servicio están: la emisión y revocación de certificados, la gestión de claves públicas y privadas, la autenticación de usuarios y dispositivos y la protección contra amenazas de seguridad.

La principal ventaja de utilizar un servicio de PKI es que permite a las organizaciones centrarse en su negocio principal en lugar de dedicar recursos y tiempo a gestionar una infraestructura de seguridad compleja. Asimismo, los proveedores de PKI como servicio suelen tener una amplia experiencia en la gestión de certificados digitales y en la protección de la seguridad en línea, lo que les permite ofrecer soluciones robustas y eficaces.

Es importante aclarar que la utilización de un servicio de PKI implica ceder el control de los certificados digitales a un tercero, lo que puede presentar inconvenientes de privacidad y seguridad. Por lo que es necesario asegurar que, para la contratación de un proveedor de este tipo, cuente con las certificaciones necesarias, lo cual brinde las garantías necesarias de acuerdo con legislaciones locales, internacionales y las mejores prácticas de seguridad de la información.

PKI como servicio es una nueva modalidad que ofrecen diversos proveedores internacionales, entre los cuales podemos mencionar: Entrust, Uanataca, GlobalSign y Digicert. De acuerdo con Entrust las ventajas de una PKI como servicios son:

- Escalabilidad: los sistemas en la nube crecen bajo demanda con una capacidad casi ilimitada.
- Velocidad: se despliega en minutos para proteger sus casos de uso empresarial.
- Sencillez: proveedor administra la PKI para que pueda el cliente centrarse en otras necesidades comerciales.
- Seguridad: CA dedicadas con sus claves protegidas en centros de datos seguros.

Entre los casos de uso habituales de la PKI o infraestructura de clave pública, podemos mencionar:

- Certificados de servidor SSL: se utiliza un certificado PKI en el servidor para aportar seguridad y confianza al cliente cuando visita una página web.
- Autenticación: la autenticación se utiliza en cualquier aplicación en la que sea necesario saber con seguridad la identidad del usuario y que el usuario es realmente el que está presente. Por lo general, la autenticación se realizaba mediante un nombre de usuario y una contraseña, pero la tecnología PKI aporta un nivel de seguridad mayor puesto que la identidad del usuario se acredita mediante una clave privada.
- Firma digital: la firma digital es el equivalente electrónico a firmar un documento con papel y bolígrafo. Sin embargo, la firma electrónica asocia el contenido concreto del documento con la firma de manera que se puede detectar cualquier manipulación de dicho contenido después de haberse firmado, lo que aporta una gran seguridad. En este caso, el usuario también posee una clave privada para poder firmar.

- Cifrado: por ejemplo, se utilizan en el caso de los correos electrónicos o de la mensajería instantánea, de forma que el usuario que recibe los datos es el único que puede descifrarlos.

1.6 Sistema de encriptación simétrica

Comúnmente llamado sistema de clave compartida es aquel en donde el emisor como el destinatario de un mensaje de datos, hacen uso de la misma clave para encriptar y desencriptar el mensaje, por lo tanto, constituye un procedimiento más sencillo de cifrado por que usan la misma clave para cifrar como para descifrar la información. Este sistema es ideal para brindar un estándar de seguridad en el que las partes involucradas se conocen previamente, por lo que su relación está basada en el principio de la confianza mutua. Pero debido que la mayoría de las comunicaciones ocurren en Internet, esto hace que las partes no siempre se conozcan, o mejor aún no deban conocerse por lo que este tipo encriptación no siempre es la mejor solución.

Dentro de los algoritmos de cifrado simétrico se ha desarrollado a lo largo del tiempo el conocido algoritmo de cifrados DES el cual es un algoritmo simétrico que utiliza bloques de 64 bits de datos y una clave secreta de 56 bits. (Stinson, 2006, págs. 100,101).

Cabe destacar que este algoritmo desarrollado por IBM en los años 70´s es muy efectivo para poder proteger la privacidad de los datos; su peculiaridad de ser muy simple y rápido siendo que el remitente y el destinatario usan la misma clave, termina dejando una brecha de seguridad. Pero a pesar de esto aún se puede recomendar para poder proteger datos en reposo. Posee algunas debilidades conocidas como que la clave de 56 bits es vulnerable a los ataques de fuerza bruta y a los ataques de criptoanálisis diferencial y lineal.

En base a estas debilidades mencionadas, se ha visto que este sistema ha sido reemplazado en una buena parte por algoritmos aún más avanzados como el AES (Advanced Encryption Standard) y también RSA (Rivest, Shamir y Adleman).

El cifrado simétrico, también conocido como cifrado convencional o cifrado de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a fines de la década de 1970. Innumerables personas y grupos, desde Julio César hasta la fuerza alemana de submarinos y los usuarios comerciales, militares y diplomáticos actuales, han utilizado el cifrado simétrico para la comunicación secreta. Sigue siendo el más utilizado de los dos tipos de cifrado. (Brown, 2015, pág. 42).

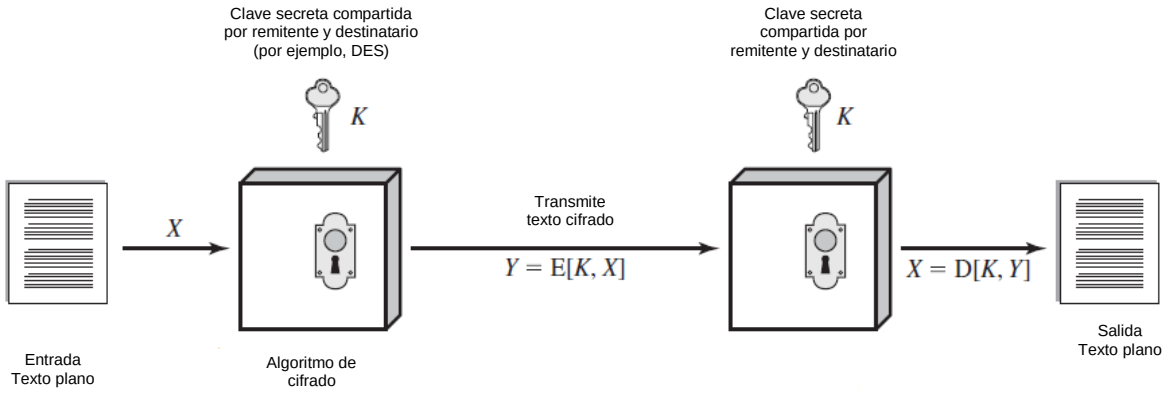

Fig. 1 Modelo simplificado de cifrado simétrico

Funcionamiento del cifrado simétrico (Fig. 1)

- Texto plano (entrada): este es el mensaje original o los datos que se introducen en el algoritmo como entrada.
- Algoritmo de cifrado: el algoritmo de cifrado realiza varias sustituciones y transformaciones en el texto plano.
- Clave secreta: la clave secreta también se ingresa en el algoritmo de cifrado. Las sustituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave.
- Texto cifrado: este es el mensaje codificado producido como salida. Depende del texto plano y de la clave secreta. Para un mensaje dado, dos claves diferentes producirán dos textos cifrados diferentes.
- Algoritmo de descifrado: este es esencialmente el algoritmo de descifrado ejecutado a la inversa.
- Toma el texto cifrado y la clave secreta y produce el texto original (texto plano).

1.7 Sistema de encriptación asimétrica

También llamado Sistema de Clave Pública, en el cual se utilizan dos tipos de claves: una pública (de libre acceso), que es la encargada de encriptar el mensaje y una privada que únicamente conoce el usuario al que pertenece, la cual se debe proteger y tiene como finalidad desencriptar el mensaje. Este sistema utiliza un método donde las dos claves solo se pueden generar una sola vez, y es imposible que dos personas obtengan la misma pareja de claves, siendo de esta forma un mecanismo donde se asegura que los mensajes no han sido alterados.

El concepto de la criptografía asimétrica nació en 1975, por lo que este ámbito se considera muy joven, teniendo en cuenta que la historia de la criptografía se remonta a más de 2000 años. La mayor ventaja de la criptografía de clave pública es, al mismo tiempo, el mayor inconveniente del cifrado simétrico: las partes que se comunican no tienen que compartir una sola clave común, sino que cada una posee una clave privada distinta.

La base de la seguridad de los sistemas de encriptación asimétrica está en la factorización de números enteros, puesto que en esto y otras medidas más radica la seguridad de los sistemas utilizados de manera asimétrica.

Uno de los más famosos sistemas dentro de la criptografía asimétrica es el RSA (Rivest-Shamir-Adleman) el cual es un algoritmo de cifrado desarrollado desde 1977 y que tiene como finalidad proteger la privacidad y autenticidad de los datos. El algoritmo RSA es seguro debido a la dificultad de factorizar el número entero grande n en sus dos factores primos diferentes. Un atacante que conozca la clave pública podría tratar de factorizar n para obtener las claves privadas, pero esta tarea se vuelve muy difícil a medida que el tamaño de n se hace más grande (Stinson, 2006, pág. 161).

El descifrado de RSA es mucho más lento que otros métodos, ya que requiere de más capacidad de procesamiento que otros tipos de algoritmos. Aunque el cifrado de un mensaje amplio es posible, se suele utilizar para contraseñas relativamente cortas y cifrar con algoritmos simétricos mensajes más largos. RSA suele usarse para transmitir claves compartidas de criptografía simétrica. Este algoritmo RSA se utiliza para proteger la privacidad de los datos en muchas aplicaciones, como el cifrado de correo electrónico, la autenticación en línea y la protección de la información de pago en línea.

Se utiliza una representación numérica para los mensajes enviados, y el funcionamiento utiliza el producto conocido de dos números primos grandes elegidos aleatoriamente y que se mantienen en secreto en todo momento. Actualmente, estos primos son del orden de 10^{200}, y sigue aumentando debido al constante crecimiento en la capacidad de cálculo actual de los ordenadores.

Esquema de cifrado de RSA

RSA consiste en los siguientes tres algoritmos:

1. Generación de llaves
   Seleccionar dos números primos grandes p y q
   $n = p * q$
   $\Phi(n) = (p - 1) * (q - 1)$

   Seleccionar un exponente público e tal que $e < n$ y

   $mcd(e, \Phi(n)) = 1$

   $d = e^{-1} \bmod \Phi(n)$

Llave pública (e, n), llave privada (d, n)

2. Cifrado para el mensaje m

   $c = m^e \bmod n$

3. Descifrado para el mensaje cifrado c
   $c^d = (m^e)^d = m^{ed} = m \bmod n$

Funcionamiento y propósito del algoritmo de cifrado asimétrico Diffie-Hellman (Brown, 2015, pág. 685)

El propósito del algoritmo es permitir que dos usuarios intercambien una clave secreta de forma segura que luego se puede usar para el cifrado posterior de mensajes. El algoritmo en sí está limitado al intercambio de claves.

El algoritmo de Diffie-Hellman depende para su eficacia de la dificultad de calcular logaritmos discretos. Brevemente, podemos definir el logaritmo discreto de la siguiente manera. Primero, definimos una raíz primitiva de un número primo p como uno cuyas potencias generan todos los números enteros de 1 a p – 1. Es decir, si a es una raíz primitiva del número primo p, entonces los números

$$a \bmod p,\ a^2 \bmod p,\ c,\ a^{p-1} \bmod p$$

son distintos y consisten en los números enteros del 1 al p - 1 en alguna permutación. Para cualquier entero b menor que p y una raíz primitiva a del número primo p, se puede encontrar un exponente único i tal que

$$b = a^i \bmod p \quad \text{donde } 0 \leq i \leq (p - 1)$$

El exponente i se conoce como el logaritmo discreto, o índice, de b para la base a, mod p. Denotamos este valor como $\text{dlog}_{a,p}(b)$.[2]

1.8 Usos de la firma electrónica en la región

En la región el uso de la firma electrónica tiene diversas aplicaciones. En la tabla 1 se listan los principales casos.

Tabla 1 Principales uso de aplicación de la firma electrónica en la región

País	Principales usos
México	Firmar digitalmente las facturas electrónicas del Servicio de Administración Tributaria (SAT).
Costa Rica	Internet Banking, Autenticación en web, firma de transacciones, tributación digital, cheque electrónico, firma de textos a ser publicados.
Colombia	Formalización de pólizas de seguro y demás documentación relacionada con su asegurado.
República Dominicana	Firma de contratos de servicios de telecomunicaciones, firmar contratos de compraventa de facturas (factoring).
Paraguay	Facturación electrónica: emitir electrónicamente sus Comprobantes de Ventas y Documentos Complementarios, Comprobantes de Retención y Notas de Remisión en los años 2023 y 2024.
El Salvador	Factura electrónica del Ministerio de Hacienda.

Fuente: Elaboración propia, tomando casos de éxitos en implementación de firma electrónica en la región.

.

Capítulo II: Casos de éxito de implementación de Firma Electrónica en El Salvador

2.1 Caso I: Ministerio de Hacienda - Factura Electrónica

El 7 de diciembre de 2016, por medio de un comunicado de prensa el Banco Interamericano de Desarrollo (BID) anunció la asignación de un préstamo de $30 millones de dólares que brindó a El Salvador, para aumentar la eficiencia de la presentación de las declaraciones de impuestos y la utilización de facturas aduaneras de manera electrónica. Con lo cual se espera aumentar la recaudación tributaria en al menos 1 por ciento del PIB en 5 años (BID, Comunicados de presa, 2016).

En el año 2018 el Ministerio de Hacienda (MH) inicio con el plan piloto diseñado para un grupo de seis empresas salvadoreñas entre ellas: un supermercado, una aerolínea, dos bancos y una empresa gasera que han sido las primeras en emitir y recibir factura electrónica. De acuerdo con el MH, se implementará progresivamente la factura electrónica a partir de enero de 2019 (Grupo Seres, 2018).

De acuerdo con el artículo Tax Newsletter de la consultora Deloitte, el MH estuvo preparando el desarrollo tecnológico para la implementación de facturación electrónica y, durante el mes de abril de 2021, se inició un plan piloto con la autorización del primer emisor de facturación electrónica, en el cual participaron alrededor de 50 contribuyentes y según los comentarios de los encargados del programa, el resultado fue exitoso (Jhonny Flores, 2022).

En el ambiente de facturación electrónica se utilizan DTE (Documentos Tributarios Electrónicos), los cuales son archivos electrónicos generados por el emisor y transmitidos al MH para su recepción y almacenamiento (Salvador, 2022).

