GUÍA DE IMPLEMENTACIÓN Y USO DE CERTIFICADOS Y FIRMAS DIGITALES PARA LAS MIPYMES QUE PERMITAN GARANTIZAR INTEGRIDAD, AUTENTICIDAD Y NO REPUDIO EN LOS DOCUMENTOS ELECTRÓNICOS PARA EL PROYECTO "ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE" EN DESARROLLO POR PARTE LA CÁMARA DE COMERCIO DE CASANARE E IMAGINA SOLUCIONES S.A.S.

WILLIAM FRANCISCO CASTILLO PENAGOS
HAIR DIYOSSET FERNANDO CORREA CORTES
JORGE ENRIQUE MUÑOZ SILVA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2014

GUÍA DE IMPLEMENTACIÓN Y USO DE CERTIFICADOS Y FIRMAS DIGITALES PARA LAS MIPYMES QUE PERMITAN GARANTIZAR INTEGRIDAD, AUTENTICIDAD Y NO REPUDIO EN LOS DOCUMENTOS ELECTRÓNICOS PARA EL PROYECTO "ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE" EN DESARROLLO POR PARTE LA CÁMARA DE COMERCIO DE CASANARE E IMAGINA SOLUCIONES S.A.S.

WILLIAM FRANCISCO CASTILLO PENAGOS
HAIR DIYOSSET FERNANDO CORREA CORTES
JORGE ENRIQUE MUÑOZ SILVA

Trabajo realizado para optar por título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesora
JENNY ALEJANDRA VARELA
Ingeniero de Telecomunicaciones

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2014

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C, 15 de abril de 2014

DEDICATORIA

A todas las personas que aportaron en mi proceso de formación en esta grandiosa universidad y en el desarrollo del presente proyecto de grado, especialmente a mis padres Delfirio Castillo y Marlenne Penagos por todo su apoyo, comprensión y confianza manifestados en el transcurso de esta especialización, a mis amigos Jorge Muñoz y Hair Correa compañeros de proyecto por su compromiso dado durante su desarrollo y a la ingeniera Jenny Varela por su constante ayuda en todas las etapas del presente trabajo.

WILLIAM FRANCISCO CASTILLO PENAGOS

Me gustaría agradecerte a Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño. A la UNIVERSIDAD PILOTO DE COLOMBIA por darme la oportunidad de estudiar y ser un profesional y ahora especialista. A mi directora de tesis, ingeniera Jenny Alejandra Varela por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito. Me gustaría agradecer a mis profesores durante toda la especialización porque todos han aportado con un granito de arena a mi formación, a mis amigos quienes han seguido conmigo estos pasos Jorge Muñoz y William Castillo, a mis padres Oscar Correa Villanueva y Carmen Inés Cortes quienes con su esfuerzo y apoyo siempre han estado conmigo y finalmente a mi compañera, amiga y novia Andrea Villanueva Gil quien siempre confió en mí y motivo cada paso en este camino.

HAIR DIYOSSET FERNANDO CORREA CORTES

Primero a DIOS por darme la vida y permitirme concluir este proceso tan importante para mí y mi familia. A mi madre Betty Silva Calderón quien supo transmitirme su mayor riqueza, su única y mejor lección de vida “El ejemplo”. A mi hermana Nurelsy y mi hermano Yuri Arvey, quien con su absoluta confianza hizo posible el logro de esta nueva meta. A todos y cada una de las personas, en especial al ingeniero Héctor Leónidas Duarte García y a la ingeniera Adriana Garcia por su apoyo incondicional. A todos mis docentes que aportaron en el proceso de formación, a mis compañeros William Castillo y Hair Correa. A la ingeniera Jenny Varela por su apoyo y colaboración para el presente proyecto.

JORGE ENRIQUE MUÑOZ SILVA

AGRADECIMIENTOS

Este proyecto no hubiese sido posible sin el apoyo de la **SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL**, **CERTICÁMARA**, especialmente a **Franck Delgado**, Especialista de Seguridad en Redes quien se desempeña como Coordinador Técnico SSL por su oportuna colaboración en la etapa de solicitud de certificados y firmas digitales de prueba para el desarrollo de esta guía, adicionalmente el suministro de información técnica usada como soporte complementario a las actividades desarrolladas por los autores del proyecto.

Adicionalmente a la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (SIC)**, especialmente a **Alejandro Giraldo López** quien se desempeña como Superintendente Delegado para el Control y Verificación de Reglamentos Técnicos y Metrología Legal por el suministro de los actos administrativos que autorizan a las entidades de certificación en el país, información que sirvió como alcance del proyecto y permitió realizar la búsqueda de entidades de certificación que ofrecieran no solamente funcionalidad técnica sino también completa validez jurídica en sus certificados y firmas digitales.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICOS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACUERDO DE LICENCIA[1]: un acuerdo de licencia es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas.

ALGORITMO DE CIFRADO[2]: operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro que permitirá obtener un texto cifrado y viceversa, garantizando la confidencialidad e integridad de la información contenida.

AUTENTICACIÓN[3]: Procedimiento de comprobación de la identidad de un usuario como medida de seguridad frente a posibles operaciones fraudulentas a través de la Red. La finalidad que persigue esta medida de seguridad es servir de salvaguarda para comprobar que los usuarios con los que se está interactuando son realmente quienes dicen ser. Este proceso constituye una funcionalidad característica para una comunicación segura en la Red.

CRIPTOGRAFÍA[4]: es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta irreconocible e ilegible para todo aquel que no conozca el sistema mediante el cual ha sido encriptado, haciendo indescifrable el contenido de la información que no conozca la forma de descifrar el criptograma.

---

[1] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Acuerdo de licencia. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Acuerdo_de_licencia>. [citado en 24 de marzo de 2014].

[2] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Algoritmo de cifrado. [en línea]. < http://www.inteco.es/glossary/Formacion/Glosario/Algoritmo_de_cifrado>. [citado en 24 de marzo de 2014].

[3] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Autenticación. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/AuTenticacion>. [citado en 24 de marzo de 2014].

[4] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptografía. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptografia_glosario>. [citado en 24 de marzo de 2014].

CRIPTOGRAFÍA ASIMÉTRICA[5]: se conoce como criptografía asimétrica o de clave pública al sistema de encriptación que consiste en utilizar un sistema de doble clave: Clave Pública y Clave Privada. Una de ellas, la conocida como Clave Pública, es conocida por todos y se utiliza para convertir el Texto en Claro que queremos cifrar en un Criptograma, que tan solo podrá volverse a convertir en un Texto en Claro mediante la Clave Privada, conocida solamente por la persona a la que va remitida la información cifrada mediante la Clave Pública.

CRIPTOGRAFÍA SIMÉTRICA[6]: este tipo de criptografía, utiliza una única clave para cifrar y descifrar la información. Es el sistema más clásico de cifrado. Su principal deficiencia reside en el hecho de que sólo existe una clave para convertir el texto en claro en criptograma y viceversa, lo que implica que ésta tiene que ser conocida por las dos partes que quieren intercambiar la información.

CRIPTOGRAMA[7]: se conoce como criptograma a aquel mensaje, documento o información, que se encuentra cifrado mediante cualquier sistema, y por tanto resulta ininteligible hasta que no es descifrado y convertido de nuevo en un texto en claro.

EJECUTABLE[8]: es el término genérico que se utiliza para definir a los programas o aplicaciones. Se utiliza sobre todo cuando se habla de ficheros, para diferenciarlos de aquellos que no se pueden ejecutar por sí mismos. Un ejemplo de fichero que no se puede ejecutar por sí mismo es un documento, una imagen o un fichero de sonido. Para poder abrir, visualizar o reproducir este tipo de ficheros se necesita un ejecutable. Los ejecutables tienen las extensiones "EXE" Y "COM".

---

[5] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptografía Asimétrica. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptografia_Asimetrica_glosario>. [citado en 24 de marzo de 2014].

[6] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptografía Simétrica. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptografia_Simetrica_glosario>. [citado en 24 de marzo de 2014].

[7] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptograma. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptograma_glosario>. [citado en 24 de marzo de 2014].

[8] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Ejecutable. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Ejecutable>. [citado en 24 de marzo de 2014].

EVIDENCIA ELECTRÓNICA[9]: las evidencias electrónicas son datos que de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática. Tienen la función de servir como prueba física (por encontrarse dentro de un soporte) de carácter intangible (no modificables) en las investigaciones informáticas.

HSM[10]: acrónimo de las siglas en inglés de Hardware Security Module, Módulo de Seguridad de Hardware. Es un dispositivo seguro de creación de firma electrónica el cual consiste en un hardware criptográfico diseñado especialmente para generar, almacenar y utilizar claves tanto simétricas como asimétricas.

HTTPS[11]: protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés Hypertext Transfer Protocol Secure, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. Dicho en otras palabras, es la versión segura de HTTP.

LOG[12]: un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

---

[9] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Evidencia Electrónica. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Evidencia_Electronica_glosario>. [citado en 24 de marzo de 2014].

[10] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - HSM. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/HSM_Glosario>. [citado en 24 de marzo de 2014].

[11] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - HTTPS. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/HTTPS>. [citado en 24 de marzo de 2014].

[12] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Log. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Log_glosario>. [citado en 24 de marzo de 2014].

PROTOCOLO[13]: conjunto de reglas acordadas entre dos o más agentes para realizar una tarea común como por ejemplo comunicarse.

SERVIDOR[14]: desde el punto de vista puramente técnico puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él. Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla, como podría ser el alojamiento de sitios web.

SISTEMA OPERATIVO[15]: un sistema operativo (SO) es un conjunto de programas destinados a permitir la comunicación del usuario con un dispositivo electrónico. Se encuentra instalado en la gran mayoría de los aparatos electrónicos que se utilizan en nuestra vida diaria (teléfonos móviles, videoconsolas, ordenadores).

SOFTWARE[16]: se considera software a todas aquellas partes inmateriales que forman un sistema informático. Se trata de los programas, aplicaciones y sistemas operativos que hacen posible el uso del equipo. Cada programa o aplicación de software puede definirse como la serie de instrucciones dirigidas al ordenador para que ejecute diversas acciones.

SUPLANTACIÓN DE IDENTIDAD[17]: es la actividad maliciosa en la que un atacante se hace pasar por otra persona. Los motivos pueden ser el fraude, acoso o cyberbulling.

---

[13] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Protocolo. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Protocolo>. [citado en 24 de marzo de 2014].

[14] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Servidor. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Servidor_Glosario>. [citado en 24 de marzo de 2014].

[15] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Sistema Operativo. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Sistema_Operativo1>. [citado en 24 de marzo de 2014].

[16] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos -Software. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Software1>. [citado en 24 de marzo de 2014].

[17] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Suplantación de identidad. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/suplantacion_de_identidad_glosario>. [citado en 24 de marzo de 2014].

TIMESTAMPING[18]: con el término "timestamping", cuyo significado en español es "sellado de tiempo", se hace referencia a un servicio electrónico que permite comprobar la existencia de una serie de datos y la integridad de los mismos, gracias a la incorporación de la fecha y hora en el documento electrónico.

TOKEN CRIPTOGRÁFICO[19]: dispositivo de seguridad que utiliza un usuario para autenticarse al acceder a un sistema informático. Suele tener una pantalla donde se muestra un código de acceso que, junto con una contraseña, el usuario debe introducir en un formulario de acceso, para probar su identidad de un cliente ante un servicio web como puede ser la banca en línea.

URL[20]: las siglas URL (Uniform Resource Locator) se corresponden con la expresión "Localizador Uniforme de Recurso" que hace referencia a la dirección que identifica un sitio web en Internet, y que como característica general, se puede visualizar en la barra de direcciones del navegador iniciando por defecto como "http". Las URLs permiten tener acceso a los recursos informáticos gracias a la dirección única que permite localizar el sitio web por el que se pretende navegar.

USUARIO[21]: sujeto o proceso automatizado para acceder a datos o recursos.

VULNERABILIDAD[22]: fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar. Estos errores de programación y/o diseño permiten que un tercero se aproveche de ellos para realizar acciones tales como ataques, intrusiones o cualquier otro uso indebido.

---

[18] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Timestamping. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Timestamping_glosario>. [citado en 24 de marzo de 2014].

[19] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Token criptográfico. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/token_criptografico>. [citado en 24 de marzo de 2014].