Los DTE implementados a la fecha son los siguientes:

a) Factura
   Nota de contabilidad que se entrega al comprador de bienes o servicios. Se detalla, según número, peso, medida, clase o calidad y precio de los artículos o servicios de una operación mercantil.
b) Factura de exportación
   Son utilizados para comprobar documentalmente que una mercancía califica como originaria.
c) Comprobante de liquidación
   Es un comprobante de carácter tributario emitido por la entidad financiera que presta el servicio de POS a compañías que utilizan métodos cobro a clientes por medio de tarjetas ya sea de crédito ó débito.

d) Comprobante de retención
   Son los documentos que acreditan las retenciones de impuestos realizadas por los agentes de retención en cumplimiento de lo dispuesto en la Ley de Régimen Tributario Interno.
e) Comprobante de Crédito Fiscal
   Son documentos mercantiles, cuya función es reflejar la información sobre la transferencia de bienes o servicios y la entrega o prestación de estos.
f) Documento Contable de Liquidación
   Es un comprobante de carácter tributario emitido por la entidad financiera que presta el servicio de POS a compañías que utilizan métodos cobro a clientes por medio de tarjetas ya sea de crédito ó débito.
g) Nota de remisión
   Es un documento provisional que simboliza la remisión, entrega u orden de servicio que respalda la venta y entrega de un servicio o producto a un cliente, al momento de realizar una transacción
h) Nota de Débito
   Es un documento contable a través del cual un vendedor notifica al cliente del aumento en el monto de su deuda por un concepto que se especifica en la misma nota
i) Nota de Crédito
   Son Títulos emitidos por el Ministerio de Hacienda, por medio de la Dirección General de Tesorería, para devolver a los contribuyentes impuestos pagados en exceso determinados en las resoluciones emitidas por las instituciones administradoras de impuestos.

Proceso de emisión de factura electrónica

El proceso que realiza el sistema de facturación electrónica de forma general según (Asamblea Legislativa, 2015-2021) adicional como complemento de los conceptos que también tomados del manual de facturación electrónica del Ministerio de Hacienda

a) Obtención del certificado de firma electrónica simple
   Este es otorgado por el Ministerio de Hacienda y determina las características informáticas, lógicas y de forma que cada campo y documento deben cumplir.
b) Implementación del certificado en su desarrollo de facturación electrónica
   El Ministerio de Hacienda valida y otorga Sello de Recepción previo a entregar al cliente.
c) Generación y firmado de archivo JSON
   En este se implementa el certificado de la facturación electrónica.
   Envío del archivo firmado a DGII para su validación de autenticidad.
   La dirección coloca como valida la autenticidad del archivo para su uso.

El miércoles 14 de diciembre 2022, el MH lanzó el Sistema de Facturación Electrónica, en el marco del Proyecto para el Fortalecimiento de la Administración Tributaria y Aduanera, financiado por el Banco Interamericano de Desarrollo (BID) por $30 millones de los cuales, $6.3 millones corresponden a dicho proyecto. “Este proyecto había estado tirado, desde junio de 2019, trabajamos arduamente para cumplir con la implementación de la Facturación Electrónica, gracias al apoyo de nuestro socio el BID, hoy estamos realizando este lanzamiento”, expresó el Ministro de Hacienda, Alejandro Zelaya, con la puesta en marcha de esta herramienta, se fortalecen las herramientas con equipo tecnológico de última generación, para una gestión más eficaz, mejorando el cruce de información y los procesos de fiscalización de la Administración Tributaria, asimismo se brinda un sistema amigable y accesible 24/7 para grandes y pequeñas empresas (Ministerio de Hacienda, 2022). Además, facilitará a todas las empresas el cumplimiento de sus obligaciones tributarias, reduciendo costos de autorización, emisión y almacenaje de documentos físicos, Se hace énfasis en que no se están creando nuevos documentos, sino mudando la estructura de ellos a un sistema electrónico funcional que cuenta con el mismo respaldo legal que los documentos físicos, con miras a un gobierno digital y una ciudadanía conectada; este proyecto busca fortalecer a la Administración Tributaria, con la implementación de estas estrategias seguiremos mejorando la recaudación fiscal (Ministerio de Hacienda, 2022).

La facturación electrónica forma parte de la de la Modernización del Estado, lo cual se encuentra plasmado en la Agenda Digital 2020-2030 que impulsa la Secretaría de Innovación de la Presidencia, como parte de la desmaterialización de documentos con la cual se busca poder ser competitivo en la región y hacer un uso de las tecnologías disponibles al momento.

El Código Tributario de El Salvador tuvo algunas reformas a partir de 2009, en las que se incorporó la posibilidad de emitir facturas electrónicas. "La administración tributaria podrá autorizar el uso electrónico de los documentos, siempre que los sistemas computacionales del contribuyente aseguren el cumplimiento y veracidad de los impuestos que se causen", (Código Tributario de El Salvador, pág. 44) Artículo 113, inciso 2º, que hace alusión a la emisión de documentos, normados entre los artículos 107 al 119. Facilitará a todas las empresas el cumplimiento de sus obligaciones tributarias, reduciendo costos de autorización, emisión y almacenaje de documentos físicos. Se hace énfasis en que no se están creando nuevos documentos, sino mudando la estructura de ellos a un sistema electrónico funcional que cuenta con el mismo respaldo legal que los documentos físicos, con miras a un gobierno digital y una ciudadanía conectada; Este proyecto busca fortalecer a la Administración Tributaria, con la implementación de estas estrategias seguiremos mejorando la recaudación fiscal.

Los requisitos mínimos que deben llevar los documentos legales que amparan las transacciones u operaciones para el control del impuesto a la transferencia de bienes

muebles y la prestación de servicios con el objeto de llevar un mejor control y garantizar el interés fiscal y su solo establece la sección Quinta del Código Tributario. “Los contribuyentes del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios están obligados a emitir y entregar, por cada operación, a otros contribuyentes un documento que, para los efectos de este Código, se denominará "Comprobante de Crédito Fiscal" que podrá ser emitido en forma manual, mecánica o computarizada. Cuando se trate de operaciones realizadas con consumidores finales, deberán emitir y entregar, por cada operación, un documento que se denominará "Factura", la que podrá ser sustituida por otros documentos o comprobantes equivalentes, autorizados por la Administración Tributaria” (Art 107).

El reglamento de aplicación del Código Tributario indica que “Los contribuyentes del impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, para soportar las transferencias de bienes, prestación de servicios y exportaciones, únicamente deben emitir y entregar los documentos que estable el Código Tributario; en tal sentido, no será válido el uso de cualquier otro documento para soportar dichas operaciones.” (Reglamento de Aplicación del Código Tributario). Art. 36.

2.2 Caso II: Apostilla Electrónica del Ministerio de Relaciones Exteriores

Otro caso de éxito a destacar es la creación e implementación de la Ley de Aplicación de la Apostilla Electrónica, la cual fue aprobada el 18 de enero de 2022 por la Asamblea Legislativa de El Salvador, el propósito es permitir la legalización de documentos públicos generados, digitalizados o reproducidos en soporte electrónico y eliminar procesos burocráticos a los que se enfrentan los salvadoreños que residen en el exterior, al momento de autenticar o certificar documentos de su interés.

De acuerdo con lo expresado por la diputada Ana Figueroa, presidenta de la Comisión de Relaciones Exteriores (Asamblea Legislativa, 2022) “El gobierno central busca la modernización de los servicios que se prestan a la población salvadoreña, con herramientas tecnológicas”. El servicio de apostilla electrónica está diseñado como parte de la automatización de los servicios del Estado y buscar acercar los servicios a la población salvadoreña, principalmente a la diáspora que tanta demanda de servicios de este tipo.

La protección de datos, eficiencia y simplificación de trámites es parte de lo que se busca con el lanzamiento oficial de la plataforma digital Simple SV con la cual facilita la ejecución de trámites gubernamentales ciudadanos y empresariales de forma accesible y simplificada.

Con esta nueva plataforma se evitará la duplicación de datos y se mejorará la coordinación de servicios públicos, sin necesidad de crear un usuario para acceder a trámites gubernamentales, utilizando solo una Identidad Digital Única, afirmaron las autoridades de El Salvador.

Uso y funcionamiento del sistema SIMPLE

Ingresa a la página digital Simple SV y regístrate con tu número de Documento Único de Identidad (DUI) y así obtiene tu Identidad Digital. La plataforma cuenta con las garantías de seguridad para la protección de los datos personales y para las autoridades salvadoreñas es un sitio 100% rápido, seguro y simple. En el sitio se pueden realizar pagos en línea y se tiene acceso a portales virtuales.

En esta plataforma los salvadoreños, tanto a nivel nacional como desde el exterior pueden realizar diversos trámites en línea como:

- Solvencia de antecedentes policiales
  Constancia legal que se emite a un(a) salvadoreño(a) al carecer de registro de antecedentes policiales para presentarla en diferentes instancias.

- Solvencia de antecedentes penales
  Esta constancia de Antecedente Penal se extiende para comprobar que el ciudadano o extranjero posee o no Registros de Antecedentes Penales por sentencia condenatoria ejecutoriada en su contra por imputársele un delito.
- Cita para pasaporte de Migración
  Este trámite permite realizar el registro de manera fácil y segura para poder seleccionar fecha y hora para la obtención del pasaporte de El Salvador.
- Pasaporte COVID-19
  Certificado que se obtiene ingresando con numero de DUI y así descargar la tarjeta de vacunación contra el COVID-19.
- Apostillado electrónico
  Es una herramienta en la que el ciudadano podrá de manera electrónica validar de manera ágil y segura sus documentos y trámites que requieren de este reconocimiento internacional
- Certificación de DUI
  Hace constar mediante un documento certificado por el RNPN la información contenida en el Documento Único de Identidad de la persona de quien se solicita la información. O que dicha persona NO posee DUI asignado.
- Certificación de título de educación media.
  Es el documento oficial emitido por el Ministerio de Educación, Ciencia y Tecnología por medio del cual se hace constar que existe un registro oficial de Título de Bachiller de la República de El Salvador a favor de una persona, éste podrá ser solicitado en casos de extravío, destrucción o pérdida del título original.
- Autorización de agente marítimo
  Autoriza el registro de empresas de transporte internacional marítimo o agentes que actúen en su representación conocidas como agencias navieras.
- Datos topográficos para fines académicos con el Ministerio de Medio Ambiente y Recursos Naturales, entre otros.
  Puesta a disposición de planos topográficos y medidas certificadas por el CNR.

El servicio está disponible en línea1, en donde tanto funcionarios, ciudadanos y empresarios pueden hacer la solicitud para apostillar documentos como: partidas de nacimiento o defunción, títulos académicos, registros de matrimonio, resoluciones judiciales, entre otros. Para uso de la plataforma se dispone de un video tutorial[2].

[1] La dirección disponible es https://apostilla.rree.gob.sv/

[2] Para el video tutorial consultar la dirección: https://simple.sv/tramite/constancia-de-antecedentes-policiales/nacionales

Caso práctico de apostilla de documento en línea

Dentro de los primeros esfuerzos para poder implementar teniendo Protección de datos, eficiencia y simplificación de trámites se implementa una plataforma digital llamada Simple SV con la cual facilita la ejecución de trámites gubernamentales ciudadanos y empresariales de forma accesible y simplificada.

Con esta nueva plataforma se evitará la duplicación de datos y se mejorará la coordinación de servicios públicos.

La plataforma cuenta con las garantías de seguridad para la protección de los datos personales y para las autoridades salvadoreñas es un sitio 100% rápido, seguro y simple.

1. Ingresamos a la URL de Ventanilla Única para ingresar nuestros tramites.

Fig. 2 Pantalla Principal de simple sv

Dentro de estos trámites que podemos realizar en línea tenemos uno de los tramites más funcionales dentro de la plataforma y también con el presente estudio, como es el Apostillado Electrónico; el cual viene a innovar la forma de autenticar o certificar documentos oficiales.

Dicho procedimiento electrónico está apoyado en la Ley de Aplicación de la Apostilla Electrónica, con la que se eliminan todos los mecanismos burocráticos que debían pasar los compatriotas en el extranjero para poder legalizar documentos. (Legislativa, 2021)

El Ministerio de Relaciones Exteriores habilitó una dirección web[3] para que los compatriotas accedan para la autenticación de documentos como: partidas de nacimiento, matrimonio y defunción; constancias de soltería, certificados de notas globales y parciales, títulos de bachiller, certificados de título universitario, certificados de títulos técnicos, certificación de maestrías, solvencia de la PNC, antecedentes penales, certificación de pasaportes, renuncia a la nacionalidad, movimiento migratorio, carné de residencia y sentencia de recuperación de nacionalidad, entre otros.

Para poder realizar el proceso de apostilla seguimos los siguientes pasos.

2. Ingresamos a la URL https://apostilla.rree.gob.sv/ autorizada por el Ministerio de Relaciones Exteriores

Fig. 3 Pantalla de configuración de Apostilla

3. Validamos la nuestra cuenta para poder registrar nuestros tramites, de no tener una cuenta la creamos.

[3] La dirección habilitada es: https://apostilla.rree.gob.sv

Fig. 4 Ingreso y/o Creación de Usuario

4. Se valida con usuario y contraseña y sino, se nos da la opción de crearlo.

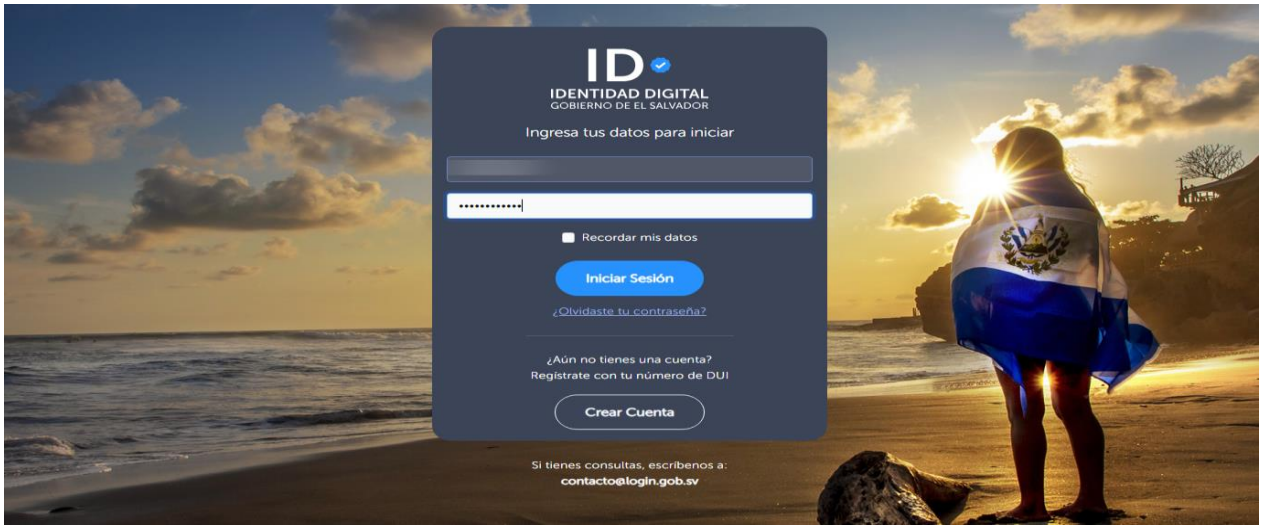

Fig. 5 Validación de usuario y contraseña si posee usuario

5. Si nuestra opción fue crear usuario entonces lo hacemos ingresando nuestros datos personales para dar paso a crear nuestros trámites.