[20] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - URL. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/URL>. [citado en 24 de marzo de 2014].

[21] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Usuario. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Usuario_Glosario>. [citado en 24 de marzo de 2014].

[22] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Vulnerabilidad. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Vulnerabilidad_Glosario>. [citado en 24 de marzo de 2014].

INTRODUCCIÓN

La constante evolución de las nuevas tecnologías que ofrecen un universo de posibilidades para la realización de todo tipo transacciones electrónicas, las cuales se han incrementado y esa tendencia es cada vez más creciente, de aquí que el concepto e integración de firma digital son necesarios para garantizar la autenticidad, la integridad y el no repudio de dichas transacciones a través de medios de transmisión no seguros como internet, que a su vez, representa nuevos riesgos y constantes amenazas que hoy en día se logran tipificar como delitos informáticos que afectan derechos consagrados en la Constitución Colombiana, como lo es, la intimidad.

Los diferentes tipos de transacciones electrónicas brindan beneficios como reducción de tiempos, costos de operación, eliminación de las distancias y hasta las fronteras geográficas, pero a su vez, representan riesgos que deben ser tratados mediante herramientas ofrecidas actualmente por la criptografía, como lo son los certificados y firmas digitales, que protegen y aseguran tanto los sitios web que prestan cualquier tipo de transacción electrónica como los diferentes archivos de usuario en formato electrónico que soportan las mismas, los que poseen valor probatorio y requieren que se garantice su confidencialidad, integridad, autenticidad y no repudio.

1. JUSTIFICACIÓN

El Gobierno Nacional mediante la Ley 590 de 2000, promueve el apoyo a la creación de empresas, mediante el fomento de la cultura empresarial, por otra parte con las leyes 905 de 2004 y 1014 de 2006 gestionan el desarrollo integral de las micro, pequeñas y medianas empresas para la generación de empleo, el desarrollo regional, la integración entre sectores económicos, el aprovechamiento productivo de pequeños capitales y la capacidad empresarial, entre otros.

La formulación de la Política Nacional de Competitividad y Productividad se basa en cinco estrategias para mejorar la competitividad del país, planteadas en la Comisión Nacional de Competitividad:

- ✓ Desarrollo de sectores o clúster de clase mundial.
- ✓ Salto en la productividad y el empleo.
- ✓ Formalización empresarial y laboral.
- ✓ Fomento a la ciencia, la tecnología y la innovación.
- ✓ Estrategias transversales de promoción de la competencia y la inversión.

Por su parte, el Plan Regional de Competitividad de Casanare – Casanare Productivo de La Comisión Regional de Competitividad, propone como visión que el Departamento de Casanare en el año 2021 será reconocido como epicentro económico de la Orinoquía, por su impacto en los mercados nacionales e internacionales, altos niveles de productividad y competitividad en agroindustria y turismo, soportados en el fortalecimiento gremial, la innovación tecnológica, la generación de conocimiento, la identidad de la cultura casanareña, el respeto de su entorno ambiental, los valores éticos y morales, y una alta calidad de vida de sus habitantes. Por otra parte propone la ciencia, innovación, desarrollo tecnológico, la infraestructura y TIC para la productividad como objetivos transversales (cimientos) para la competitividad.

La Administración Departamental de Casanare en su Plan de Desarrollo “La que gana es la gente 2012 – 2015”, plantea fomentar la formación de una cultura de investigación para la ciencia, tecnología

e innovación en todos los niveles de educación, su articulación con los sectores productivos y su proyección hacia la productividad y la competitividad, fortaleciendo el programa ONDAS como estrategia pedagógica. De igual forma propone promover la consolidación de las cadenas productivas en el Departamento para hacerlas más productivas y competitivas, implementando el Plan Regional de Competitividad, las Alianzas para la Prosperidad Social y la Agenda Regional de Ciencia y Tecnología con mecanismos de asociaciones público privadas e "incrementar la productividad y competitividad de la economía del Departamento, para que todas y todos los casanareños tengan la oportunidad de participar de sus beneficios, fomentando la generación del nuevo conocimiento, investigación aplicada, transformación productiva, desarrollo tecnológico e innovación del sector empresarial y productivo".

Mediante el Programa Fortalecimiento en Ciencia, Tecnología e Innovación para un crecimiento sostenible, se plantea fomentar las TIC, como una nueva fuerza capaz de impulsar los cambios socioeconómicos, que se articulan con los ecosistemas digitales, ecosistemas Gobierno en Línea, para estimular e inspeccionar espacios de formación de una comunidad más activa, teniendo acceso a la conectividad digital, conexión a Internet en los entes públicos que permitan desarrollar acciones destinadas a fortalecer la infraestructura tecnológica en sus principales componentes como son: hardware, software, redes, conectividad y comunicaciones.

Específicamente para el subprograma: Estrategias digitales para el Departamento de Casanare, cuyo objetivo es fomentar el uso de las TIC en el Departamento, creando puntos virtuales para el acceso a la información por parte de la comunidad en general, se propone como meta desarrollar un sistema departamental de información fortalecido, implementado y en línea.

El constante crecimiento poblacional ha traído modificaciones en las estructuras productivas y sociales. Las formas económicas tradicionales del Departamento, fundamentadas en la prestación de servicios administrativos, se han diversificado ampliamente con preponderancia de la prestación de servicios como la hotelería, los restaurantes, los servicios financieros, el auge de la construcción y el nacimiento de una incipiente industrialización. Consecuentemente, la estructura ocupacional se ha

modificado con el surgimiento de nuevas ocupaciones, categorías ocupacionales y ramas de actividad que antes no existían.

La Cámara de Comercio de Casanare, en su Estrategia Corporativa, propone generar estrategias para la formalización del 90% de las empresas presentes en el Departamento de Casanare, contribuyendo así a la consolidación de Casanare como el departamento llanero más próspero y competitivo mediante la promoción del desarrollo regional y la construcción del tejido empresarial.

Es importante mencionar también que diversos estudios aplicados al sector empresarial en el Departamento, han generado un conocimiento de sus características y problemáticas relacionadas con los índices de productividad y competitividad fundamentada en la aplicación de las Tecnologías de la Comunicación y la Información por parte de los sectores productivos. La incorporación y apropiación de las TIC en las empresas en particular y en la sociedad en general, las ha convertido en una variable determinante para el desempeño y la competitividad, al punto de considerar que se está presenciando la aparición de una nueva economía digital.

La desintegración de los sectores productivos y de las instituciones públicas y privadas, es una realidad que imposibilita el desarrollo económico de las micro, pequeñas y medianas empresas, debido a la falta de unificación de estrategias y al desconocimiento del mercado existente, para el establecimiento de alianzas empresariales que permitan potenciar la capacidad productiva de los sectores económicos.

Si bien existen iniciativas tecnológicas que permiten a los empresarios y comerciantes promocionar sus productos y servicios en línea, es necesario fortalecer e incrementar su impacto socioeconómico en los sectores productivos del Departamento de Casanare.

En la actualidad, los establecimientos comerciales que prestan el servicio de domicilios reciben sus solicitudes por vía telefónica, lo que generalmente ocasiona falta de control en las ordenes, debido a la inexistencia de un registro organizado que permita establecer el estado de cada una de las solicitudes.

La publicación aislada de eventos sociales, promociones, ofertas especiales, convocatorias y en general la invitación a reuniones sobre temáticas específicas, no es una técnica de difusión efectiva, debido a que el público objetivo no siempre recibe el mensaje, por tanto se plantea la creación de un sitio exclusivo para la publicación de eventos de interés general.

La formalización de la actividad económica para los empresarios y comerciantes del Departamento, es uno de los principales factores en el Plan Estrategia Corporativa 2012 – 2022 de la Cámara de Comercio de Casanare. La publicación de un directorio empresarial para el Departamento, en el cual se pueda consultar de forma rápida la información de identificación de cada uno de los establecimientos comerciales formalizados, incentivará el proceso de formalización por parte de los empresarios y comerciantes informales, debido a la publicidad adicional que tendrán por este medio.

A pesar de la existencia de una herramienta en línea que permite la publicación de hojas de vida y el registro de ofertas de empleo por parte las empresas, no existe una bolsa de empleo específica para el Departamento de Casanare, donde los empresarios puedan identificar rápidamente y de forma confiable los perfiles que apliquen para las convocatorias vigentes.

Según lo establecido en el artículo 166 del Decreto 019 del 10 de enero de 2012, las Cámaras de Comercio deben realizar los procesos de solicitud, inscripción y actualización anual en el Registro Nacional de Turismo. La inexistencia de un sitio especializado en el turismo, que permita promover el sector a nivel nacional e internacional, impide a los turistas el acceso a información completa sobre los establecimientos prestadores de estos servicios y sobre la diversidad natural y cultural que posee el Departamento de Casanare.

La información geoespacial del Departamento de Casanare relacionada con la ubicación de cada uno de los establecimientos comerciales no se encuentra disponible en línea, por lo cual se dificulta la localización mediante un sistema de información geográfico especializado en la búsqueda y clasificación de dichos establecimientos.

Ahora bien, los empresarios y comerciantes del Departamento, carecen de un espacio digital, que les permita establecer relaciones empresariales, mediante la consolidación de grupos y alianzas estratégicas para el mejoramiento de la productividad y competitividad, además de permanecer informados sobre el estado de la actividad empresarial del Departamento, para identificar fácilmente oportunidades que les permita aportar en el mejoramiento del desarrollo social y económico de Casanare.

La industria y el comercio son actividades propias del sector privado, al cual le corresponde asignar inversiones en aquellos sectores que presentan una mayor rentabilidad y tengan un mayor beneficio económico y social. Por su parte al Estado y a las demás instituciones que han incursionado en el Departamento de Casanare les corresponden suministrar las herramientas propias para que el sector empresarial sea cada vez más competitivo.

El contexto expuesto habituado a los constantes avances en la tecnología a su vez representa riesgos inherentes a los ambientes digitales, que se evidencian en las nuevas modalidades de delitos informáticos como el Fishing, la suplantación de identidad, interceptación (Eavesdropping) sobre medios de información tanto cifrada como no cifrada, entre otros. Surgen todo un nuevo mundo para los ciber delincuentes que tienen motivaciones como la ausencia de daños a su integridad física, ingenuidad de los usuarios y la falta de seguridad; quienes no solo buscan motivaciones económicas y pueden mediante diversas modalidades delictivas lograr afectación a la integridad, autenticidad y no repudio de la información.

La firma digital ofrece ventajas inmejorables como la reducción del riesgo legal mediante ahorro de largas, complejas e inciertas etapas probatorias en trámites judiciales y administrativos para demostrar que la firma electrónica es efectivamente equivalente, se evitan desplazamientos y colas de las personas involucradas en los procesos de firma, los documentos firmados pueden recogerse y archivarse en formato digital, sin tener que trasladarse nunca al papel, la distancia deja de ser un problema, por lo que cualquier documento quedará firmado por todas las partes, mucho más rápidamente, y de forma más eficiente que si se firmara a mano, al quedar archivados en formato digital, su posterior localización también es mucho más fácil y rápida, gracias a las herramientas

informáticas de búsqueda, es una tecnología más segura que la firma manuscrita, por lo que suplantar una identidad resulta mucho más complejo, ahorros de costes tangibles, evitando envíos, o reduciendo el consumo de tinta o papel.

Las ventajas de la firma electrónica respecto a la firma manuscrita son evidentes, de aquí que cualquier entidad u organización que haga uso de la firma manuscrita, puede obtener grandes beneficios en ahorro de costes y mejora de servicio, rapidez y tiempo de respuesta, a través de su aplicación.

2. PLANTEAMIENTO DEL PROBLEMA

¿Cómo garantizar la integridad, autenticidad y no repudio de los archivos en formatos digitales generados por las Micro, Pequeñas y Medianas Empresas (MIPYMES) del departamento de Casanare que formen parte del proyecto “ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE” en desarrollo por parte de La Cámara de Comercio de Casanare e Imagina Soluciones S.A.S.?.

3. OBJETIVO GENERAL

Elaborar una guía de implementación y uso de certificados y firmas digitales para archivos en formatos digitales generados por las Micro, Pequeñas y Medianas Empresas (MIPYMES) del departamento de Casanare pertenecientes al proyecto "ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE" en desarrollo por parte de La Cámara de Comercio de Casanare e Imagina Soluciones S.A.S.

3.1. OBJETIVOS ESPECÍFICOS

- ✓ Capturar los requerimientos técnicos para la implementación de certificados y firmas digitales.
- ✓ Establecer el contexto jurídico para la implementación de certificados y firmas digitales en Colombia.
- ✓ Ejecutar una estrategia de capacitaciones que permitan fortalecer las capacidades en el uso de certificados y firmas digitales.
- ✓ Crear y ejecutar pruebas piloto para evaluar la guía de implementación de certificados y firmas digitales.

4. ¿A QUIÉN VA DESTINADA ESTA GUÍA?

Esta guía está orientada en principio a todas las Micro, Pequeñas y Medianas Empresas (MIPYMES) del Departamento de Casanare que formen parte del proyecto "ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE" en desarrollo por parte de La Cámara de Comercio de Casanare e Imagina Soluciones S.A.S., sin embargo puede ser consultada e implementada por cualquier persona natural o jurídica que desee conocer qué es una firma y/o certificado digital y que transacciones pueden realizar con esta herramienta tecnológica siempre y cuando se haga mención explícita a los autores de la presente guía sin realizar ningún tipo de modificación, copia o alteración sin previa autorización.

5. MARCO TEÓRICO

5.1. DOCUMENTO ELECTRÓNICO

Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares[23].

5.1.1. Clases de documento electrónico. Los documentos electrónicos se clasifican de acuerdo a determinados criterios como por ejemplo:

- ✓ Por su forma de creación. Que se divide en documentos nativos electrónicos, cuando han sido elaborados desde un principio en medios electrónicos y permanecen en estos durante toda su vida o documentos electrónicos digitalizados, cuando se toman documentos en soportes tradicionales (como el papel) y se convierten o escanean para su utilización en medios electrónicos.
- ✓ Por forma y formato. Ya que encontramos documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

5.1.2. Características del documento electrónico. Los documentos electrónicos deben poseer ciertas características:

- ✓ Autenticidad. Que pueda demostrarse que el documento es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el momento que se afirma.

[23] Congreso de Colombia. Ley 527 de 2009. Artículo 2°. La definición de documento electrónico corresponde con la de Mensaje de Datos

- ✓ Integridad. Hace referencia al carácter completo e inalterado del documento electrónico. Es necesario que un documento esté protegido contra modificaciones no autorizadas. Las políticas y los procedimientos de gestión de documentos deben decir qué posibles anotaciones o adiciones se pueden realizar sobre el mismo después de su creación y en qué circunstancias se pueden realizar. No obstante, cualquier modificación que se realiza debe dejar constancia para hacerle su seguimiento o debe ser inherente a su proceso de transmisión.
- ✓ Fiabilidad. Su contenido representa exactamente lo que se quiso decir en él. Es una representación completa y precisa de lo que da testimonio y se puede recurrir a él para demostrarlo.
- ✓ Disponibilidad. Se puede localizar, recuperar, presentar, interpretar y leer. Su presentación debe mostrar la actividad que lo produjo. El contexto de los documentos debe ser suficientemente claro y contener la información necesaria para la comprensión de las operaciones que los crearon y usaron.

5.1.3. Estructura lógica del documento electrónico. El concepto de estructura "está relacionado con la forma en que se registra el documento, lo que incluye la utilización de signos, el diseño, el formato, el soporte, etc." En el caso de los documentos electrónicos, se distingue entre una estructura física y una estructura lógica, la estructura física de un documento electrónico es variable y depende del hardware y del software, es decir del equipo que se utilizó y el programa en el que se creó; su estructura lógica (es decir, la relación entre las partes que lo componen) lo hace inteligible.

- ✓ Contenido. Es la materia del documento electrónico, es decir el conjunto de datos e información del documento. Dependiendo del formato en el que se cree será la forma definitiva del documento.
- ✓ Firma del documento electrónico. El artículo 7 de la Ley 527 de 1999 establece que "cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación; b) Que el método sea tanto confiable como

apropiado para el propósito por el cual el mensaje fue generado o comunicado". En Colombia se han reglamentado dos mecanismos de firma: la firma electrónica y la firma digital.

- ✓ Metadatos del documento electrónico. Los metadatos son los datos que describen el contexto, el contenido y la estructura de los documentos del archivo y su gestión a lo largo del tiempo.

  Los metadatos se pueden clasificar según su finalidad, en categorías:

  - ➢ Metadatos de información: Que ofrecen información útil para la identificación de la entidad o del documento, como puede ser el procedimiento al que pertenece o el organismo asociado.
  - ➢ Metadatos de seguridad: Que permiten definir todos los parámetros del documento que tengan relación con el control, seguridad y acceso del documento. Entre estos metadatos están los de control de acceso.
  - ➢ Metadatos de trazabilidad: Que informan acerca de todas las acciones que se han realizado sobre el documento. También permiten la localización física del documento.
  - ➢ Metadatos de firma: Entre los que se encuentran los metadatos que guardan la información relativa a las diferentes firmas que se han realizado sobre el documento. A su vez, se guarda la identificación de cada firmante, la fecha en la que se firmó y la propia firma electrónica.
  - ➢ Metadatos de estampado cronológico. Que son los encargados de guardar toda la información relacionada con el estampado cronológico aplicado al documento. La identificación del firmante, el tipo de estampado o la fecha exacta del estampado son algunos de los metadatos de esta categoría.

5.1.4. Formato de documento electrónico

- ✓ Consideraciones. Se entiende por formato la manera en que los datos están contenidos en un documento electrónico en el momento de su creación y la forma en que han sido codificados.

  Es recomendable que los formatos de los documentos electrónicos se ajusten a los formatos establecidos en las normas internacionales.

La determinación de formatos idóneos para la conservación a largo plazo de información, pasa por evaluar el nivel de cumplimiento de los siguientes aspectos:

- Cifrado: un formato de conservación no debe contener datos cifrados, cuya interpretación y buena lectura dependa de algoritmos o claves externas al propio documento.
- Compresión: los algoritmos de compresión deben ser públicos, gratuitos y no estar sujetos al pago por uso.
- Contenido multimedia: no es recomendable el uso de audio y video, cuya reproducción implique el uso de programas externos o de dispositivos y equipos específicos.
- Referencias a contenido externo: no debe haber referencias a contenido externo, ya que la modificación del contenido o de la propia referencia puede alterar el documento o hacerlo poco entendible.
- Código ejecutable: No se debe admitir la ejecución de código JavaScript o de cualquier otro tipo de fichero o programa.
- Fuentes: las fuentes de representación de los caracteres o tipo de letra del documento deben estar en el mismo, siendo fuentes abiertas que no requieran de ningún tipo de licencia.

La elección del formato se realizará de acuerdo al tipo de información que se vaya a manejar, primando la finalidad para la cual fue definido cada uno.

Se podrán utilizar otros formatos cuando existan particularidades que lo justifiquen o sea necesario para asegurar el valor como prueba a presentar del documento electrónico y su confiabilidad como evidencia electrónica de las actividades y procedimientos, en caso de tener que convertirlo a otro formato. Para la elección del formato a utilizar debe tenerse en cuenta que cada uno de ellos podrá ser usado de acuerdo al tipo de información que se vaya a consignar, debiendo primar la finalidad para la cual cada uno de ellos fueron definidos.

- ✓ Formatos admitidos. Todo tipo de archivo electrónico elaborado a partir de cualquier tipo de software como procesadores de texto, hojas de cálculo, presentaciones, imágenes, video, etc.

5.2. CERTIFICACIÓN DIGITAL[24]

Es un sistema que garantiza la identidad y otras cualificaciones de una persona que actúa a través de una red informática, un sistema de información, y en general, cualquier medio de comunicación y/o información digital.

La certificación digital permite garantizar:

- ✓ Identidad y capacidad de las partes que tratan entre sí sin conocerse (emisor y receptor del mensaje).
- ✓ Confidencialidad de los contenidos de los mensajes (ni leídos, ni escuchados por terceros).
- ✓ Integridad de la transacción (no manipulada por terceros).
- ✓ Irrefutabilidad de los compromisos adquiridos (no repudiación).

5.3. FIRMA DIGITAL[25]

Dado que suelen presentarse confusión con los términos "firma digital" y "firma electrónica" se hará la aclaración, en general se suele considerar que un esquema de firma digital es un esquema basado en determinadas propiedades matemáticas que permiten demostrar la autenticidad de un documento electrónico o un mensaje de datos; mientras que una firma electrónica es un medio electrónico que indica que una persona es responsable del contenido de un documento electrónico.

La firma digital es equivalente a la firma manuscrita y permite incorporar las garantías básicas de seguridad de autenticidad, confidencialidad, integridad y no repudio. "Se entenderá como un valor

[24] Certicamara. ¿Qué es certificación digital? [en línea]. Certicamara, Validez y seguridad jurídica electrónica, 2013 [Fecha de consulta: 07 de septiembre]. Disponible en http://web.certicamara.com/soporte_interna_faqs_2.aspx
[25] Certicamara. ¿Qué es firma digital? [en línea]. Certicamara, Validez y seguridad jurídica electrónica, 2013 [Fecha de consulta: 07 de septiembre]. Disponible en http://web.certicamara.com/soporte_interna_faqs_2.aspx

numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación"[26].

Las firmas digitales, son documentos electrónicos emitidos por entidades certificadores previamente autorizadas bajo la Ley 527 de 1999 y que permiten identificar de manera inequívoca a una persona en medios digitales. Adicionalmente califica tanto su actividad profesional, como el rol que desempeña en el momento.

5.3.1. Características de la firma digital. La certificación de Firma Digital permite garantizar:

- ✓ Identidad y capacidad de las partes que tratan entre sí sin conocerse (emisor y receptor del mensaje).
- ✓ Integridad de la transacción (verificar que la información no fue manipulada).
- ✓ Irreductibilidad de los compromisos adquiridos (no repudiación).
- ✓ Confidencialidad de los contenidos de los mensajes (solamente conocidos por quienes estén autorizados).

5.3.2. Atributos jurídicos de la firma digital. Mediante la utilización de certificados digitales es posible firmar digitalmente información electrónica obteniendo los siguientes atributos jurídicos:

- ✓ Autenticidad permite garantizar la identidad del emisor de un mensaje y/o el origen del mismo, y tener la plena seguridad que quien remite el mensaje es realmente quien dice ser.
- ✓ Integridad garantiza que el mensaje de datos o información electrónica no haya sido alterado ni modificado.

[26] Ley 527 de 1999: Artículo 20. Definiciones Tag C: Firma Digital http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999.html

- ✓ No repudio el emisor no podrá negar el conocimiento de un mensaje de datos y de los compromisos adquiridos a partir de éste.

Adicionalmente algunas tecnologías de certificación digital permiten el cifrado de mensajes de datos incorporando un atributo adicional:

- ✓ Confidencialidad permite garantizar que un mensaje de datos no pueda ser conocido sino por su emisor y los receptores deseados. El contenido del mensaje de datos no podrá ser conocido por ningún tercero no autorizado. Las firmas digitales generadas mediante el uso de certificados digitales emitidos por las autoridades avaladas cuentan con el mismo valor probatorio y fuerza obligatoria de una firma manuscrita.

5.3.3. Clasificación de las firmas digitales. Las firmas digitales se puedes clasificar de la siguiente manera:

- ✓ Implícitas: Son las firmas que se incluyen en el mismo fichero que el mensaje.
- ✓ Explicitas: Son las firmas que se añaden al mensaje, si bien no forman parte del mismo fichero electrónico.
- ✓ Privadas: Son aquellas firmas que permiten identificar al firmante cuando se comparte un secreto con este último.
- ✓ Publicas: Son las firmas para las que se puede probar la identidad del firmante de modo que éste negar su autenticidad.
- ✓ Revocables: Una firma se dice que es revocable si el firmante puede negar que tal firma le pertenece.
- ✓ Irrevocables: Son las firmas para las que se puede probar la identidad del firmante de modo que este no pueda negar su autenticidad.

5.4. CERTIFICADO DIGITAL[27]

Un certificado digital es la versión digital de un certificado ordinario en el que se garantiza que la clave pública y el resto de información contenida en el mismo pertenecen al mismo usuario que se especifique en dicho certificado. La validez de dicha información está garantizada por una entidad reconocida y autorizada conocidas como autoridades de certificación (**CA, Certification Authority**), por ende un certificado digital es el equivalente electrónico a un documento de identidad. El certificado digital asocia una clave criptográfica a una identidad, de tal forma que esta quede fehacientemente ligada a los documentos electrónicos sobre la que se aplica.