Fig. 6 *Creación de Usuario en Sistema*

6. Ingresados en nuestro perfil del sistema SIMPLE SV damos paso a la generación del trámite que necesitamos apostillar.

Fig. 7 *Selección de nuevo trámite*

7. Trámites disponibles para poder solicitar de manera electrónica.

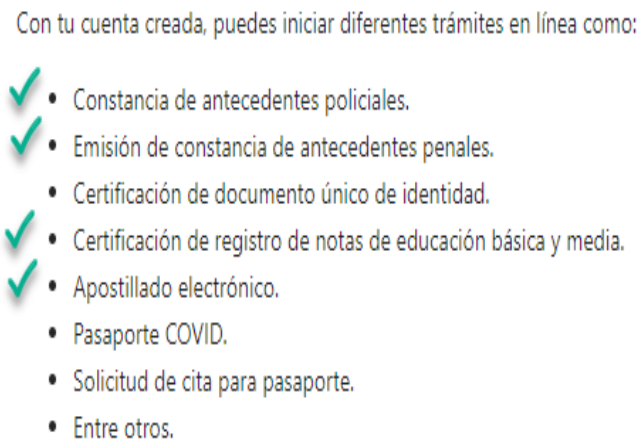

Fig. 8 *Trámites disponibles para apostilla.*

8. Cuando logramos identificar el trámite a apostillar lo seleccionamos para dar inicio.

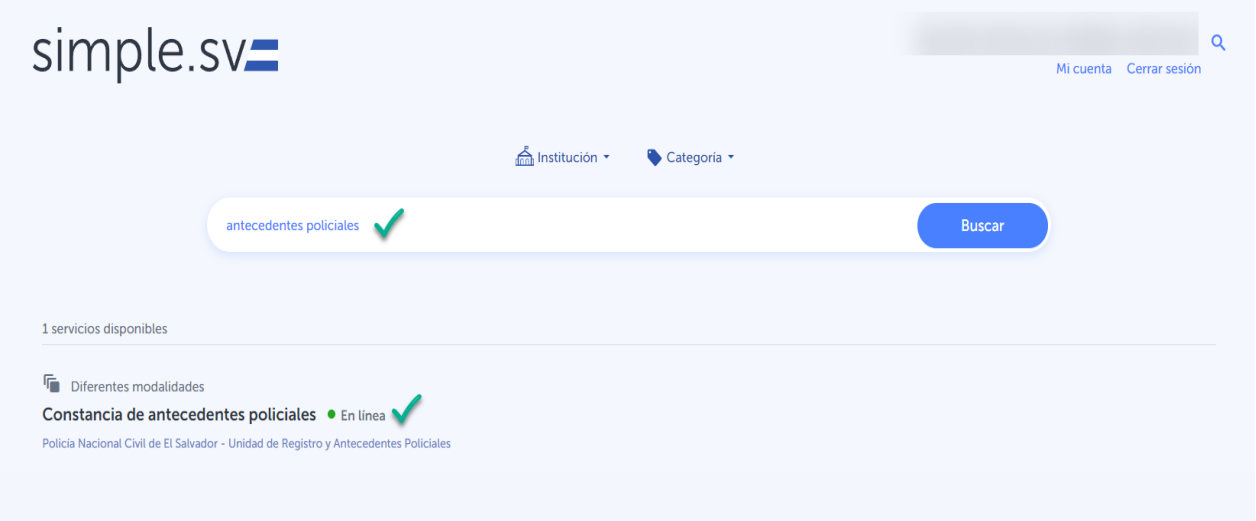

Fig. 9 *Nombre del documento digital a solicitar*

9. En esta parte obtenemos la informacion de la solicitud hecha incluyendo el costo del tramite.

Fig. 10 Características de Documento a solicitar

10. En este paso nos muestra el formulario para completar con nuestros datos personales y otros detalles de la solicitud.

Fig. 11 Formulario de solicitud de Documento (Antecedentes Policiales)

11. Una vez que hemos completado el formulario nos da paso a la confirmación de los datos recién ingresados, y nos advierte que no podrán ser modificados.

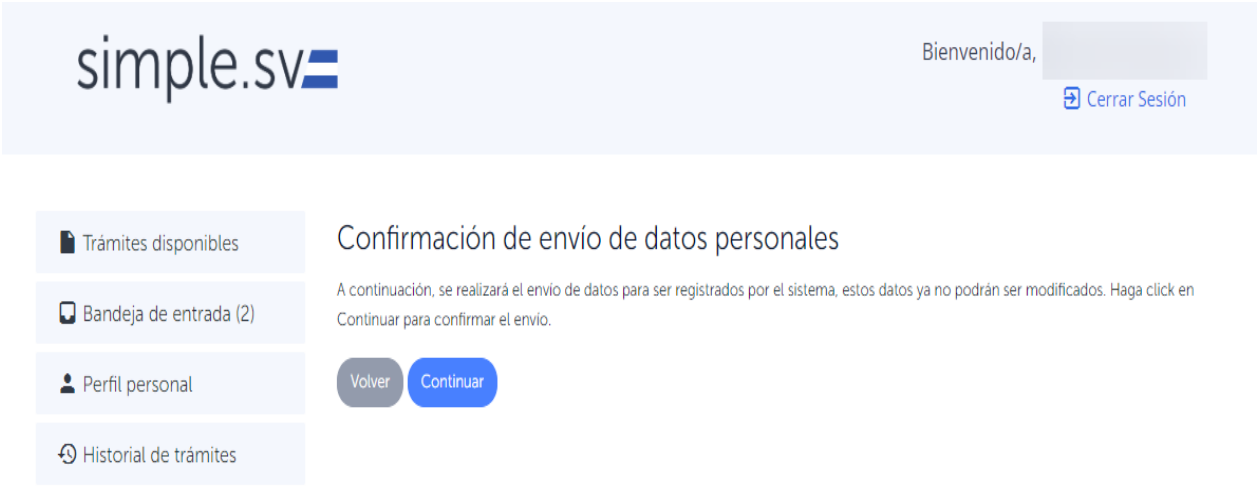

Fig. 12 *Formulario de confirmación de datos personales*

12. Nos muestra las formas de pago a través de tarjetas débito/crédito y el monto del trámite.

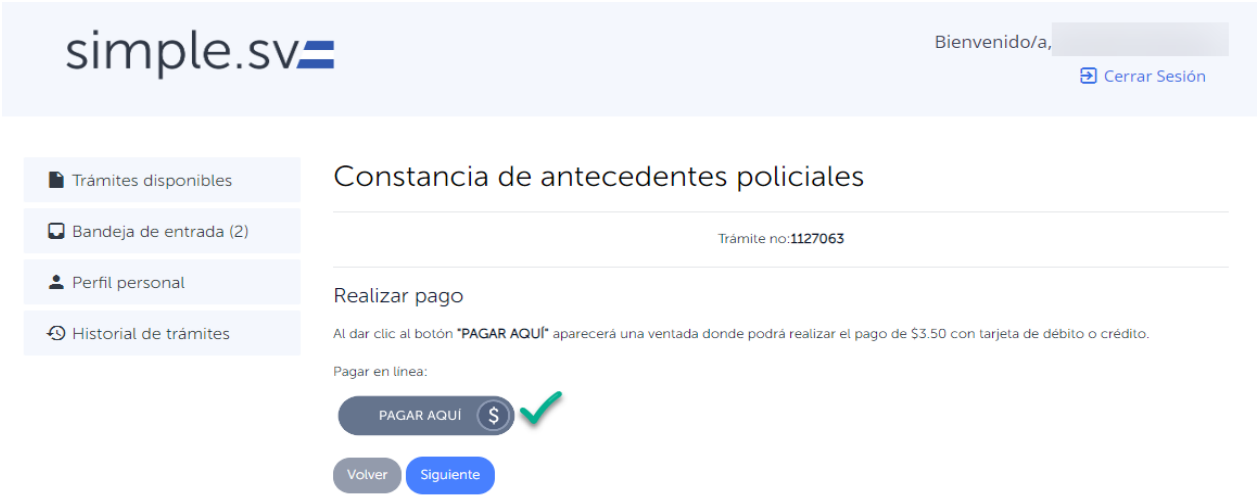

Fig. 13 *Realización de pago tarjeta débito o crédito*

13. Nos direcciona al formulario de pago a travez de serfinsa con los datos de nuestra tarjeta de crédito o débito.

Fig. 14 *Formulario de pago en línea*

14. Una vez realizado el pago nos da la opción para la descarga del comprobante en formato .pdf

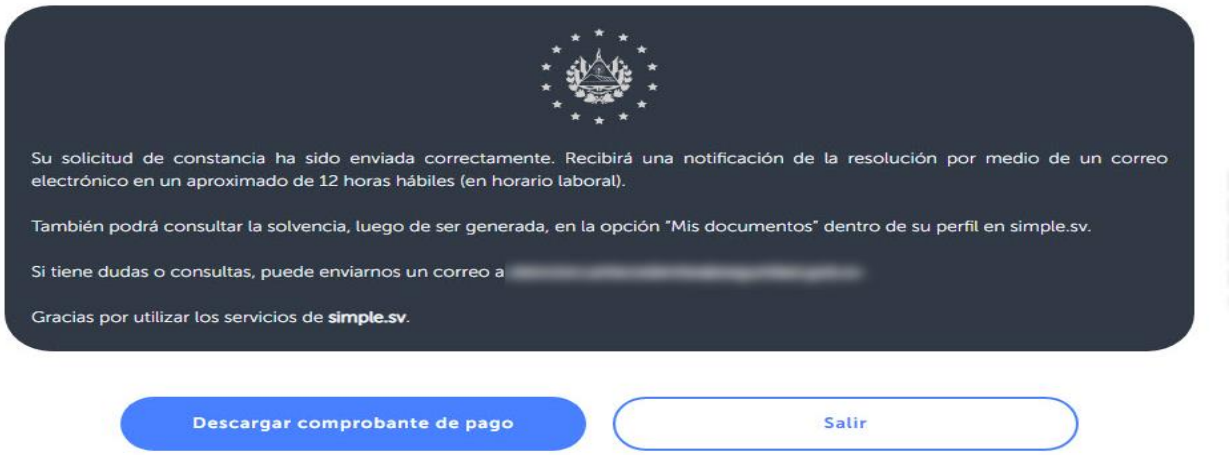

Fig. 15 *Notificación de aprobación del pago con adjunto de correo*

15. Luego nos permite ver el documento apostillado, de igual manera en pdf y para poderlo descargar.

Fig. 16 *Documento correctamente generado y apostillado.*

16. Pantalla que nos muestra todos los tramites que tenemos y sus diferentes estados de avance.

Fig. 17 *Formulario de solicitud de Apostilla del documento generado y apostillado correctamente dentro del formulario de trámites*

Capítulo III: Revisión de la Ley de Firma Electrónica

Si bien El Salvador ha dado un paso significativo en definir una Ley de Firma Electrónica, es importante mencionar que hay aspectos en dicha ley que se deben revisar y ajustar, para hacer que la misma propicie las condiciones para promover su uso por parte de la población en general, así mismo en dar las garantías jurídicas para que se enmarque en el Estado de Derecho.

La firma electrónica buscar automatizar procedimientos manuales en diferentes áreas. Así mismo, a través de las reformas realizadas busca brindar una mayor seguridad jurídica a los proveedores de servicios de certificación, a los usuarios de dichos servicios, así como fortalecer y dinamizar el clima de inversión en el país; a través del incentivo de nuevos modelos de negocios basados en estos servicios tecnológicos.