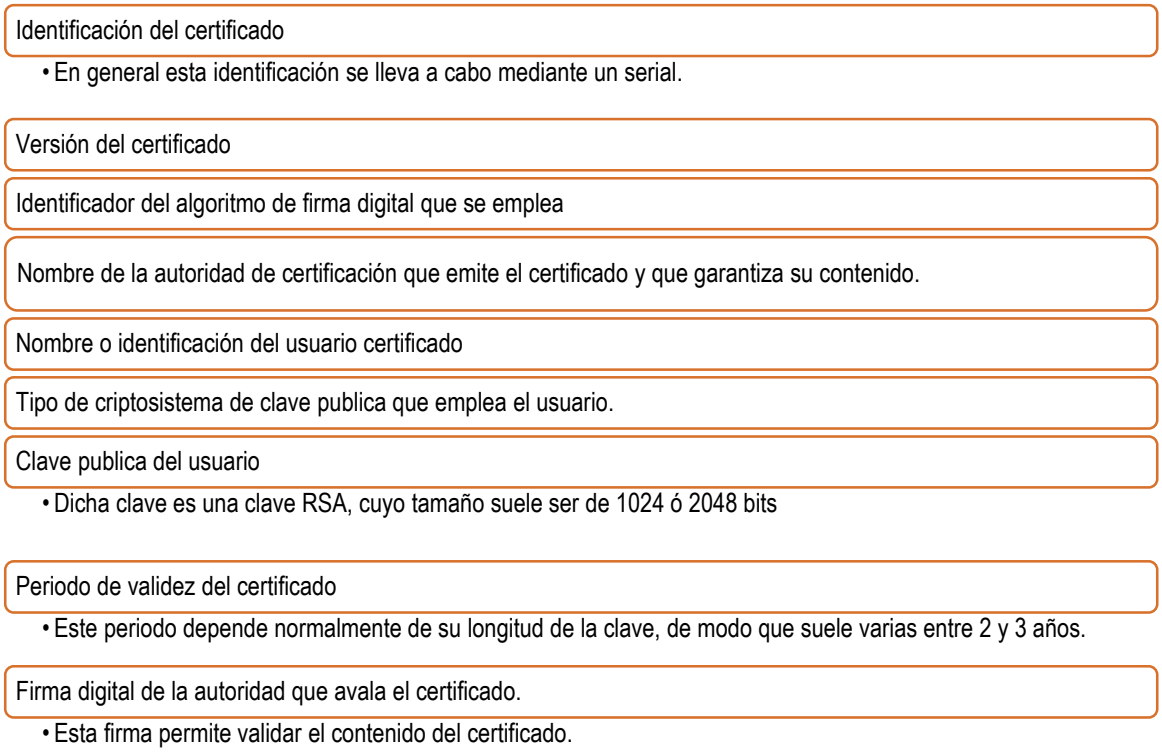
Los certificados son documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. Permiten verificar que una clave pública específica pertenece efectivamente a un individuo o entidad. Los certificados, de esta forma, ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

La norma del certificado digital se conoce como **X.509** y está diseñada para permitir que cualquier usuario pueda verificar la autenticidad de los datos contenidos en el mismo y que hacen referencia a su propietario. En particular, su clave pública y el periodo de validez de la misma. La versión actualmente empleada de este certificado es la v3 y data de junio de 1996 (ISO/ECI, 2000).

Los certificados digitales contienen, entre otra, la siguiente información:

[27] Certicamara. ¿Qué es un certificado digital? [en línea]. Certicamara, Validez y seguridad jurídica electrónica, 2013 [Fecha de consulta: 07 de septiembre]. Disponible en http://web.certicamara.com/soporte_interna_faqs_2.aspx

Figura 1. Información contenida en el certificado digital



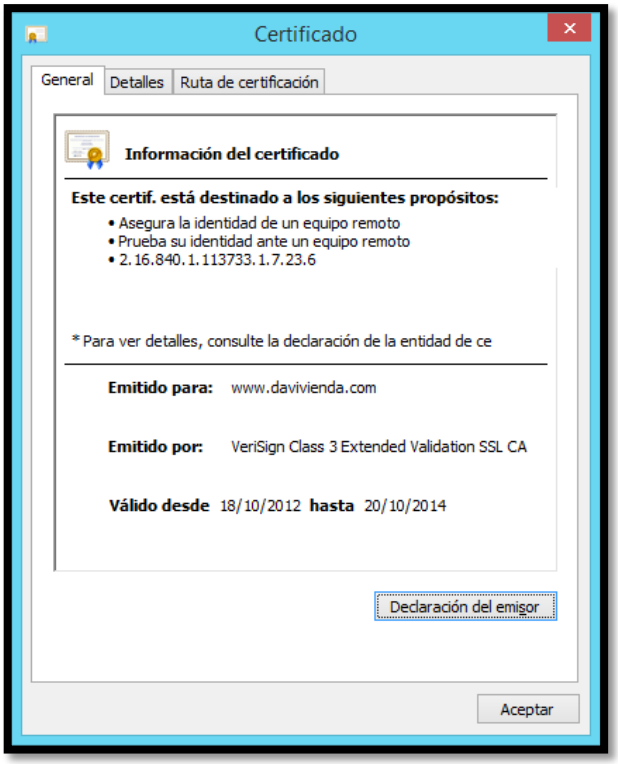
Fuente: Fuster Sabater, Amparo. Hernández Encinas, Luis. Martin Muñoz, Agustín. Montoya Vitini, Fausto. Muñoz Masque. Jaime. Criptografía protección de datos y aplicaciones: Guía para estudiantes y profesionales. México: Alfaomega grupo editor, 2013. 250p

Documento digital de identidad emitida a un individuo. El Certificado Digital permite a su titular:

- ✓ Identificarse ante terceros.
- ✓ Firmar documentos electrónicamente.
- ✓ Evitar la suplantación de la identidad.
- ✓ Proteger la información transmitida.
- ✓ Garantizar la integridad de la comunicación entre las partes.

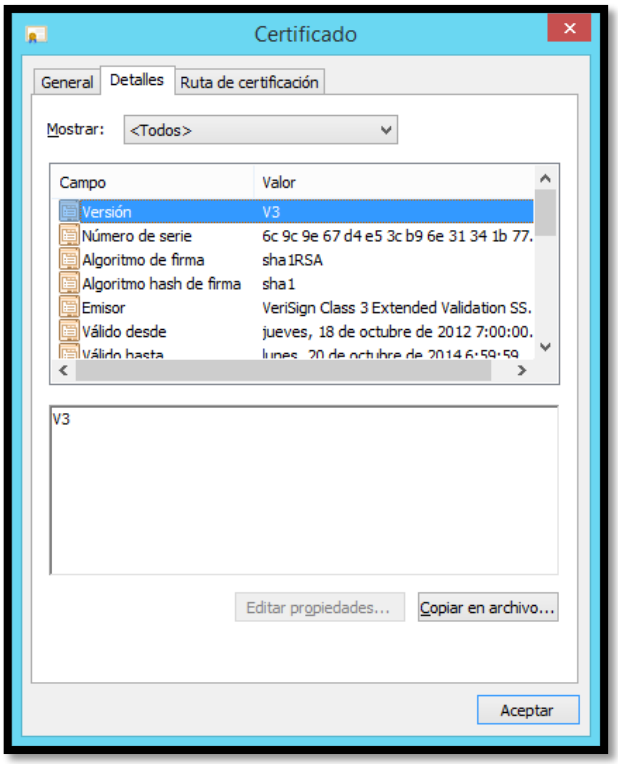
5.4.1. Información contenida en certificado digital. En este ejemplo podemos observar la información del certificado utilizado para la navegación segura en portales de banca electrónica, para este ejemplo específico el Banco Davivienda.

Figura 2. Ejemplo de certificado digital banco Davivienda, General



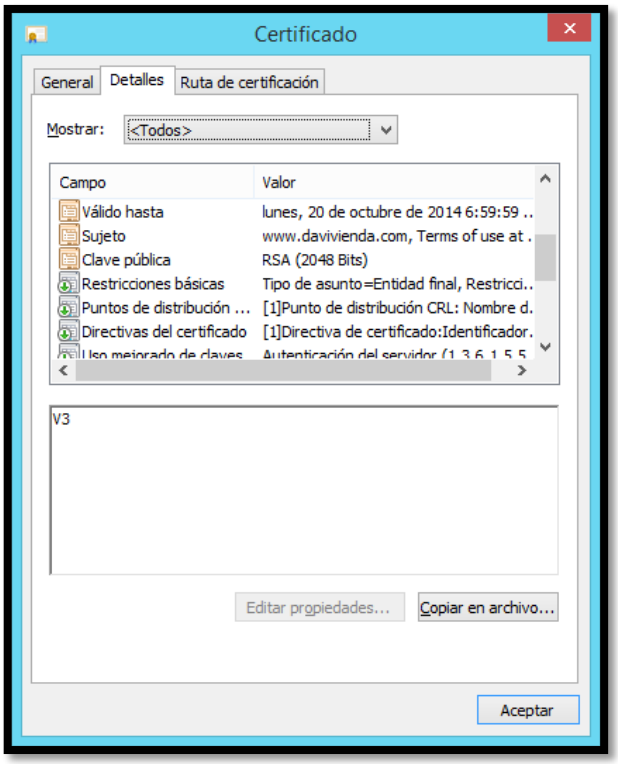
Fuente: Autores del proyecto.

Figura 3. Ejemplo de certificado digital banco Davivienda, Detalles A



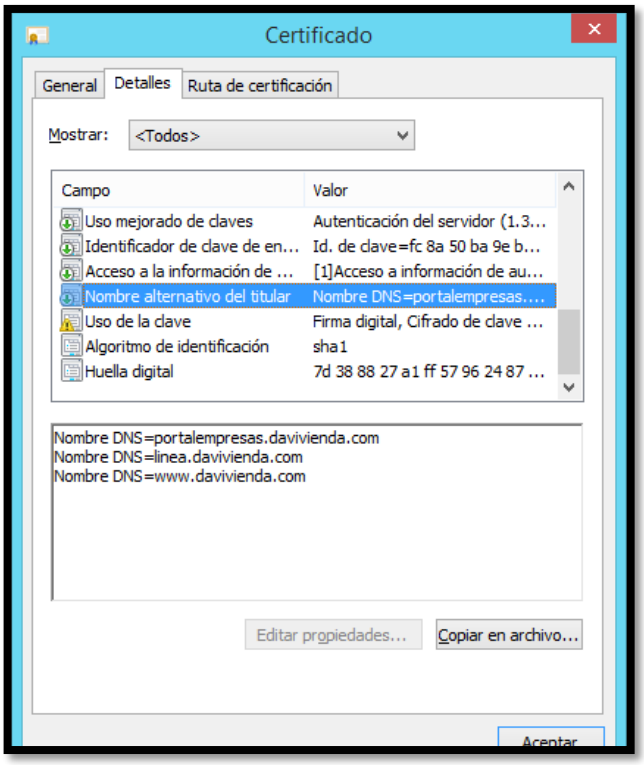
Fuente: Autores del proyecto

Figura 4. Ejemplo de certificado digital banco Davivienda, Detalles B



Fuente: Autores del proyecto

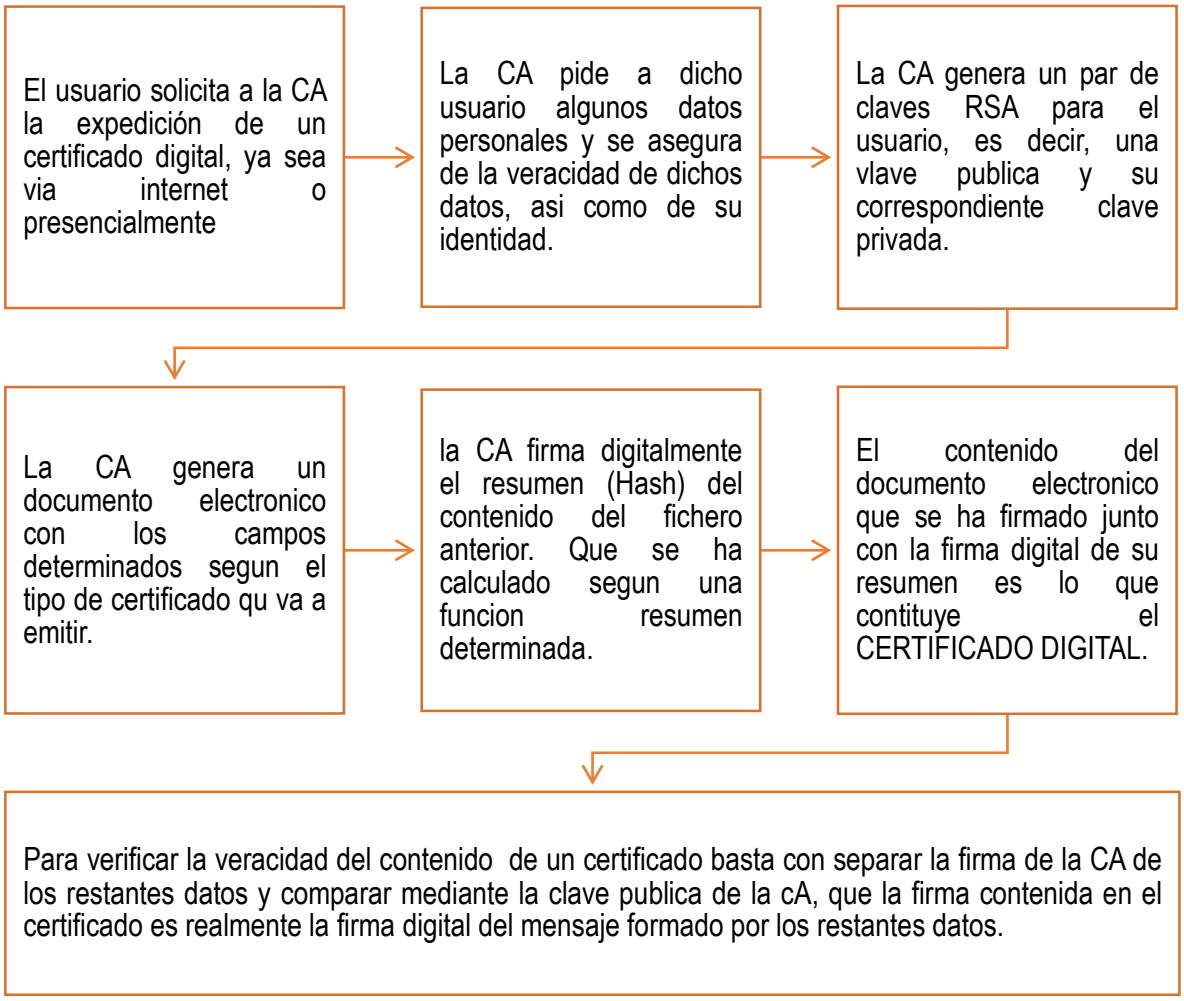
Figura 5. Ejemplo certificado digital banco Davivienda, Detalles C



Fuente: Autores del proyecto

5.4.2. Procedimiento general de solicitud, generación y validación de certificado digital

Figura 6. Procedimiento general de solicitud, generación y validación de certificado digital



Fuente: Fuster Sabater, Amparo. Hernández Encinas, Luis. Martin Muñoz, Agustín. Montoya Vitini, Fausto. Muñoz Masque. Jaime. Criptografía protección de datos y aplicaciones: Guía para estudiantes y profesionales. México: Alfaomega grupo editor, 2013. 250p

5.4.3. Aplicaciones certificados digitales. Algunas aplicaciones de los certificados digitales que se encuentran en la actualidad son:

- ✓ Correo electrónico seguro: Si un usuario desea recibir correos electrónicos seguros, es decir, confidenciales, lo único que debe hacer es lograr que los posibles emisores obtengan su clave pública, que podrán usar para cifrar los mensajes dirigidos a él. Para ello basta con que dicho usuario envié su certificado digital. Quienes reciban este certificado solo tendrán que validarlo para asegurarse de que la clave que contiene es realmente de quien dice ser su propietario. A partir de este momento, bastara con que emisor y receptor acuerden un software criptográfico capaz de utilizar las claves contenidas en los certificados.
- ✓ Navegación Segura: En numerosas ocasiones es necesario que la navegación por páginas web se lleve a cabo de modo seguro, con el fin de que la información transmitida entre los correspondientes navegadores no sea accesible a terceras partes. Esta situación se presenta, por ejemplo, cuando se accede electrónicamente a una cuenta bancaria o cuando se rellenan formularios con datos confidenciales. En estas ocasiones se suele emplear un protocolo conocido como protocolo de capa de protección segura (**SSL, Secure Sockets Layer**) o su sucesor, protocolo de seguridad de la capa de transporte (**TLS, Transport Layer Security**).
- ✓ Comercio electrónico: Cada día más las empresas ofrecen sus productos en internet, de modo que facilitan a los usuarios la compra de los mismo a través de la red. En general, este servicio consta de una página web a la que el usuario accede de forma libre y abierta y en la que el servidor ofrece una serie de mercancías. El usuario elige los productos que desea comprar y los va almacenando en su “carrito de compra”. Terminando el proceso de elección, se lleva a cabo un protocolo en el que el usuario paga las mercancías adquiridas. La forma correcta de efectuar el pago depende en gran medida de la empresa que oferta el servicio: Tarjetas de crédito, tarjetas débito, pasarelas de pago, etc., la más extendida es mediante protocolo de transacción electrónica segura (**SET, Secure Electronic Transaction**).

5.5. ENTIDAD DE CERTIFICACIÓN DIGITAL[28]

"Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales".

5.6. LISTA DE RENOVACIÓN DE CERTIFICADOS[29]

Es una lista de certificados revocados, conocida como CRL por sus siglas en inglés (**Certificate Revocation List**). En esta lista se incluyen todos los certificados digitales revocados por la entidad de certificación hasta la fecha de la lista.

5.7. INFRAESTRUCTURA DE CLAVE PÚBLICA

Public Key Infrastructure o PKI o por sus siglas en ingles es el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados digitales basados en la criptografía asimétrica. El director objetivo para el desarrollo de una PKI es permitir la adquisición segura, conveniente y eficiente de las claves públicas.

Los objetivos de PKI son:

- ✓ Autentificación de usuarios
- ✓ No repudio
- ✓ Integridad de la información
- ✓ Auditabilidad
- ✓ Acuerdo de claves secretas

[28] Ley 527 de 1999: Artículo 20. Definiciones Tag D: Entidad de Certificación http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999.html

[29] Certicamara. ¿Qué es la CRL? [en línea]. Certicamara, Validez y seguridad jurídica electrónica, 2013 [Fecha de consulta: 07 de septiembre]. Disponible en http://web.certicamara.com/soporte_interna_faqs_2.aspx

La infraestructura de clave pública puede ser usada para en diferentes contextos, como se desarrolla a continuación:

- ✓ Gestión de claves: nos permite crear, revisar o revocar claves, así como gestionar niveles de confianza.
- ✓ Publicación de claves: una vez creadas las claves, el PKI permite difundir nuestra Clave pública, así como localizar las claves públicas de otros usuarios junto con su Estado (clave revocada, etc.).
- ✓ Utilización de claves: una vez recuperada una clave, PKI facilita el uso de la misma.

5.8. FUNCIONES HASH O RESUMEN

Es una función que se aplica a un mensaje de datos (M) de tamaño variable y proporciona un resumen que siempre es del mismo tamaño, estas funciones son públicamente conocidas, es decir, se conoce un algoritmo eficiente que permite determinar el resumen, m, de un mensaje de datos cualquiera.

5.8.1. Características Funciones Hash o Resumen.

Una característica relacionada con la seguridad de estas funciones resumen es que no debe ser fácil, computacionalmente hablando, encontrar dos mensajes diferentes cuyo resumen sea el mismo. Así pues, las funciones resumen deben verificar las siguientes condiciones:

- ✓ Dependencia de bits: El resumen de un mensaje, debe depender de todos los bits del mensaje, de modo que si se cambia un único bit del mensaje, su resumen debería cambiar, por término medio, en la mitad de sus bits.
- ✓ Resistencia a la preimagen: Dado un resumen m, debe ser computacionalmente difícil obtener el mensaje M, es decir, la función resumen debe ser difícil de invertir.
- ✓ Resistencia a la segunda preimagen: Dada un mensaje cualquiera M, debe ser computacionalmente difícil encontrar otro mensaje diferente N, cuyos resúmenes coincidan.
- ✓ Resistencia a colisiones: Debe ser computacionalmente difícil, encontrar una colisión, es decir, determinar dos mensajes distintos cualesquiera M y N, cuyos resúmenes coincidan, dicho de otro

modo, debe ser computacionalmente imposible encontrar dos mensajes diferentes cuyos resúmenes colisionen.

5.8.2. Tipos de funciones hash o resumen. Actualmente podemos encontrar varios tipos de funciones resumen como lo son:

- ✓ MD5: Proporciona resúmenes de 128 bits.
- ✓ SHA-0: Proporciona resúmenes de 160 bits.
- ✓ SHA-1: Proporciona resúmenes de 160 bits. Sus resúmenes son más largos que los de MD5.
- ✓ SHA-2: Contiene 4 subalgoritmos que proporcionan resúmenes de 224, 256, 384 y 512 bits, el hecho de incrementar la longitud de los resúmenes hace que la seguridad de cada uno de ellos sea mayor.
  - ➢ SHA-224
  - ➢ SHA-256
  - ➢ SHA-384
  - ➢ SHA-512

5.8.3. Aplicaciones de las funciones hash o resumen. Algunas aplicaciones de las funciones hash o resumen que se encuentran en la actualidad son:

- ✓ Firmas digitales: En la mayor parte de estos esquemas, en lugar de firmar digitalmente un mensaje de datos, lo que se hace es firmar un resumen del mismo, lo cual hace que se gane eficiencia en los protocolos correspondientes.
- ✓ Certificados digitales: Los certificados digitales X509 V3 incluyen funciones MD5 y SHA-1 como funciones resumen para elaborar firmas digitales.
- ✓ Integridad de datos: Una forma fácil y rápida para comprobar y detectar la integridad de datos y ficheros almacenados en un equipo de cómputo consiste en calcular los resúmenes de los ficheros que interesen y guardar dicho valor fuera del equipo de cómputo. En el momento en que se desee

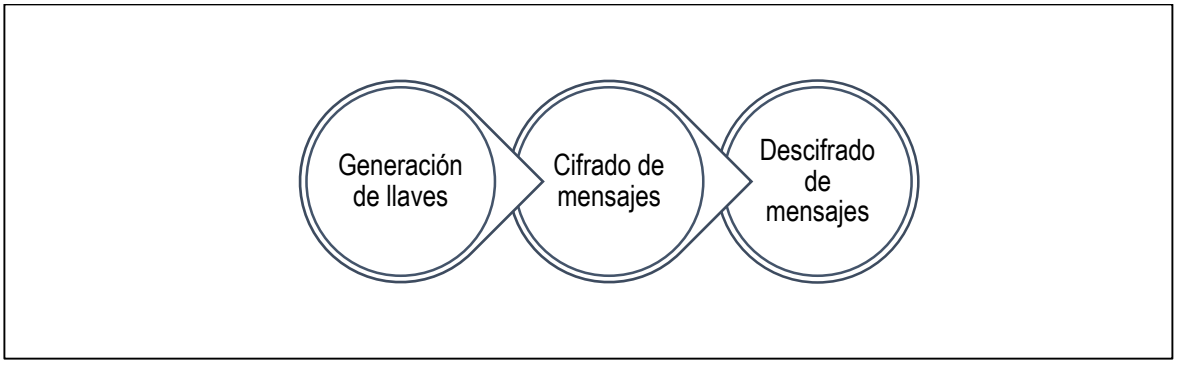
comprobar si tales ficheros han sido modificados o alterados, basta con volver a calcular su resumen y contrarrestar si el mismo coincide con el resumen calculado inicialmente.