Algunos de los apartados a revisar y proponer mejoras en la LFE son los siguientes:

Tabla 2 Aspectos importantes de mejora en la Ley de Firma Electrónica

Aspectos actuales de la ley de firma electrónica	Aspectos de mejora en la ley de firma electrónica
• Artículo 4 del reglamento características vigentes para los requisitos de jefe de Unidad de Firma electrónica. • Ser salvadoreño; • De reconocida honorabilidad; • Contar con título universitario; • De notoria competencia para el ejercicio del cargo, contando con amplio conocimiento técnico y experiencia en la materia, y, • No tener conflictos de interés con lo regulado en la Ley de Firma Electrónica, en adelante "la Ley" y este Reglamento.	• Artículo 4 del reglamento, debería incluir que, para ser jefe de la Unidad de la Firma electrónica, se posea una certificación de la familia ISO 27000, por ser un puesto que requiere un conocimiento y experiencia en la materia. De igual forma debería tener de forma puntual el requisito de mínimo de experiencia en un área específica que esté relacionada al puesto.
• Artículo 9 del reglamento indica que los proveedores de los servicios regulados deberán rendir una fianza del 5% de sus activos, lo cual para las organizaciones con fuertes activos representan una inversión significativa, lo que a su vez	• Como recomendación en este apartado se debería dejar una fianza fija para iniciar operaciones, la cual no este directamente en función del monto de sus activos, y para la renovación anual de dicha fianza se debería establecer un

representa una barrera de entrada para poder ofrecer dichos servicios, por ejemplo grandes empresas y bancos nacionales o extranjeros podrían ofrecer estos servicios por que ya poseen infraestructuras tecnológicas muy robustas y a la vez son consumidores de servicios de servicios regulados en la ley, pero no encuentran atractivo, porque la fianza representa una alta erogación de fondos.	porcentaje sobre los contratos de servicios que el proveedor ha tenido durante el año. Esto sería más adecuado, ya que al inicio de la prestación de estos servicios las empresas pueden tener bajas ventas por ser servicios especializados y no requieren mantener activos grandes montos de las fianzas
• El número de servicios es limitado, lo que también limita el ámbito donde se pueda desarrollar la firma electrónica.	• Un catálogo más amplio de servicios a ser prestados por los proveedores de servicios de almacenamiento de documentos electrónicos, incluido el servicio de desmaterialización de documentos físicos que se pretendan almacenar electrónicamente.
• Artículo 18 del reglamento no indica que pasa si el proveedor no cumple con los requisitos para acreditarse, es decir si debe esperar cierta cantidad de tiempo para volver a registrarse o definitiva no puede volver a hacer el trámite de registro	• Artículo 18 del reglamento no indica que pasa si el proveedor no cumple con los requisitos para acreditarse, es decir si debe esperar cierta cantidad de tiempo para volver a registrarse o definitiva no puede volver a hacer el trámite de registro
• Artículo 23 del reglamento no indica que pasa si el proveedor de servicios no avisa del inicio de actividades con 10 días de anticipación.	• La reglamentación más precisa en cuanto a los requisitos y el procedimiento aplicable para la acreditación de los proveedores de servicios de certificación, en consideración del establecimiento de las cuatro modalidades aplicables a dichos servicios: firma electrónica certificada, sello electrónico, sello de tiempo y autenticación de sitios web.

Por otro lado, es importante mencionar que las expresadas reformas a la LFE han sido acompañadas con la reciente aprobación de la primera revisión al Reglamento Técnico Salvadoreño RTS 35.01.01:20, que establece los requisitos técnicos para la prestación de servicios de emisión de certificados electrónicos, siendo que dicha revisión sustituye la reglamentación técnica original que, con vigencia transitoria de un año, que fue aprobada en el mes de julio del año 2020.

También las reformas realizadas vienen a establecer un marco jurídico más claro en cuento a la equivalencia y valor probatorio de la firma electrónica simple o certificada.

Capítulo IV: Propuestas para promover el uso de la firma electrónica

El uso de la firma electrónica es una realidad en el mundo altamente digitalizado en el que vivimos, pero en El Salvador su nivel de avance ha sido bajo en comparación con otros países, por lo que es recomendable emprender acciones, las cuales deben ser creadas desde el Estado para facilitar las condiciones para que la población en general pueda tener acceso y utilizar estas tecnologías.

Para determinar las propuestas que promuevan el uso de la firma electrónica, se realizó como instrumento una encuesta en formato digital, en la cual se obtuvo respuesta de 47 personas y en función de sus respuestas se han realizados diversas propuestas:

Propuesta 1: Crear programas de educación virtual para reducir la brecha de conocimiento de la temática.

Para crear esta propuesta se han analizado las respuestas de las siguientes preguntas:

- Pregunta 2 ¿Ha utilizado la Firma Electrónica alguna vez?
  49% indica que no, a raíz de un número de causas como desconocimiento y desconfianza; lo que ha permitido este porcentaje tan alto.
- Pregunta 7 ¿Conoce los dispositivos que se utilizan para poder realizar una firma electrónica?
  79% indica que no conoce los dispositivos por diferentes razones, que se derivan en mucho del poco ó nulo uso de tecnología.
- Pregunta 5 ¿Conoce sobre la ley de Firma Electrónica aprobada en El Salvador?
  79% no conoce a Ley de Firma Electrónica con sus respectivas ventajas lo que limita el uso y hace crecer la inseguridad que puede otorgar la ley amparando al usuario de esta.
- Pregunta 8 ¿Participaría en una capacitación para conocer sobre la Firma Electrónica en nuestro país?
  93% indica que participaría en una capacitación, lo que permite que se vislumbre una enorme oportunidad para poder aprender e implementar primeramente de manera adecuada y con el conocimiento de las leyes que respaldan a los usuarios de firma electrónica.

La propuesta consiste en diseñar un programa de educación virtual para la población en general, donde se expliquen los beneficios de los certificados digitales, así como la forma de utilizarlos para operaciones y actividades cotidianas que realizamos cuando accedemos a servicios públicos y privados. Este programa también podría formar parte de la malla curricular del sistema de educación, el cual se incluya desde la educación básica para fomentar en los primeros años la adopción de estas tecnologías.

Los elementos claves que el programa de educación virtual necesita incluir son:

- **Definir que son los certificados digitales:** explicar de manera clara y concisa lo que son los certificados digitales, cómo funcionan y que beneficios pueden aportar a las personas.
- **Mencionar porqué son importantes los certificados digitales:** explicar por qué los certificados digitales son una forma segura de autenticar la identidad de un usuario en línea y por qué son esenciales en la actualidad.
- **Explicar para qué es la Unidad de Firma Electrónica:** explicar el papel que desempeña la Unidad de Firma Electrónica del Ministerio de Economía (MINEC).
- **Tipos de certificados digitales:** mencionar los diferentes tipos de certificados digitales que existen, tales como SSL, TLS, S/MIME, firma digital, entre otros.
- **Autoridad de Certificación:** explicar qué es una Autoridad de Certificación (CA) y cómo se utiliza para verificar y validar los certificados digitales.
- **Proceso de emisión:** detallar el proceso de emisión de los certificados digitales y cómo se garantiza la autenticidad de estos.
- **Uso de los certificados digitales**: mostrar ejemplos de cómo se utilizan los certificados digitales en diferentes entornos, como el comercio electrónico, la banca en línea, la firma electrónica, etc.
- **Seguridad**: hacer énfasis en la importancia de la seguridad en línea y cómo los certificados digitales pueden ayudar a prevenir fraudes y ataques cibernéticos.
- **Renovación de los certificados digitales:** explicar el proceso de renovación de los certificados digitales y por qué es importante mantenerlos actualizados.
- **Ventajas y desventajas:** explicar las ventajas y desventajas de los certificados digitales, incluyendo la facilidad de uso, el costo y la seguridad.
- **Preguntas frecuentes**: responder a preguntas comunes que los usuarios pueden tener sobre los certificados digitales, como validez, renovación, instalación entre otros.

Propuesta 2: Crear una institución o dar a la potestad a una institución del Estado para convertirse en Proveedor de Servicios de Certificación

Para crear esta propuesta se han analizado las respuestas de las siguientes preguntas:

- Pregunta 11: ¿Estaría dispuesto a asumir los costos económicos, por utilizar la firma electrónica?

  43% indica que no asumiría los costos por el uso de la firma electrónica.
- Pregunta 12: ¿Si en su trabajo o lugar de estudio le facilitan la Firma Electrónica para uso personal estaría dispuesto a utilizarla?

  91% de las personas indican que, si utilizaran la firma electrónica, si desde su lugar de trabajo o estudio se les brinda, por lo tanto es una oportunidad para poder implementar el uso de masivo de la firma.

- ¿Cuáles serían las principales limitantes para el uso de la Firma Electrónica?
  27% indica que el costo que pueda tener es una limitante, pues son conscientes que este tipo de servicios tiene costos asociados.

El objetivo de esta propuesta es que el Estado por medio de una institución pueda ser un Proveedor de Servicios de Certificación (PSC), tanto para ciudadanos, funcionarios públicos y empresas. En esta propuesta el Estado podría ofrecer servicios de certificación a un bajo costo en relación con precios ofertados por el mercado en general, dado que podría aplicar economías de escala en la emisión de certificados, lo cual se traduciría en un ahorro para la población y empresas. Así mismo, estas acciones contribuirían a intensificar el uso de estas tecnologías de forma general.

Al disponer de certificados digitales de bajo costo, su uso se podría implementar en una serie de servicios públicos y privados que traerían diversas ventajas y beneficios, como, por ejemplo:

- Registros de gremios de profesionales como doctores, ingenieros, arquitectos, psicólogos, odontólogos entre otras.
- Representantes o apoderados legales de empresas.
- Funcionarios públicos que emiten documentos.
- Firmas en operaciones bancarias como depósitos y retiros del público en general.
- Firmas de contratos de alquiler de inmuebles y prestación de servicios.
- Pasaporte digital el cual este respaldo por un certificado digital.
- Emisión de citas y recetas médicas de la red de hospitales públicos, privados y del ISSS.
- Emisión de notas del sistema de educación público y privado.

Dentro de los casos de usos de estos servicios y sus ventajas podemos mencionar:

a) Registro de profesionales de diferentes gremios en línea.
   Ventajas:
   - Mejorar eficiencia en el proceso de registro, eliminando la necesidad de documentación en papel.
   - Facilitar la verificación de la validez de la certificación por parte de las autoridades competentes.
   - Reducir errores y fraude en el proceso de registro.

b) Firma de contratos
   Ventajas:
   - Eliminar documentación física y desplazamiento a oficinas, propiciando la reducción de costos y tiempo.

- Aumentar la seguridad y autenticidad de las firmas, por medio de la encriptación y autenticación de la identidad del firmante.
- Facilitar la firma de contratos con personas en diferentes ubicaciones geográficas.

c) Gestión de tramites en línea

Ventajas:

- Posibilitar la realización de trámites en línea, al permitir una identificación segura y autenticada del usuario.
- Acortar el tiempo y costos asociados con los trámites presenciales.
- Ofrecer de trámites desde cualquier lugar con acceso a internet.

d) Prestación de servicios de salud y de asesorías técnicas en línea.

Ventajas:

- Facilitar la autenticación y verificación de la identidad del paciente y del profesional médico.
- Mayor privacidad y seguridad de la información médica del paciente.
- Gestionar las citas, recetas y resultados de exámenes en línea.
- Brindar servicios y consultas profesionales en línea ofreciendo servicios a personas nacionales y extranjeras, lo cual generaría ingresos para el país.

e) Autenticación y validación de títulos en línea

Ventajas:

- Proveer la validación de la autenticidad de títulos y credenciales académicas, eliminando la necesidad de la presencia física de los documentos.
- Mejorar seguridad en el proceso de validación, gracias a la encriptación y autenticación de la identidad del titular del título.
- Ofrecer la posibilidad de validar títulos y credenciales académicas de personas en diferentes ubicaciones geográficas del país y dar la posibilidad a la diáspora de acercar los servicios.

f) Acceso a plataformas de educación en línea

- Facilitar la autenticación y verificación de la identidad del estudiante.
- Elevar el nivel de privacidad y seguridad de la información académica del estudiante.
- Mejorar la gestión de cursos, evaluaciones y certificaciones en línea.

g) Acceso a plataformas de trabajo remoto
    - Suministrar la autenticación y verificación de la identidad del trabajador.
    - Incrementar la privacidad y seguridad de la información laboral del trabajador.
    - Facilita la gestión de proyectos y tareas en línea.

h) Verificación de antecedentes laborales
    - Permitir la verificación de los antecedentes laborales de un candidato a un puesto de trabajo.
    - Mejorar la seguridad y autenticidad de la información laboral verificada.
    - Descartar la necesidad de documentos físicos y desplazamiento a oficinas.

i) Acceso a diversos servicios financieros

    Ventajas
    - Acercar préstamos a la población, eliminado la necesidad de firmar documentos de forma presencial, lo cual reduce costos para la población y aumenta la automatización de los servicios financieros.
    - Consultar buros de créditos por parte del ciudadano y regular el uso desmedido de este tipo de empresas, asegurando que las consultas que realizan tengan en aval de la persona que investigan.

j) Gestión de una identidad digital para la población

    Ventajas
    - Ofrecer a la población la posibilidad de generar identidades digitales de forma segura que le permitan además de la identificación, el poder realizar trámites en línea de forma ágil.
    - Tener un registro actualizado y moderno de la población, lo cual permita integrar los expedientes personales, médicos, académicos, laborales y cualquier historial que sea a de interés para el Estado.

Propuesta 3: Crear Instituto de Ciberseguridad

Para crear esta propuesta se han analizado las respuestas de las siguientes preguntas:

- **Pregunta 5:** ¿Conoce sobre la Ley de Firma Electrónica aprobada en El Salvador?

    79% indica que no conoce la Ley de Firma Electrónica

- **Pregunta 6:** ¿Estaría dispuesto a dejar de firmar en papel si pudiera hacerse por un medio electrónico?
    64% indica que si estuviera dispuesto en dejar de firmar en papel.
- **Pregunta 10:** ¿Considera que la Firma Electrónica es tan segura como una Firma Manuscrita?
    Un 31% no considera segura la firma electrónica, por lo tanto, se debe trabajar mucho en educar a la población en este tema.
- **Pregunta 18:** ¿Cuáles serían las principales limitantes para el uso de la Firma Electrónica?
    18% solo confía en la firma que se hace papel

La creación del Instituto de Ciberseguridad puede apoyar en la divulgación y fortalecimiento del marco legal en la ciberseguridad, así mismo puede financiar a jóvenes para formar profesionales de IT a lo largo del país en el área de ciberseguridad. Además, este instituto puede ayudar a fortalecer la seguridad informática de la infraestructura del país, así como aportar en investigaciones tecnológicas que permitan acercar servicios de forma segura a la población.

Los elementos claves que debe poseer este instituto para ofrecer seguridad de la información a la población son:

- **Marco legal:** El instituto debe contar con un marco legal y regulador claro, que permita la implementación efectiva de políticas y procedimientos de seguridad cibernética. Es importante mencionar que, de la encuesta realizada un 21% conoce sobre la Ley de Firma Electrónica, lo cual también hace necesario que las normativas sean divulgadas por diversos medios para llegar a la población. A la fecha, ya se inició el fortalecimiento del marco legal en el país, con creación de la Política de Ciberseguridad de El Salvador, sin embargo, es importante destacar que es necesario más normativas como la Ley de Protección de Datos Personales, la cual es un hito clave en la seguridad de los datos de la población y poder darle mayor confianza por medio de las tecnologías, ya que de acuerdo con la encuesta realizada hay 18% que solo confía en la firma que se hace en papel, por lo que es clave tener un marco legal robustecido y divulgado, y de esta forma poder dar la tranquilidad a la población.
- **Una estructura organizativa sólida:** el instituto debe estar estructurado de manera clara y definida para garantizar una gestión eficaz de las operaciones de seguridad cibernética.
- **Personal altamente capacitado:** el instituto debe contar con un equipo de expertos altamente capacitados en ciberseguridad para realizar análisis y evaluaciones de riesgos, desarrollar y aplicar políticas y procedimientos de seguridad y responder rápidamente a incidentes de seguridad.