- ✓ Repositorios de datos: Es conocida la existencia de repositorios de datos en los que es posible almacenar grandes ficheros de modo que posteriormente puedan ser descargados. Dado que el proceso de descarga puede ser algo lento es conveniente asegurarse que el fichero que se va a descargar es realmente el que se desea, de modo que se eviten demoras y pérdidas de tiempo. En general, tales ficheros se almacenan con una nota en la que se indica el valor del resumen mediante alguna función resumen conocida. Conociendo el valor del resumen del fichero de antemano, se puede verificar la integridad y autenticidad del fichero en cuestión.
- ✓ Detección de software dañino: La mayor parte de los programas de antivirus y detectores de software dañino utilizan funciones resumen con el fin de realizar una búsqueda de dicho software en el disco duro.

5.9. RSA (RIVEST, SHAMIR, ADLEMAN)

Es un criptosistema propuesto por **Ronald Rivest**, **Adi Shamir** y **Leonard Adleman** en 1978, es el criptosistema de clave pública más utilizado en la actualidad. Su seguridad se basa en la dificultad computacional de factorizar números enteros. El protocolo para cifrar y descifrar mensajes propuesto por RSA consta de tres partes:

Figura 7. Fases para cifrar y descifrar mensajes en protocolo RSA.

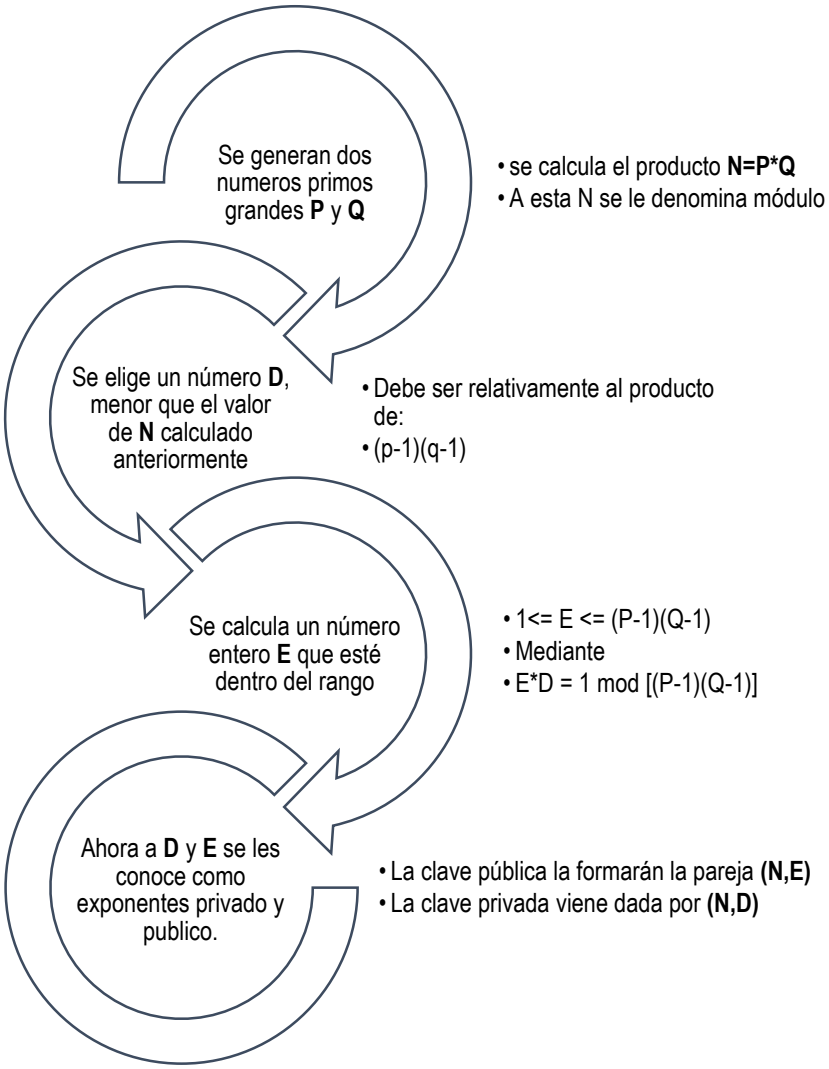


Fuente: Autores del proyecto

5.9.1. Generación de llaves. Para que obtener un par de llaves (pública y privada), debe seguir el siguiente protocolo:

- ✓ n, es el modulo del criptosistema RSA
- ✓ e, es el exponente de cifrado
- ✓ d, es el exponente de descifrado

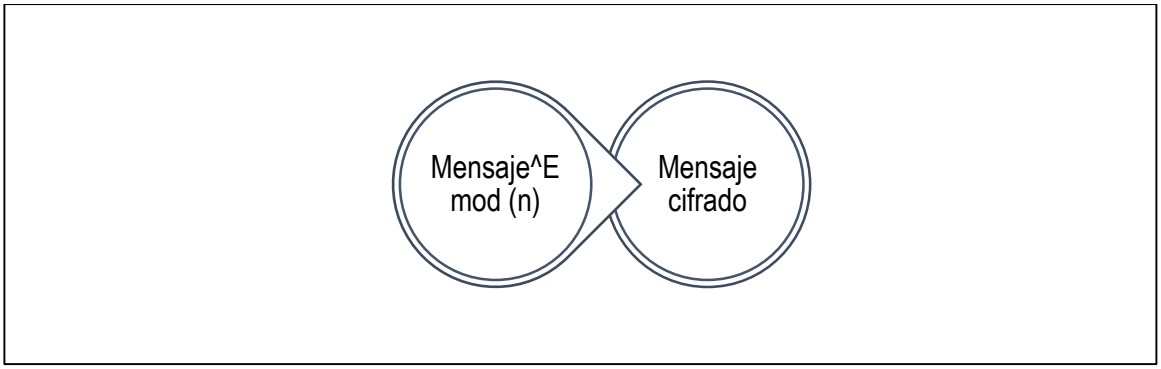
Figura 8. Proceso de generación de llaves en protocolo RSA



Fuente: Autores del proyecto

5.9.2. Cifrado de mensajes. Para cifrar un mensaje, simplemente se debe elevar el dato o el mensaje a **E**, que como sabemos de acuerdo al proceso de generación de llaves, es el número de la llave pública.

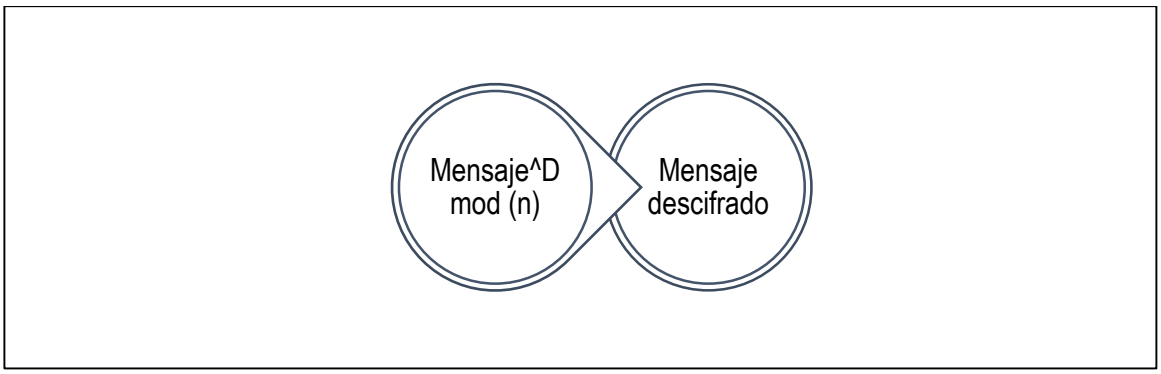
Figura 9. Proceso de cifrado en protocolo RSA.



Fuente: Autores del proyecto

5.9.3. Descifrado de mensajes. Para descifrar un mensaje, simplemente se debe elevar el dato o el mensaje a **D**, que como sabemos de acuerdo al proceso de generación de llaves, es el número de la llave privada.

Figura 10. Proceso de descifrado en protocolo RSA.



Fuente: Autores del proyecto

5.10. MODELO DE INTERCAMBIO DE LLAVES DIFFIE-HELLMAN

Establece un protocolo por el que dos usuarios llegan a intercambiarse información secreta haciendo uso de un canal inseguro, de modo que nadie más que los dos intervinientes sea capaz de conocer tal información. Tal protocolo recibe el nombre protocolo de acuerdo o intercambios de llaves de Diffie-Hellman.

5.11. SECURE SOCKETS LAYER (SSL) – TRANSPORT LAYER SECURE (TLS)

Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar. SSL implica una serie de fases básicas:

Figura 11. Fases del protocolo SSL.

Fuente: Autores del proyecto

Ambos protocolos permiten la comunicación segura, confidencialidad, autenticación frente a un servidor, aunque existen algunas diferencias. SSL fue desarrollado por Netscape (v2 y v3) para agregar HTTP y fue estandarizado por IETF como TLS. TLS 1.0 sería como SSL 3.1 (parecido a SSL 3.0 pero Incompatible).

Figura 12. Características protocolo TLS

Versión actual TLS 1.2

Utiliza el cifrado simétrico de clave publica

Cuando cliente y servidor establecen conexión, cliente y servidor intercambian certificados.

- Estos certificados son actualmente X.509

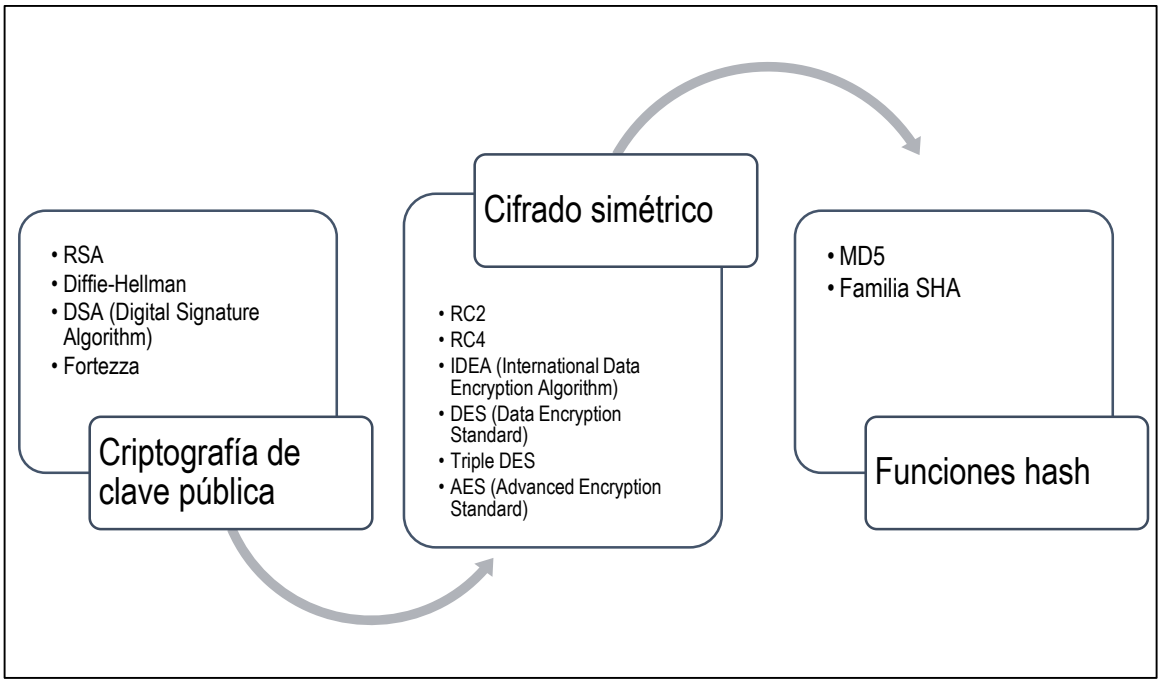
Se implementa a nivel de la capa de transporte (capa OSI)

Corre por debajo de los protocolos usuales: HTTP, FTP, POP, etc

Fuente: Autores del proyecto

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

Figura 13. Opciones de implementación SSL/TLS



Fuente: Autores del proyecto

5.11.1. Aplicaciones SSL/TLS. SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Puede proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP).

- ✓ Sitios Web: Uno de los usos más importantes es junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.
- ✓ Intercambio de claves o acuerdo de clave: Antes de que un cliente y el servidor pueden empezar a intercambiar información protegida por TLS, deben intercambiar en forma segura o acordar una clave de cifrado y una clave para usar cuando se cifren los datos. Entre los métodos utilizados para el intercambio/acuerdo de claves son:

- Las claves públicas y privadas generadas con RSA (denotado TLS_RSA en el protocolo de handshake TLS)
- Diffie-Hellman (llamado TLS_DH)
- Diffie-Hellman efímero (denotado TLS_DHE)
- Diffie-Hellman de Curva Elíptica (denotado TLS_ECDH),
- Diffie-Hellman de Curva Elíptica efímero (TLS_ECDHE)
- Diffie-Hellman anónimo (TLS_DH_anon)
- PSK (TLS_PSK).

6. DOCUMENTOS COMPLEMENTARIOS

Como material complementario se propone una serie de documentos que pueden ser consultados con el objetivo de ahondar sobre certificados y firmas digitales.

7. OBTENCIÓN DE CERTIFICADOS DE FIRMA DIGITAL

El proceso para la obtención de los certificados de firma digital depende de la entidad de certificación digital autorizada.

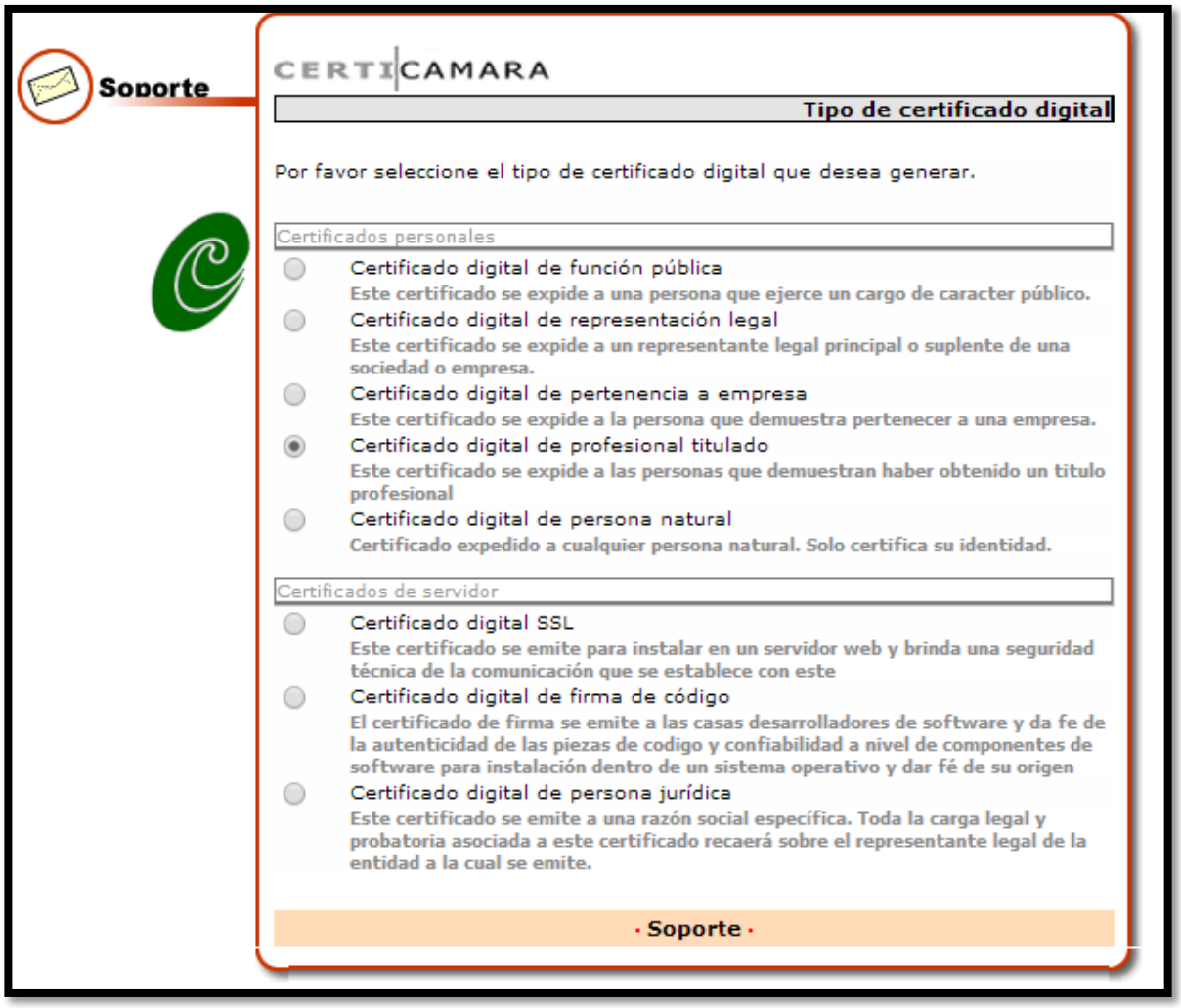
7.1. OBTENCIÓN DE CERTIFICADOS DE FIRMA DIGITAL MEDIANTE CERTICÁMARA

CERTICÁMARA permite obtener certificados de firma digital para la ejecución de pruebas piloto que se requieran, estos serán procesados a través de nuestra autoridad de certificación (CA) Demo de CERTICÁMARA la cual tiene las mismas características técnicas y funcionales de un certificado de producción, lo único diferente es que este certificado de demostración no tendría "validez jurídica".

Para la obtención de estos certificados de demostración es necesario realizar el procedimiento que se describe a continuación para la generación de cada uno de los certificados, esto no tendrán ningún tipo de costo y tendrán vigencia de 1 año.

Para iniciar debemos ingresar a la dirección web establecida por CERTICÁMARA http://www.certicamara.com.co/generacionllaves/pages/formPaso0.html en esta página de internet encontrará un listado con los tipos de certificado digital que se pueden solicitar, seleccione la opción correspondiente al tipo de certificado digital requerido. (Véase la figura 14)

Figura 14. Formulario de solicitud de certificados digitales Certicámara



Fuente: Autores del proyecto

7.1.1 Tipos de certificados CERTICÁMARA. Los tipos de certificados ofrecidos por CERTICÁMARA son de dos tipos:

- ✓ Certificados Personales
  - ➢ Certificado digital de función pública: Este certificado se expide a una persona que ejerce un cargo de carácter público.

- Certificado digital de representación legal: Este certificado se expide a un representante legal principal o suplente de una sociedad o empresa.
- Certificado digital de pertenencia a empresa: Este certificado se expide a la persona que demuestra pertenecer a una empresa.
- Certificado digital de profesional titulado: Este certificado se expide a las personas que demuestran haber obtenido un título profesional.
- Certificado digital de persona natural: Certificado expedido a cualquier persona natural. Solo certifica su identidad.

✓ Certificados de Servidor

- Certificado digital SSL: Este certificado se emite para instalar en un servidor web y brinda una seguridad técnica de la comunicación que se establece con este.
- Certificado digital de firma de código: El certificado de firma se emite a las casas desarrolladores de software y da fe de la autenticidad de las piezas de código y confiabilidad a nivel de componentes de software para instalación dentro de un sistema operativo y dar fe de su origen.
- Certificado digital de persona jurídica: Este certificado se emite a una razón social específica. Toda la carga legal y probatoria asociada a este certificado recaerá sobre el representante legal de la entidad a la cual se emite.

Al seleccionar el tipo de certificado se abrirá un formulario de solicitud el cual deberá diligenciar cuidadosamente, puesto que los datos allí diligenciados serán empleados para la generación de su certificado digital. Por favor, tenga en cuenta las siguientes recomendaciones para el diligenciamiento del formulario de solicitud:

✓ En el campo Nombres y apellidos diligencie su nombre tal como aparece en su documento de identificación (Cédula de ciudadanía o cédula de extranjería).

✓ El campo Número de documento de identificación deberá ser diligenciado sin emplear signos de puntuación.

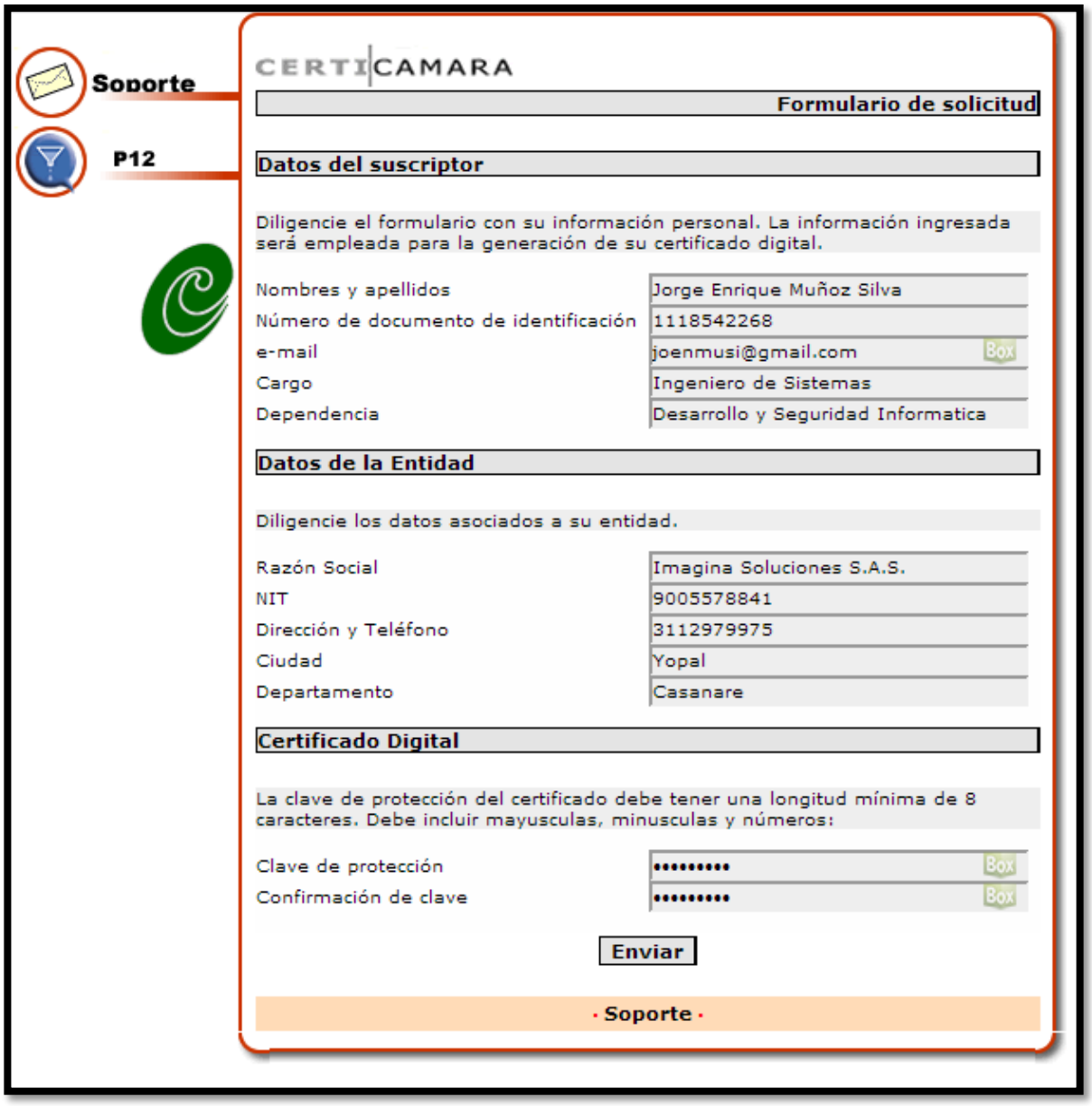
✓ En el campo de Email diligencie una dirección de correo electrónico válida.

- ✓ En el campo Razón social diligencie la razón social de su compañía.
- ✓ En el campo de NIT deberá diligenciar el NIT de su entidad con digito de verificación, sin emplear guiones o signos de puntuación.
- ✓ Al final del formulario de solicitud se le pedirá que ingrese una contraseña y su correspondiente confirmación. Esta contraseña será empleada para el cifrado de su certificado digital y será requerida más adelante para la descarga del certificado digital generado, por lo tanto, es muy importante que recuerde la contraseña generada porque de lo contrario no podrá descargar su certificado digital.
- ✓ La clave solicitada deberá tener una longitud mínima de ocho caracteres y deberá incluir únicamente mayúsculas, minúsculas y números (no debe incluir caracteres especiales)

Dependiendo del tipo de certificado seleccionado pueden cambiar los campos en el formulario.