- **Tecnología avanzada:** el instituto debe tener acceso a tecnología avanzada para monitorear, detectar y responder a las amenazas de seguridad cibernética, como firewalls, sistemas de detección de intrusiones y herramientas de análisis de datos.
- **Colaboración con otras organizaciones:** el instituto debe colaborar con otras organizaciones gubernamentales, industrias y grupos de la sociedad civil para compartir información y recursos, y para coordinar la respuesta a incidentes de seguridad cibernética.
- **Programas de concientización y capacitación:** el instituto debe ofrecer programas de concientización y capacitación en ciberseguridad para la población, con el objetivo de educar a las personas sobre los riesgos y amenazas cibernéticas y proporcionarles las habilidades necesarias para protegerse.
- **Planes de continuidad del negocio:** el instituto debe tener planes de continuidad del negocio en caso de que ocurra un incidente de seguridad cibernética grave, para garantizar la continuidad de las operaciones críticas y minimizar el impacto en la población.

Propuesta 4: Crear infraestructura pública para brindar acceso a Internet

Las propuestas antes descritas también necesitan de otras acciones complementarias para que la aplicación y funcionamiento de estas tengan los resultados esperados, ya que muchas de estas transformaciones plantean retos para el Estado, el cual debe reinventar las instituciones y trabajar en la automatización de procesos y servicios que se brindan en cada una de las instituciones, asegurar el marco normativo para el respaldo jurídico de las operaciones y autorizaciones electrónicas que se estarían realizando por medios de las plataformas tecnológicas. El Estado debería de tomar como referencia la automatización realizada por Estonia, en donde el 99% de los servicios gubernamentales se brindan en línea y el 99% de la población tiene una identidad electrónica (Porrúa, 2022).

Para el éxito de todas estas medidas es clave crear una infraestructura pública para brindar acceso a Internet a la población en general, la cual, de cobertura a todo el territorio nacional, para asegurar que se brinda la carretera digital en la cual puedan transitar los datos. El Estado debe asegurar que el Internet sea un servicio público, así mismo crear las condiciones para que la población pueda acceder a los servicios.

Es importante aclarar que el asegurar los servicios básicos no riñe con los servicios que brindan las empresas privadas de telecomunicaciones, ya que estas acciones son propias del libre mercado donde cada uno puede competir con las reglas claras, y eso a su vez traerá una mejora en la calidad de los servicios de telecomunicaciones y permitirá generar precios más competitivos.

Como referencia El Estado salvadoreño pudiera retomar el caso de éxito de Uruguay, donde ha desarrollo una serie de programas y políticas que mejoran las condiciones tecnológicas de la población, entre las cuales podemos mencionar:

- **Políticas de inclusión digital:** el gobierno uruguayo ha implementado políticas de inclusión digital para promover el acceso a Internet y la tecnología en todo el país. Estas políticas incluyen la distribución de computadoras portátiles a estudiantes de escuelas públicas (lo cual en El Salvador ya se realiza por parte del Estado) y la creación de centros de acceso público a Internet (lo cual también en El Salvador muestra avances por medio del programa de los Centros Urbanos de Bienestar y Oportunidades CUBO).
- **Infraestructura de banda ancha:** Uruguay ha invertido en la construcción de una infraestructura de banda ancha de alta velocidad en todo el país, lo que ha permitido una mayor penetración de Internet. Además, el gobierno ha trabajado en la implementación de tecnologías como la fibra óptica y el cable submarino para mejorar la calidad del servicio de Internet. En El Salvador las telecomunicaciones están privatizadas desde finales de la década de los 90, pero el Estado podría generar un proyecto para crear una red de fibra óptica en el país, así como en aquellos lugares de difícil acceso realizarlo por medios de conexiones satelitales como por ejemplo los servicios de Starlink.
- **Costos accesibles:** el gobierno uruguayo ha trabajado para garantizar que los servicios de Internet sean accesibles para todos los ciudadanos. Esto ha sido posible gracias a las políticas de regulación de precios y la competencia en el mercado.
- **Educación y capacitación:** el gobierno uruguayo ha invertido en la educación y la capacitación en tecnología para los ciudadanos. Esto ha sido posible gracias a la implementación de programas de educación digital para estudiantes y adultos mayores.

Capítulo V: Conclusiones sobre firma electrónica

1. Los principales mecanismos para promover el uso de la firma electrónica, es en primer lugar la educación, es decir en dar a conocer a la población salvadoreña la teoría básica sobre la firma electrónica, los beneficios de esta y todos los posibles ahorros que su uso podría representar.

2. La automatización de la factura y apostilla electrónica que El Salvador ha iniciado es la punta lanza de la automatización de procesos y como parte de la modernización del Estado, si bien aún falta mucho por hacer, es importante destacar que los dos proyectos mencionados van a generar muchos beneficios a la población salvadoreña.

3. Conforme se va aumentando el uso de internet y se modernice con tecnología, existirán siempre en la población en general esos paradigmas y dudas con respecto a transacciones electrónicas y/o firma electrónica, como medida de seguridad para los usuarios y como método prioritario es contar con leyes que estén acordes con los avances tecnológicos del momento y que den respaldo al usuario final.

4. En referencia a las actualizaciones también se debe poner especial cuidado al tipo infraestructura, herramientas y costos que permitan emitir firma electrónica, con toda la seguridad y formalidad que la misma requiere.

Anexos

Anexo I: Encuesta de la Firma Electrónica

Objetivo: Conocer el nivel de uso y dominio respecto a la utilización de la Firma Electrónica en El Salvador.

* Indica que la Pregunta es obligatoria.

1. ¿Conoce qué es la Firma Electrónica?

Si ⬭
No ⬭

2. ¿Ha utilizado la Firma Electrónica alguna vez? *

Si ⬭
No ⬭

3. ¿Conoce para que sirve la Firma Electrónica? *

Si ⬭
No ⬭

4. ¿En qué sector productivo labora?

Selecciona todos los que correspondan.

- ☐ Empresario
- ☐ Profesional Independiente

- [ ] Emprendedor
- [ ] Empleados de empresa privada
- [ ] Empleados gubernamentales
- [ ] Estudiante
- [ ] No Trabajo

Público en General

Estas son las preguntas esenciales para conocer su opinión sobre la Firma Electrónica.

5. ¿Conoce sobre la ley de Firma Electrónica aprobada en El Salvador?

Si ⬭
No ⬭

6. ¿Estaría dispuesto a dejar de firmar en papel si pudiera hacerse por un medio electrónico?

Si ⬭
No ⬭

7. ¿Conoce los dispositivos que se utilizan para poder realizar la firma electrónica?

Si ⬭
No ⬭

8. ¿Participaría en una capacitación para conocer sobre la Firma Electrónica en nuestro país?

Si ⬭
No ⬭

Preguntas de Encuesta.

Esta sección es para poder conocer su opinión sobre la firma electrónica

9. ¿En qué tipo de documentos o trámites considera que se puede utilizar la Firma Electrónica en nuestro país?

Seleccionar Documento

DUI ☐

Pasaporte ☐

Licencia de conducir ☐

Firma de préstamos bancarios ☐

Firma de contratos en general ☐

Emisión de recetas médicas ☐

Garantías ☐

Trámites en instituciones públicas ☐

Trámites en aseguradoras ☐

10. ¿Considera que la Firma Electrónica es tan segura como una Firma Manuscrita?

Si ◯

No ◯

11. ¿Estaría dispuesto a asumir los costos económicos, por utilizar la firma electrónica?

Si

No

12. ¿Si en su trabajo o lugar de estudio le facilitan la Firma Electrónica para uso personal estaría dispuesto a utilizarla?

Si

No

13. ¿Conoce si es de uso legal la Firma Electrónica en El Salvador?

Si

No

14. ¿Conoce algún país del mundo que utiliza Firma Electrónica?

Si su respuesta es "SI" indique el país del cual tiene conocimiento, caso contrario dejar en blanco su respuesta.

15. ¿Considera que firmar documentos desde su casa u oficina y/o negocio le traería beneficios en lugar de ir físicamente a firmarlos?

Si

No

16. ¿Considera que la Firma Electrónica ayuda al medio ambiente respecto a la disminución del consumo de papel y tala de árboles?

Si

No

17. ¿Considera que la Firma Electrónica llegará a sustituir a la firma en papel?

Si

No

18. ¿Cuáles serían las principales limitantes para el uso de la Firma Electrónica?

Seleccionar Documento

No saber usarla

Solo confía en la firma que se hace papel

No confío en una firma electrónica

El costo que pueda tener

Desconocimiento

Anexo II: Resultados de encuesta de la Firma Electrónica

1. ¿Conoce qué es la Firma Electrónica?

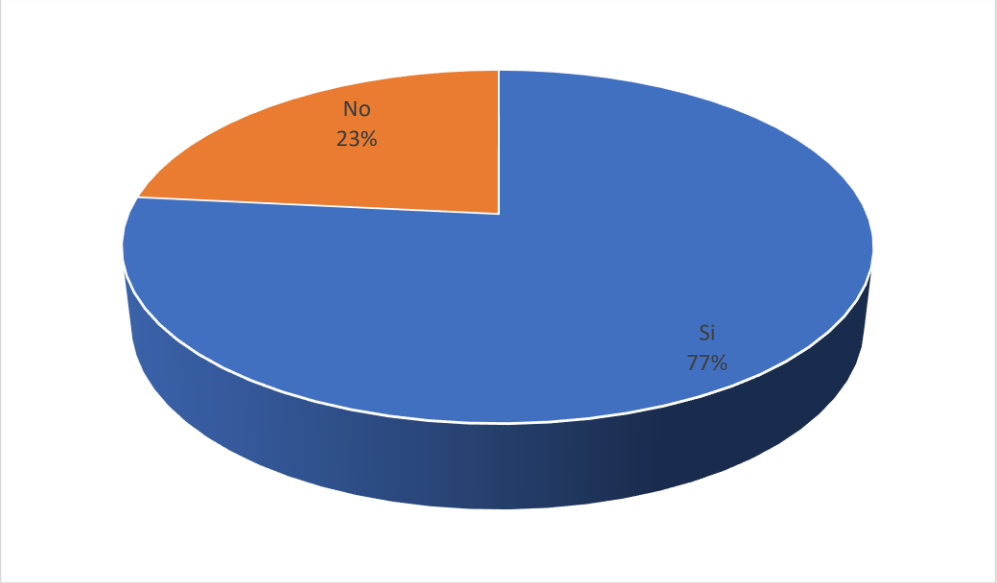

Fig. 18 Gráfico de resultados de quienes conocen que es firma electrónica.

En el presente gráfico del total de los encuestados podemos observar que el 77% conocen de alguna medida la Firma Electrónica, lo cual da un punto de partida para trabajar en los grupos que aún no conocen sobre este tema, que, aunque parezca pequeño es cerca de la cuarta parte, por lo tanto, la parte de educar y expandir el conocimiento es clave.

Como propuesta de acción para los datos en cuestión se debe solidificar la promoción de la información referente a la ley de firma electrónica y así poder sentar un precedente de uso antes de utilizarla y generar confianza en el usuario.

2. ¿Ha utilizado la Firma Electrónica alguna vez?

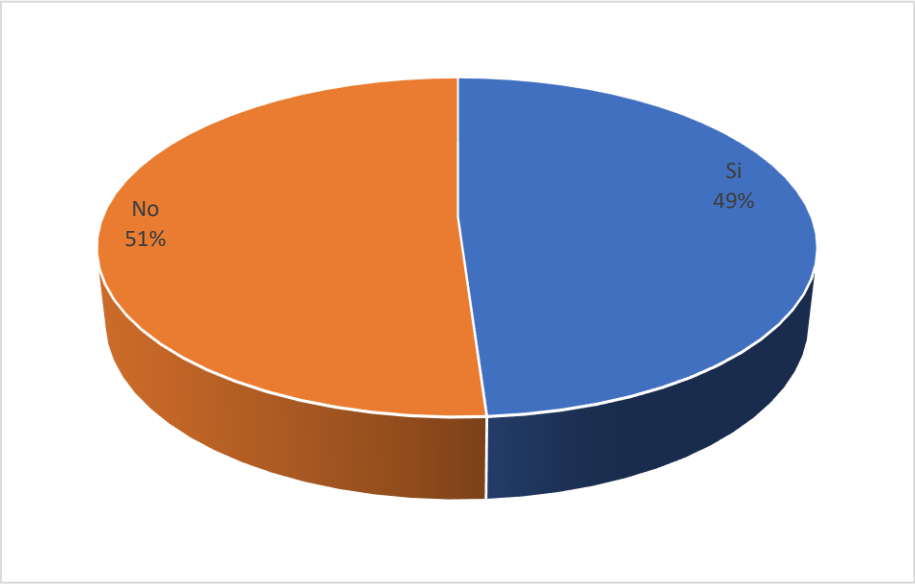

Fig. 19 Gráfico de resultados de las personas que ya utilizaron la firma electrónica.

A pesar de que se conozca lo que es la firma electrónica, la interacción con esta no ha sido la mejor en cuanto a su uso refiere, puesto que el 51% no ha hecho uso de esta. Para poder aumentar la utilización de la firma electrónica, es preciso la adecuada promoción para el uso y dar a conocer los beneficios de esta.

Como propuesta de acción para los datos en cuestión se debe solidificar la promoción de la información referente a la ley de firma electrónica y así poder sentar un precedente de uso antes de utilizarla y generar confianza en el usuario.

Adicional a que la ley debería proporcionar a las personas y/o empresas la posibilidad de elegir el tipo de firma a utilizar para poder adaptar a sus modelos de negocios.

3. ¿Conoce para que sirve la Firma Electrónica?

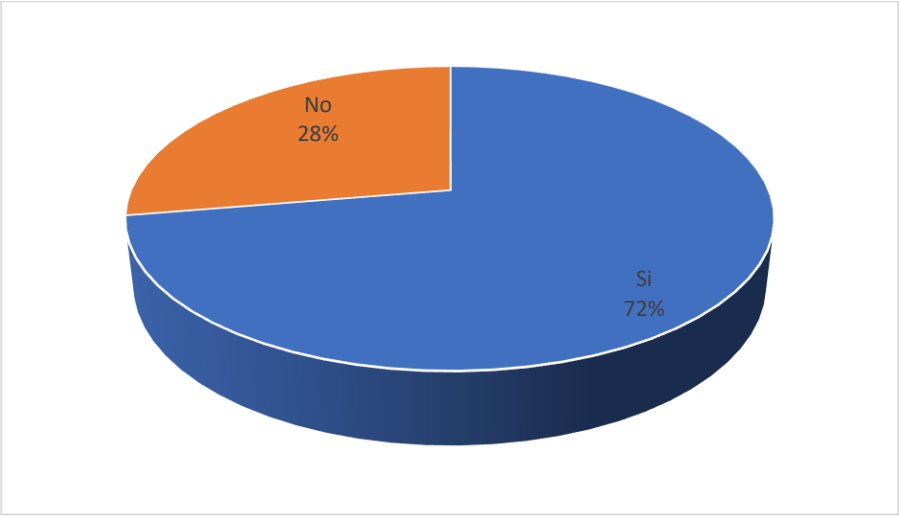

Fig. 20 Gráfico de resultados de la interrogante para que sirve la firma electrónica.

Los resultados reflejan que un 72% de los evaluados han manifestado, que, si conocen para que sirve la firma electrónica, más esto no les exime de la poca utilización que tienen de la misma en los diferentes entornos posibles para aplicarla. Es importante reconocer que el grueso de la población encuestada son empleados tanto privados como gubernamentales, el cual les permite permanecer en un ámbito que les obliga a conocer de alguna medida el tema de la firma electrónica.

4. ¿En qué sector productivo labora?

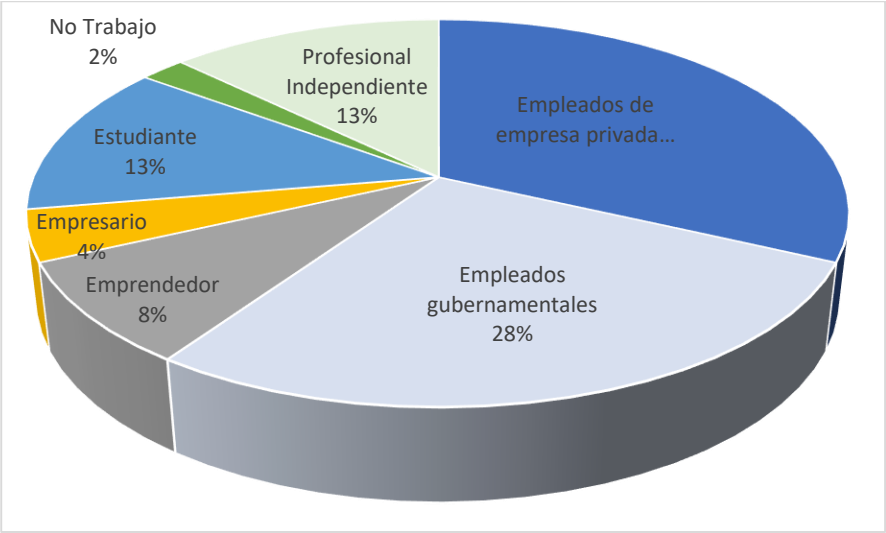

Fig. 21 Gráfico de resultados de ocupación de los encuestados.

A partir de esta pregunta nos podemos encontrar que más del 50% son empleados de la empresa privada como del sector público, lo que nos da la pauta para una posible estrategia para el uso de la firma electrónica con un poco más de facilidad para asimilar los cambios en los que incurre su implementación.

5. ¿Conoce sobre la ley de Firma Electrónica aprobada en El Salvador?

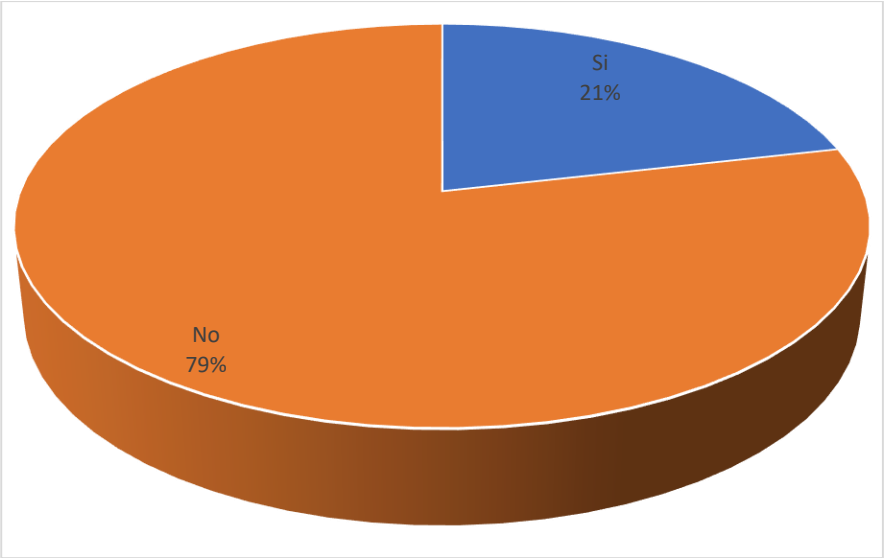

Fig. 22 Gráfico de resultados del conocimiento sobre ley de firma electrónica.

El resultado denota que un 79% de los encuestados no tienen conocimiento referente a la ley que respalda el uso e implementación de la firma electrónica en El Salvador, lo cual ofrece una oportunidad de mejora en trabajar en la educación de la población para dar a conocer la normativa relacionada con la firma electrónica, es decir, una promoción de dicha ley por los diferentes medios de comunicación, incluyendo las redes sociales.

6. ¿Estaría dispuesto a dejar de firmar en papel si pudiera hacerse por un medio electrónico?

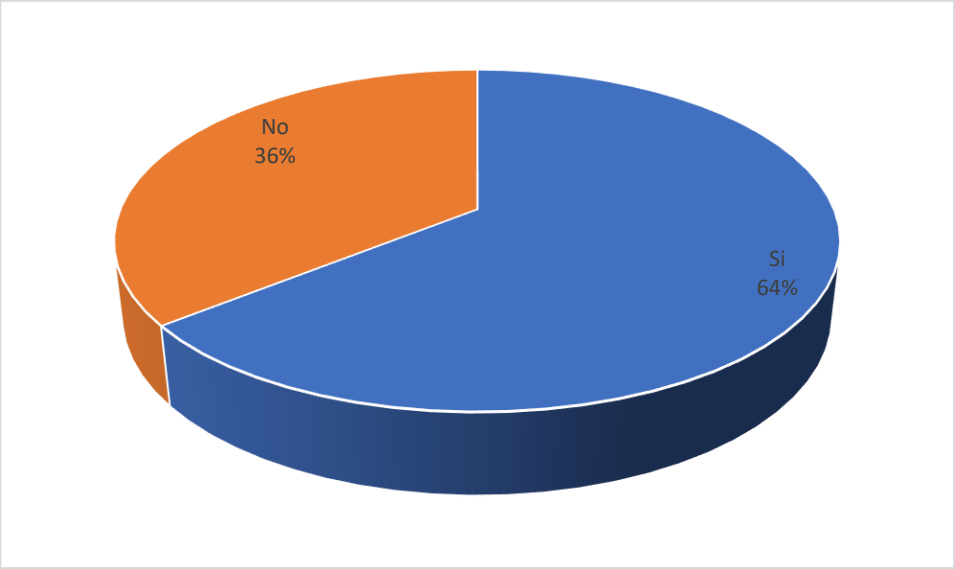

Fig. 23 Gráfico de resultados de quienes sustituirían la firma en papel por la firma electrónica.

Dentro del número de encuestados el 64% considera que es una muy buena opción el dejar de firmar en papel, sin embargo, es importante mencionar que el 36% no está de acuerdo, ya que hay un número determinado de personas que, por temor, desconocimiento e inseguridad, no está dispuesto a dar el paso, por lo tanto, se debe trabajar en educar a la población en mostrar los beneficios de la firma electrónica, así como también en dar a conocer las medidas de seguridad que ofrece.

7. ¿Conoce los dispositivos que se utilizan para poder realizar una firma electrónica?

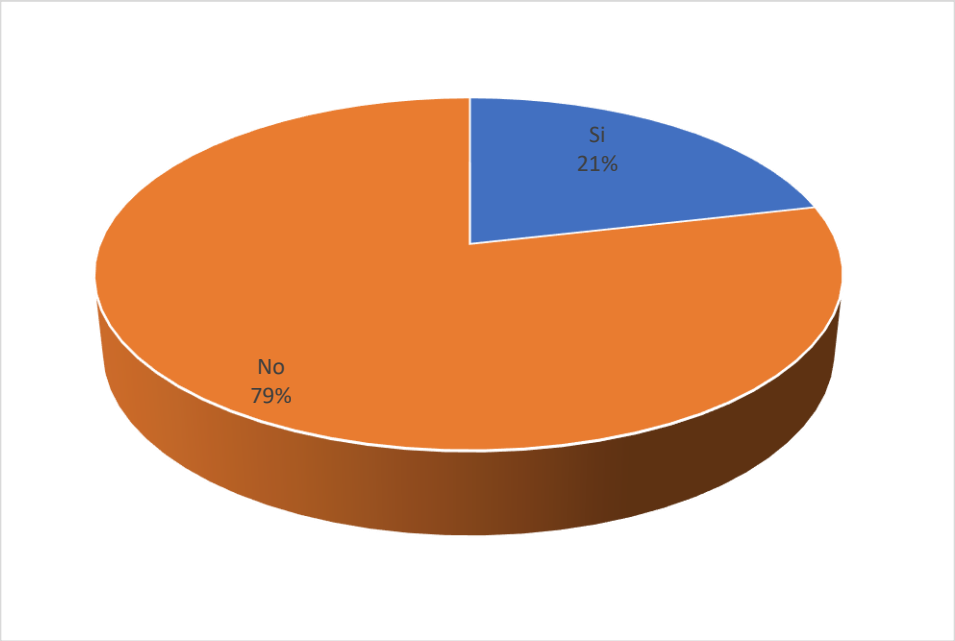

Fig. 24 Gráfico de resultados de los dispositivos utilizados para la firma electrónica.

El 79% de los encuestados desconocen la tecnología para implementar la firma electrónica, lo que indica que se debe capacitar en este tipo de tecnologías, herramientas y dispositivos para que la población pueda tener los conocimientos de esta área.

8. ¿Participaría en una capacitación para conocer sobre la Firma Electrónica en nuestro país?

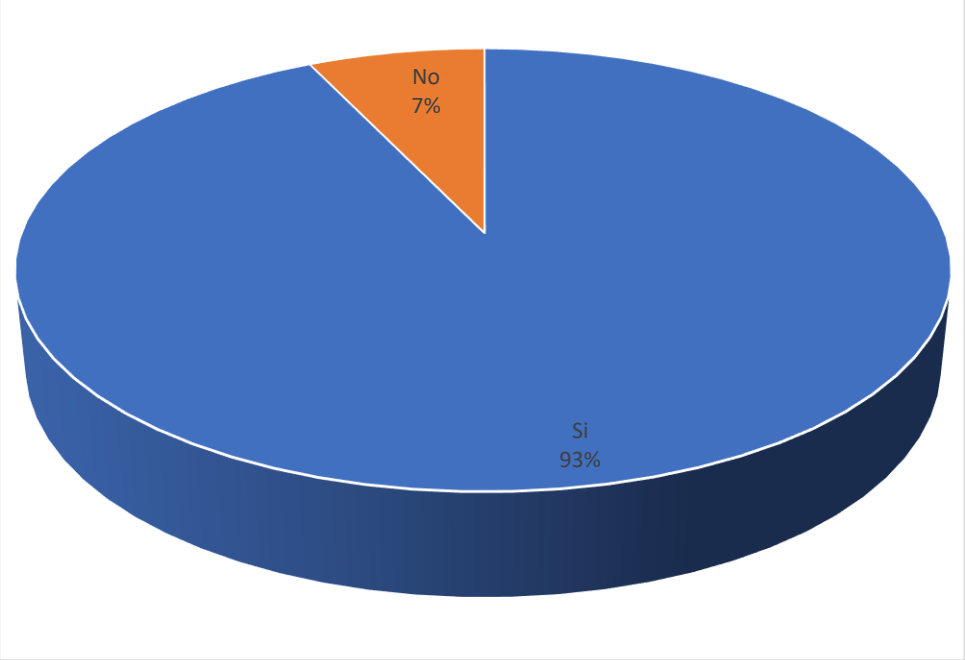

Fig. 25 Gráfico de resultados de quienes participarían en capacitación de firma electrónica.

El 93% del personal entrevistado estaría en la disposición de participar en una capacitación sobre la firma electrónica, lo cual muestra una apertura por parte de la población en formarse sobre nuevas tendencias tecnológicas disponibles.

9. ¿En qué tipo de documentos o trámites considera que se puede utilizar la Firma Electrónica en nuestro país?

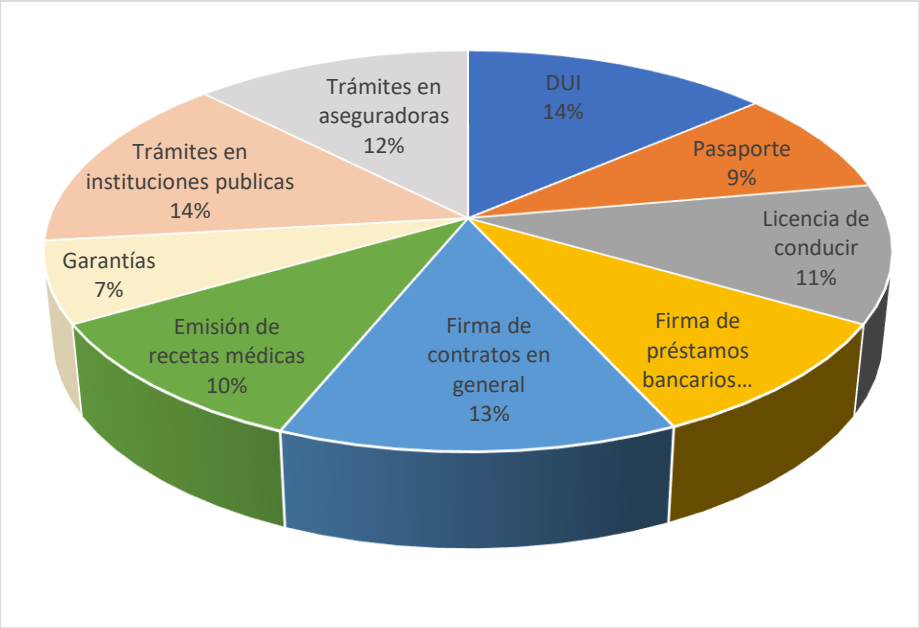

Fig. 26 Gráfico de resultados de documentos posibles a utilizar en la firma electrónica.

Es importante destacar que la firma electrónica para la población encuestada ofrece mucha utilidad para la gestión de tramites en las instituciones públicas, la cual es la opción que cuenta con 14%, seguida de la firma de contratos en general. Las cuáles deberían ser las principales áreas que se deben explotar para intensificar el uso de la firma digital.

10. ¿Considera que la Firma Electrónica es tan segura como una Firma Manuscrita?

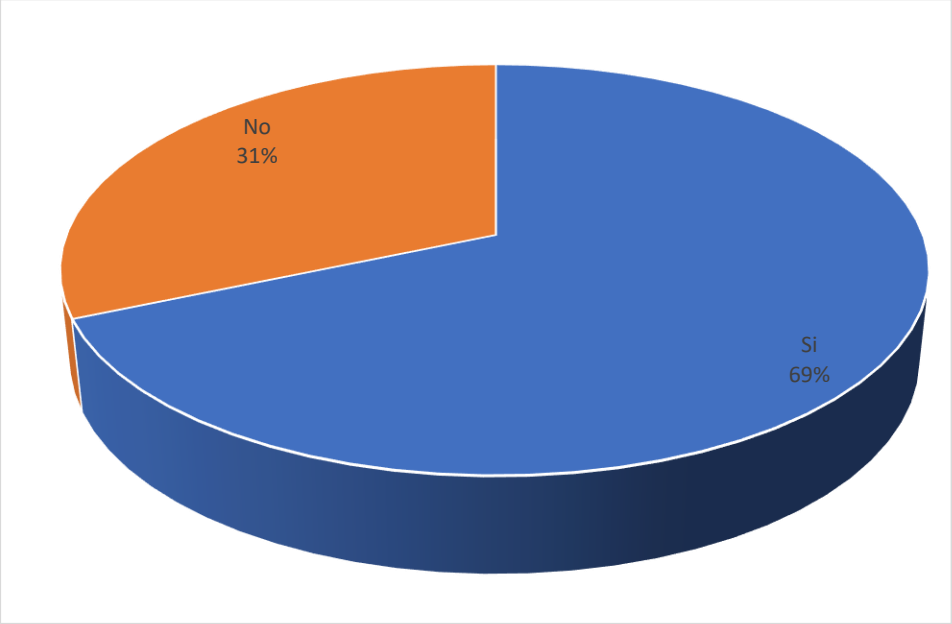

Fig. 27 Gráfico de resultados de quienes consideran que la firma electrónica es segura.

El 69% de los encuestados consideran que la firma electrónica es suficientemente segura al igual que la manuscrita, lo que da un indicio de confianza en la misma, sin embargo, es importante aclarar que se debe educar en el tema, sobre todo para mostrar las medidas de seguridad que ofrece la firma electrónica.

11. ¿Estaría dispuesto a asumir los costos económicos, por utilizar la firma electrónica?

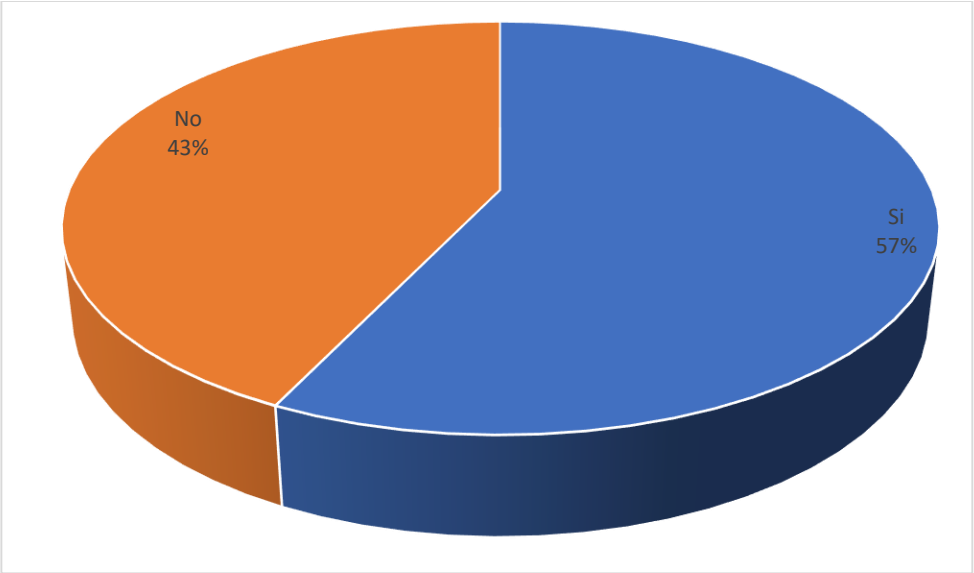

Fig. 28 Gráfico de resultados de quienes podrían pagar por usar la firma electrónica.

El 57% de los entrevistados está en la disposición de cubrir costos económicos que pueda representar la firma electrónica, pero también es importante mencionar que el 43% no estaría en la disposición de asumirlos, por lo tanto, también se pueden buscar mecanismos para que el costo económico que representa la firma electrónica en un inicio pueda ser en alguna medida financiado por parte del Estado como incentivación de su uso.

12. ¿Si en su trabajo o lugar de estudio le facilitan la Firma Electrónica para uso personal estaría dispuesto a utilizarla?

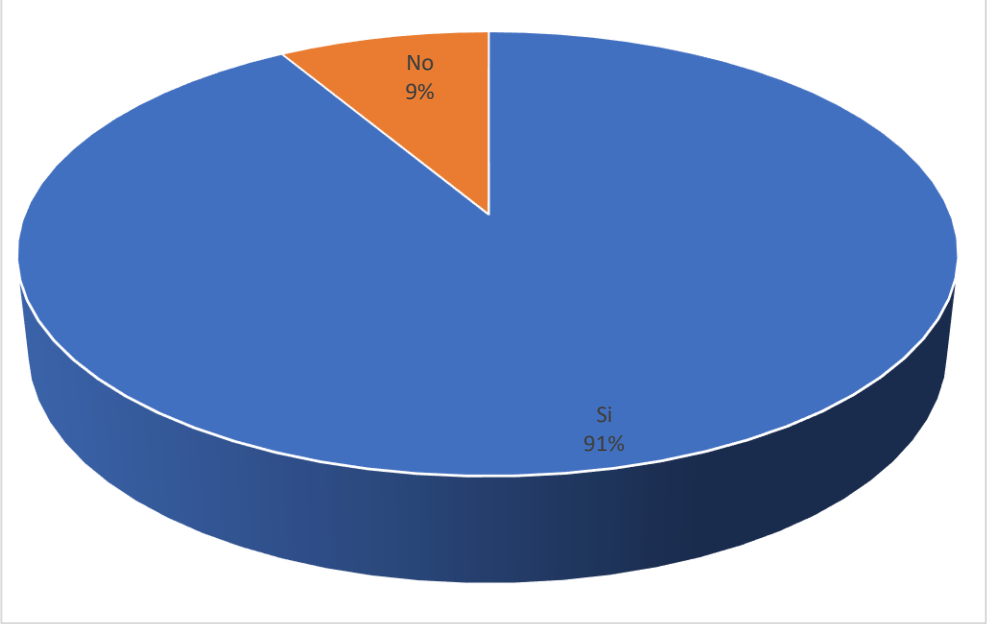

Fig. 29 Gráfico de resultados de quienes utilizarían la conocen firma electrónica en su trabajo.

Los lugares de trabajo o estudio son la mejor forma de propiciar el uso de la firma digital, como se observa en la encuesta, el 91% de las personas manifestaron que la usarían si se les facilita desde su trabajo o lugar de estudio. Sin duda tenemos claro que los empleados y estudiantes tienen mayor acceso a la tecnología, lo que facilita la adopción de cualquier herramienta.

13. ¿Conoce si es de uso legal la Firma Electrónica en El Salvador?

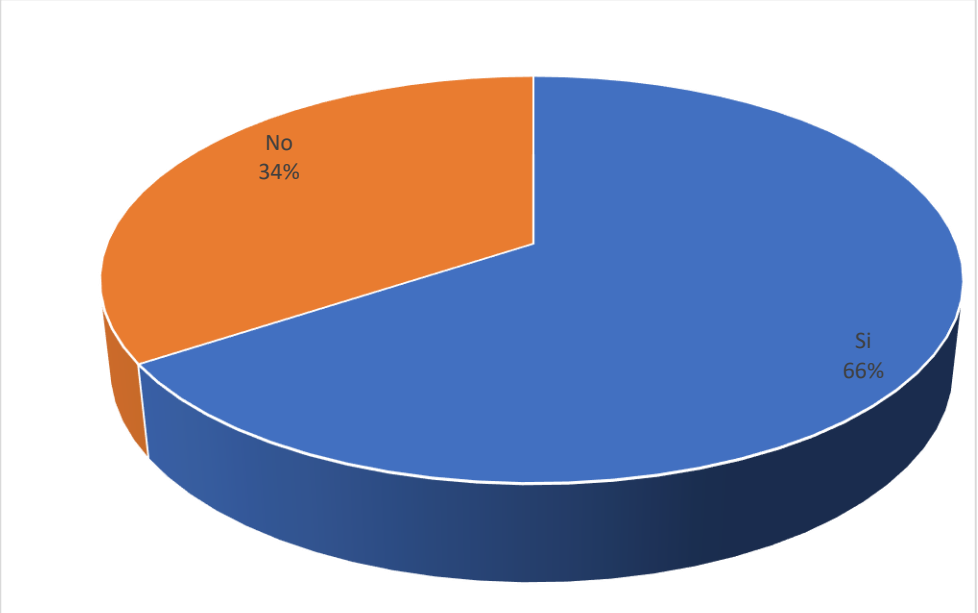

Fig. 30 Gráfico de resultados de que tan legal es la Firma Electrónica.

De los encuestados el 34% manifiesta desconocimiento de la Ley de la Firma electrónica, lo cual es una oportunidad para trabajar en la divulgación de la dicha ley, lo cual es clave para que también se aumente el uso.

14. ¿Conoce algún país del mundo que utiliza Firma Electrónica?

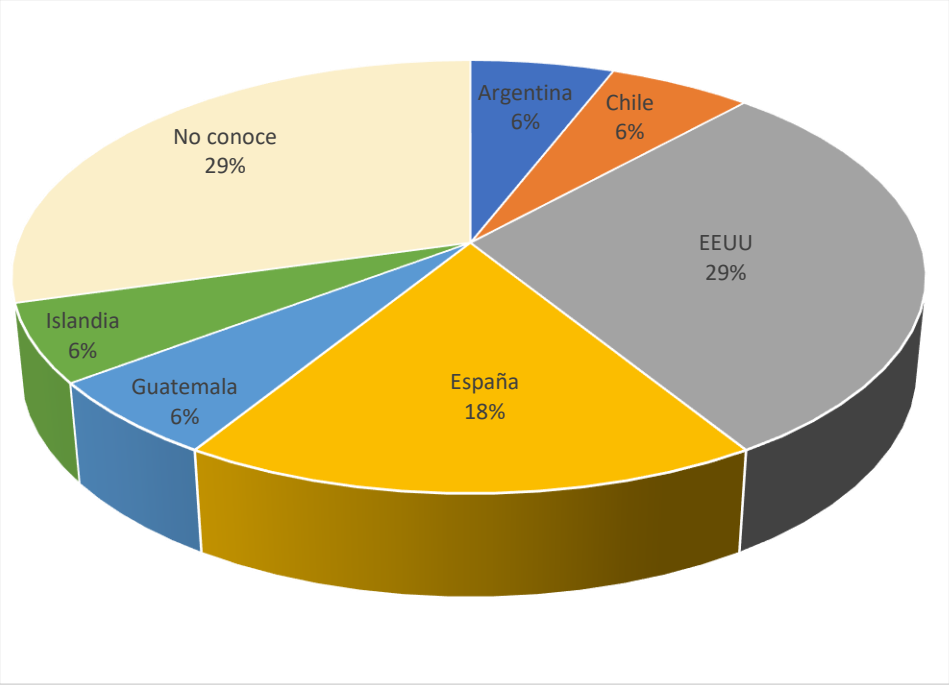

Fig. 31 Gráfico de resultados de países que tienen establecida la firma electrónica.

El 29% de los encuestados conocen que en Estados Unidos se utiliza la firma electrónica, así mismo hay un 29% que desconoce algún país donde esta se utiliza, por lo que también es necesario que en la temática de capacitación para la Firma Electrónica incluya casos de éxitos de diversos países de la región.

15. ¿Considera que firmar documentos desde su casa u oficina y/o negocio le traería beneficios en lugar de ir físicamente a firmarlos?

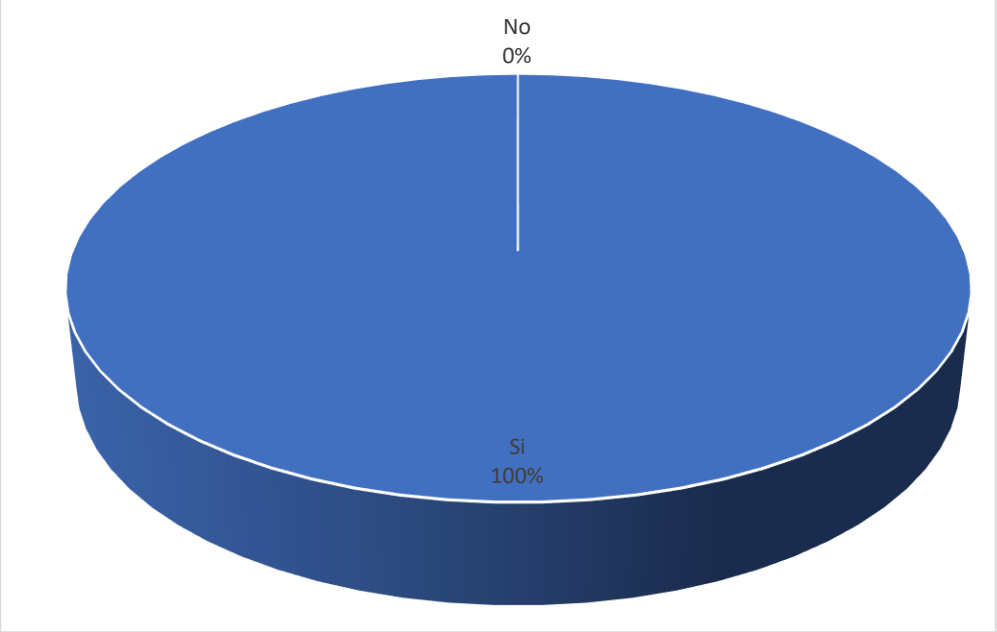

Fig. 32 Gráfico de resultados de los que están convencidos de los beneficios de la firma electrónica.

El 100% de los encuestados indican que firmar documentos de forma electrónica le traería beneficios, entre los cuales podemos mencionar tiempo y dinero. Así mismo se aumentaría la eficiencia en las respuestas a los tramites disponibles.

16. ¿Considera que la Firma Electrónica ayuda al medio ambiente respecto a la disminución del consumo de papel y tala de árboles?

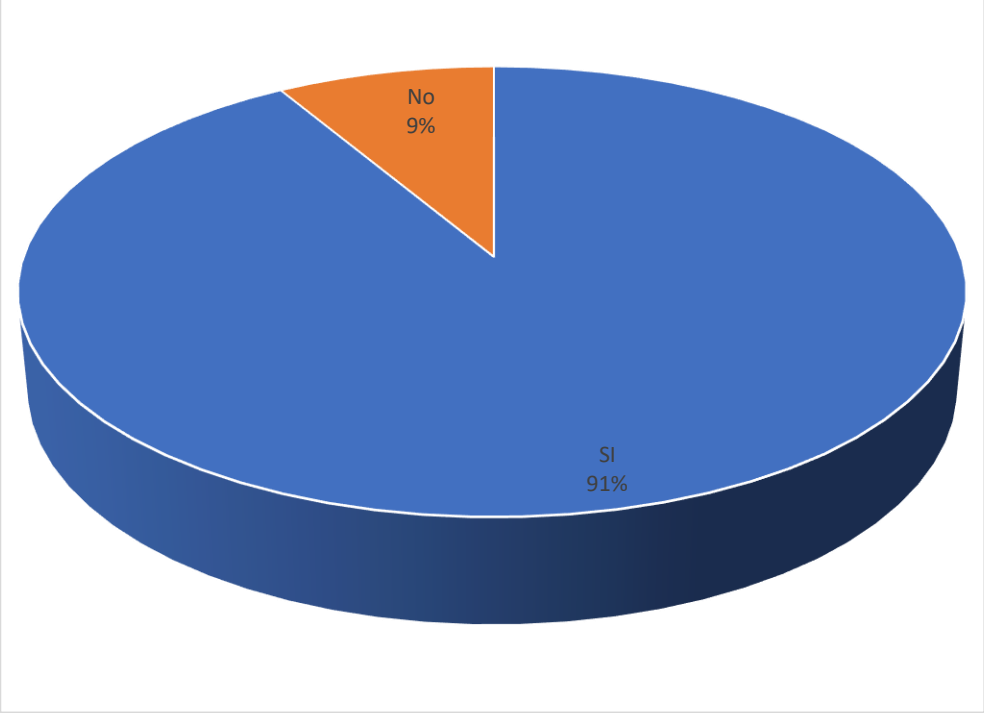

Fig. 33 Gráfico de resultados de los que consideran que la firma electrónica es amigable con el medio ambiente.

El 91% de los encuestados indican que el uso de la Firma Electrónica disminuiría el consumo de papel, esto debido que no es necesario hacer firmas autógrafas, por lo tanto, tampoco se necesitan hacer impresiones.

17. ¿Considera que la Firma Electrónica llegará a sustituir a la firma en papel?

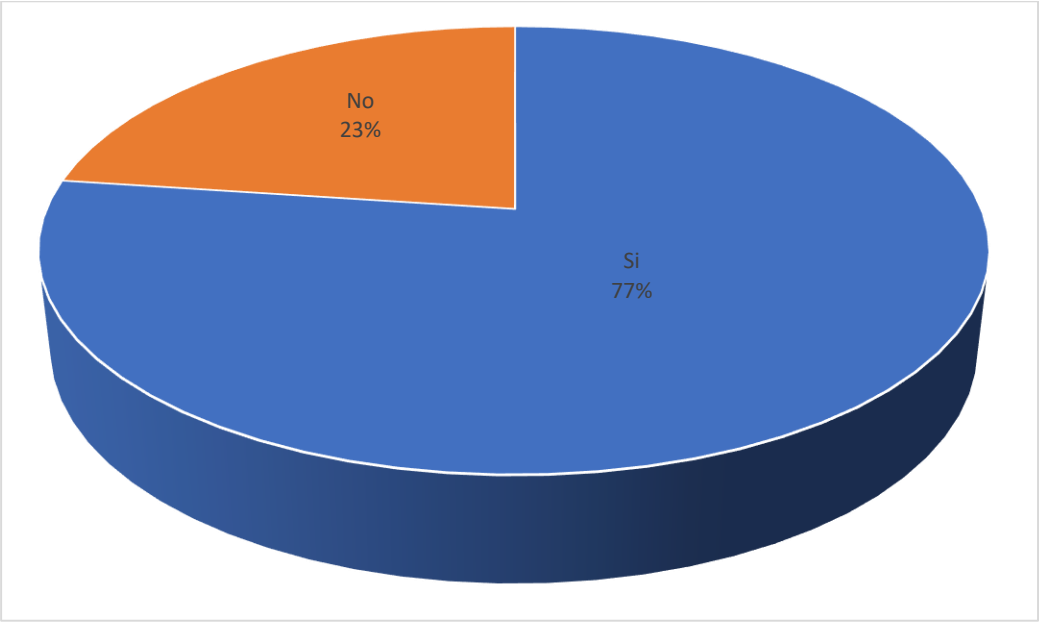

Fig. 34 Gráfico de resultados de quienes consideran que la firma electrónica sustituirá a la manuscrita.

El 77% de los encuestados consideran que la Firma Electrónica sustituirá a la firma en papel, lo cual significa que hay disposición en adoptar una tecnología para este fin.

18. ¿Cuáles serían las principales limitantes para el uso de la Firma Electrónica?

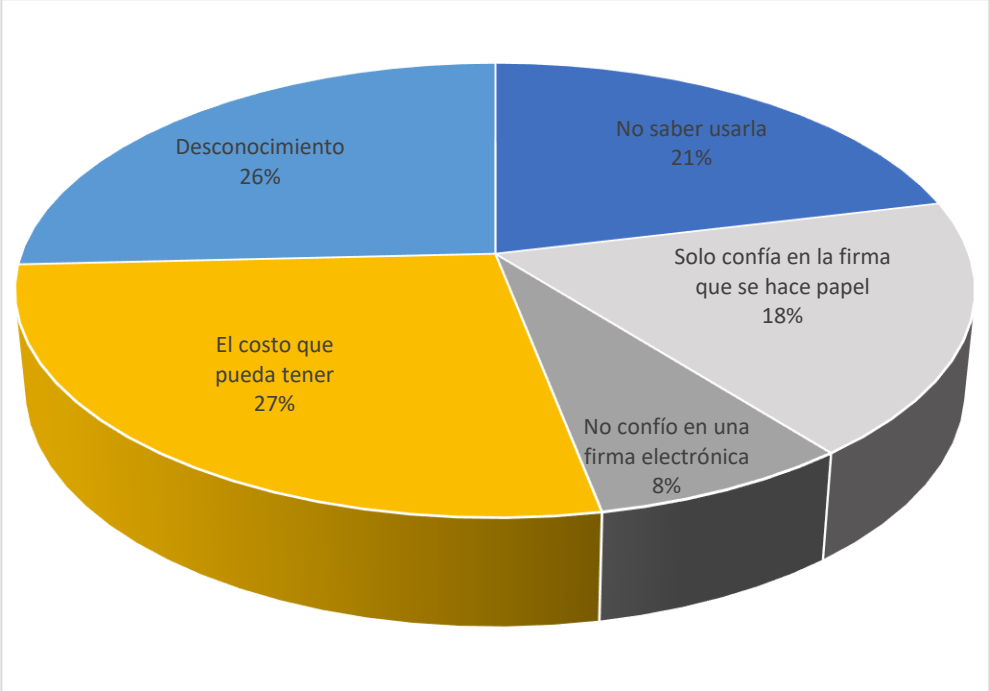

Fig. 35 Gráfico de resultados de quienes expresan porque no usarían la firma electrónica.

El 27% de los encuestados indican que la principal limitante para el uso de la Firma electrónica es el costo que puedan tener, así mismo existe un 26% que mencionan que es por desconocimiento, por lo que es importante trabajar en capacitar a las personas para cerrar esta brecha de desconocimiento.

Recomendaciones

- **Realizar un trabajo interinstitucional** que adopte un rol más protagónico en la divulgación y fortalecimiento para el uso de la firma electrónica, así como en impulsar el avance del proceso de establecimiento de la estructura necesaria para la aplicación de la firma electrónica en El Salvador, cabe enfatizar que el país ha sido de los últimos en promulgar una ley de esta naturaleza y que a la fecha la misma aún no está en aplicación.

- **Cumplir con la Legislación Local**: asegúrate de comprender y cumplir con los requisitos legales establecidos en la Ley de Firmas y Documentos Electrónicos de El Salvador. Esto incluye utilizar certificados electrónicos válidos y seguir los procedimientos adecuados para realizar firmas electrónicas.

- **Utilizar Proveedores Acreditados**: al elegir un proveedor de servicios de firma electrónica o adquirir certificados digitales, asegúrate de que estén acreditados y reconocidos por las autoridades competentes en El Salvador.

- **Garantizar la Autenticidad**: verifica la identidad del firmante y asegúrate de que esté debidamente autorizado para firmar el documento. Esto puede incluir la autenticación del firmante mediante una clave privada o el uso de un certificado digital emitido por una autoridad de confianza.

- **Pruebas de Integridad y Autenticidad**: Verificar la integridad de los documentos firmados y la autenticidad de las firmas mediante herramientas o servicios de verificación adecuados.

- **Respaldo de Documentos Firmados**: realiza copias de seguridad periódicas de los documentos firmados y guárdalos en lugares seguros.

Bibliografía

Alfred J. Menezes, P. C. (1997). *Handbook of Applied Cryptography.* Taylor & Francis Group.

Asamblea Legislativa. (2015-2021). *Ley de Firma Electrónica con sus reformas.* Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/1FCA8599-F96E-43C6-A46A-650BF091BCB7.pdf

Asamblea Legislativa. (6 de marzo de 2022). *Asamblea Legislativa avala creación de la Ley de Aplicación de la Apostilla Electrónica*. Obtenido de https://www.asamblea.gob.sv/node/11886

Asamblea Legislativa. (24 de agosto de 2022). *Reformas a Ley de Firma Electrónica permitirán a más instituciones dar servicios de certificación*. Obtenido de https://www.asamblea.gob.sv/node/12356

BID, Comunicados de presa. (7 de diciembre de 2016). Obtenido de https://www.iadb.org/es/noticias/comunicados-de-prensa/2016-12-07/el-salvador-mejorara-gestion-de-impuestos-y-aduaneras%2C11674.html

Brown, L. (2015). *Computer Security Principles and Practice.* Pearson.

CIEX El Salvador, Banco Central de Reserva. (2022). *Pago Eletrónico de los Servicios Brindados por CIEX El Salvador.* Obtenido de https://www.ciexelsalvador.gob.sv/ciexelsalvador/wp-content/uploads/2022/05/Pagos_Electronicos.pdf

Código Tributario de El Salvador. (s.f.).

E-Sign Act, Public Law EEUU, 106–229. (2000). Obtenido de https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

Grupo Seres. (17 de diciembre de 2018). *El Salvador se une a la factura electrónica*. Obtenido de https://blog.groupseres.com/el-salvador-se-une-a-la-factura-electr%C3%B3nica

Jhonny Flores, F. P. (julio de 2022). *Tax Newsletter Noticias e información oportuna sobre la temática tributaria nacional.* Obtenido de https://www2.deloitte.com/sv/es/pages/tax/articles/tax-newsletter.html

Legislativa, A. (01 de Noviembre de 2021). *www.asamblea.gob.sv*. Obtenido de www.asamblea.gob.sv: https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/1BA33F21-9FC2-4ADC-8E98-8C2629D02E83.pdf

Ministerio de Hacienda. (diciembre de 2022). Obtenido de https://www.mh.gob.sv/el-salvador-lanza-el-sistema-de-facturacion-electronica/

Ministerio de Hacienda. (15 de diciembre de 2022). *El Salvador lanza el Sistema de Facturación Electrónica*. Obtenido de https://www.mh.gob.sv/el-salvador-lanza-el-sistema-de-facturacion-electronica/

Porrúa, M. A. (25 de junio de 2022). *8 enseñanzas de la transformación digital de Estonia para América Latina y el Caribe*. Obtenido de https://blogs.iadb.org/administracion-publica/es/8-ensenanzas-de-la-transformacion-digital-de-estonia-para-america-latina-y-el-caribe/

Reglamento de Aplicación del Código Tributario. (s.f.).

Salvador, A. L. (20 de Septiembre de 2022). *Decreto Legislativo No. 487 Reformas al Código Tributario.* Obtenido de https://www.mh.gob.sv/wp-content/uploads/2022/10/Reformas-DTE-D.O.-20-09-2022.pdf

Stinson, D. R. (2006). *Cryptography Theory and Practice.* University Of Waterloo, Canada.: Chapman & Hall/CRC.