- ✓ Certificado digital de profesional titulado. Al abrir el formulario se debe ingresar cuidadosamente la información solicitada para la generación del certificado teniendo en cuenta las recomendaciones. (…Véase la figura 15…).

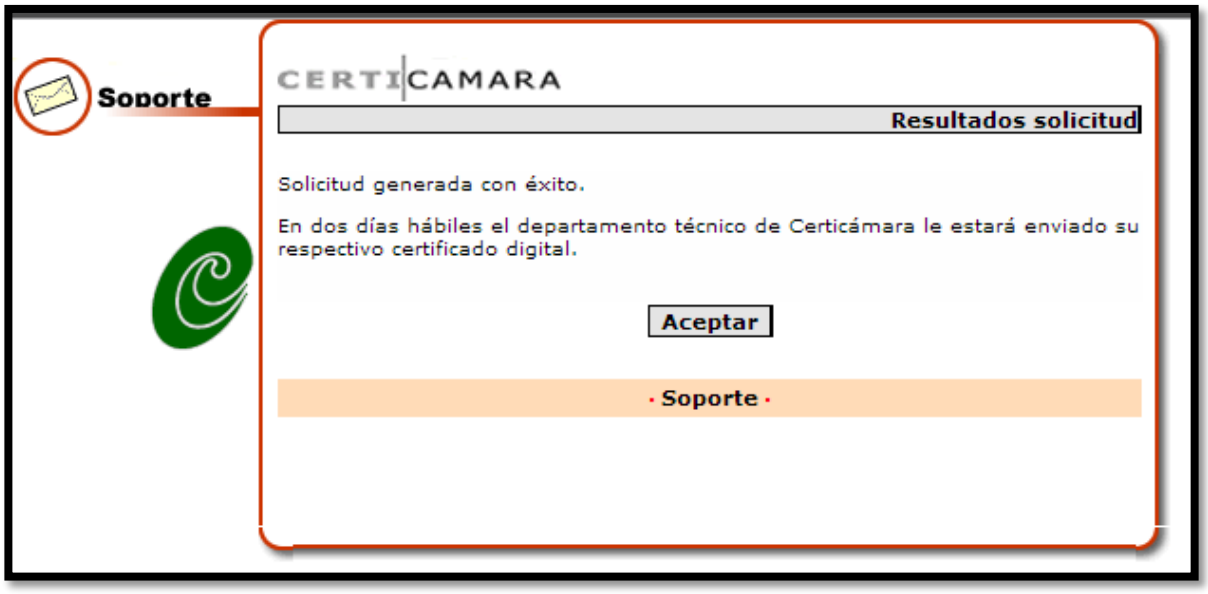
Figura 15. Formulario de solicitud certificado digital profesional titulado Certicámara



Fuente: Autores del proyecto

Finalmente una vez diligenciado el formulario de solicitud hacer clic en el botón "**Enviar**", la solicitud debe generar un mensaje de confirmación informando que la solicitud fue generada de forma exitosa. (…Véase la figura 15…).

Figura 16. Resultado de solicitud certificado digital profesional titulado Certicámara



Fuente: Autores del proyecto

Una vez observado el mensaje de confirmación podemos hacer clic en el botón "**Aceptar**" o cerrar la ventana del navegador de internet.

Advertencia: Es necesario confirmar el registro al correo al correo electrónico **ssl@certicamara.com** indicando el número de cédula ingresado en el formulario, de lo contrario la solicitud no será procesada.

8. GENERACIÓN DEL CERTIFICADO DE FIRMA DIGITAL

Para realizar este procedimiento previamente debe haber completado los pasos mencionados en el punto de "**Obtención de certificados de firma digital**".

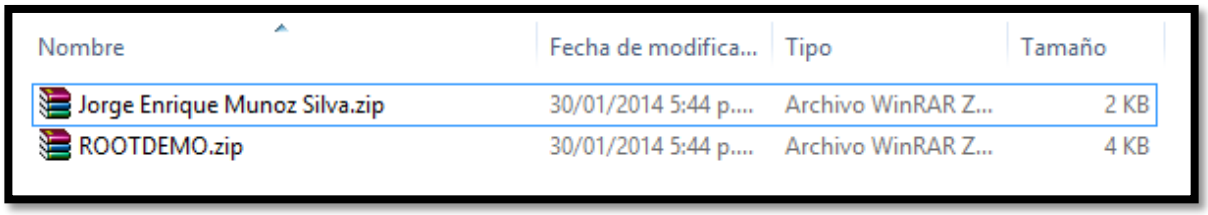
Recibirá un correo electrónico de la dirección **ssl@certicamara.com** en el cual vendrá el archivo comprimido que contiene el certificado digital solicitado anteriormente, con lo anterior se podrá llevar a cabo la finalización del proceso de generación de su certificado digital. A continuación se muestra un ejemplo del archivo adjunto. (Véase la figura 17).

Figura 17. Archivos de certificado digital en la bandeja de correo electrónico

Fuente: Autores del proyecto

Realice la descarga de los archivos adjuntos a una ubicación de fácil acceso como el escritorio "**Escritorio**", obtendrá dos (2) archivos comprimidos. (Véase la figura 18).

Figura 18. Archivos comprimidos resultado de la solicitud de certificado digital profesional titulado Certicámara.



Fuente: Autores del proyecto

Para poder continuar es necesario realizar la descompresión para obtener el certificado de firma digital; es posible realizar la descompresión con una herramienta gratuita llamada 7zip. Descargar de los siguientes enlaces y realizar la instalación que consta de pocos y sencillos pasos.

Figura 19. Enlaces de descarga herramienta 7Zip

7Zip - Arquitecturas 32 bits

- http://downloads.sourceforge.net/sevenzip/7z920.msi

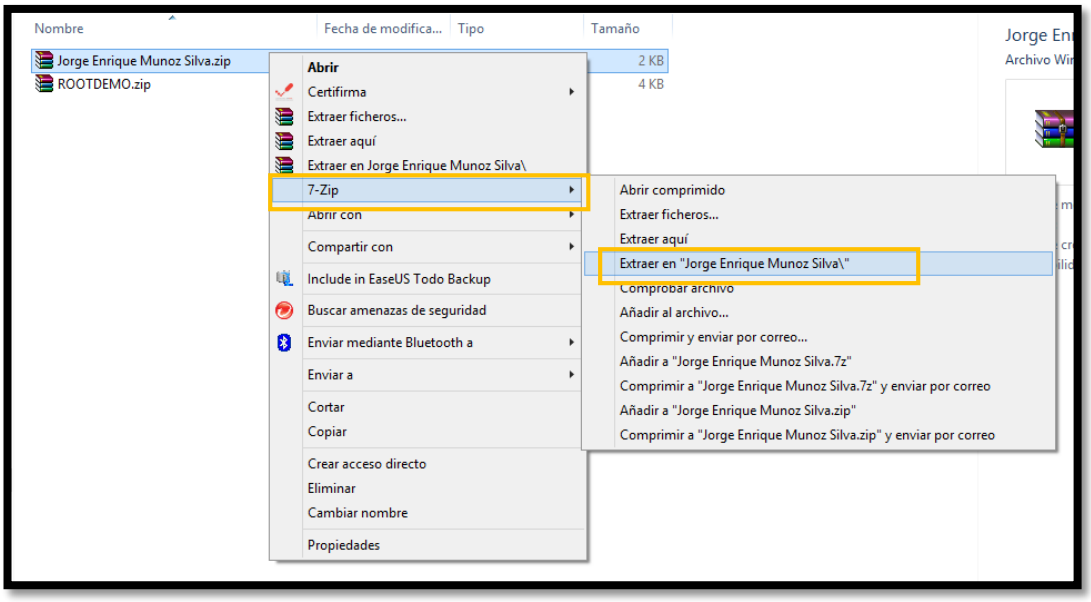
7Zip - Arquitectura 64 Bits

- http://downloads.sourceforge.net/sevenzip/7z920-x64.msi

Fuente: Autores del proyecto

Ejecutamos la descompresión del certificado de firma digital haciendo clic derecho sobre el archivo descargado denominado "**Jorge Enrique Munoz Silva.zip**", buscamos dentro del menú contextual la opción 7-Zip y dentro del submenú la opción Extraer en "**Jorge Enrique Munoz Silva**", (Véase la figura 20).

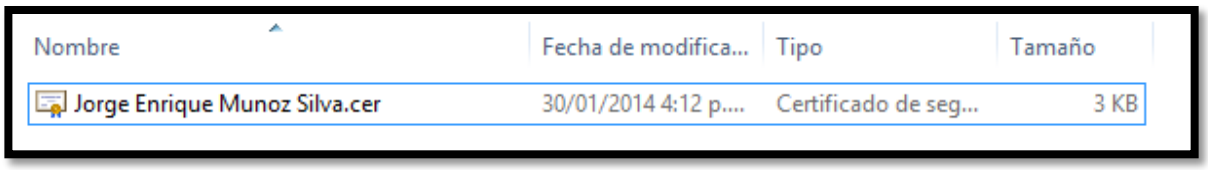
Figura 20. Proceso para realizar descompresión de los archivos mediante 7Zip



Fuente: Autores del proyecto

Esperamos a que se realice la descompresión del certificado de firma digital y obtendremos la carpeta, nos desplazamos en ellas hasta ubicar el archivo "**Jorge Enrique Munoz Silva.cer**". (Véase la figura 21).

Figura 21. Certificado de firma digital enviado por la entidad de certificación posterior a la solicitud



Fuente: Autores del proyecto

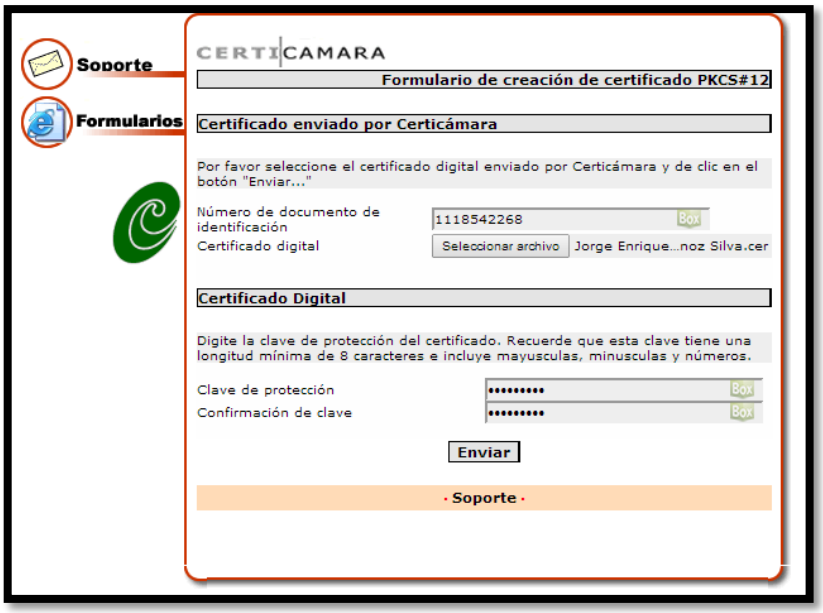
Procedemos a la generación del certificado de firma digital, para iniciar debemos ingresar a la dirección web establecida por CERTICÁMARA:

http://www.certicamara.com.co/generacionllaves/pages/personalCertificate/formPaso2.html

En esta página de internet encontrará un formulario con el que podrá hacer la generación y descarga del certificado de firma digital en formato "**p12**"[30]. PKCS#12 "Este estándar especifica un formato portátil para transportar llaves privadas de un usuario".

Debemos realizar el diligenciamiento del formulario ingresando el número de identificación con el que se solicitó el certificado digital, seleccionar el archivo "**Jorge Enrique Munoz Silva.cer**" que se obtuvo al realizar la descarga y descompresión del archivo adjunto recibido en el correo electrónico enviado desde la dirección "**ssl@certicamara.com**", finalmente debemos ingresar la contraseña de seguridad que se definió en el formulario para la obtención del certificado de firma digital y hacer clic en el botón "**Enviar**". (Véase la figura 22).

Figura 22. Formulario de creación de certificado PKCS#12

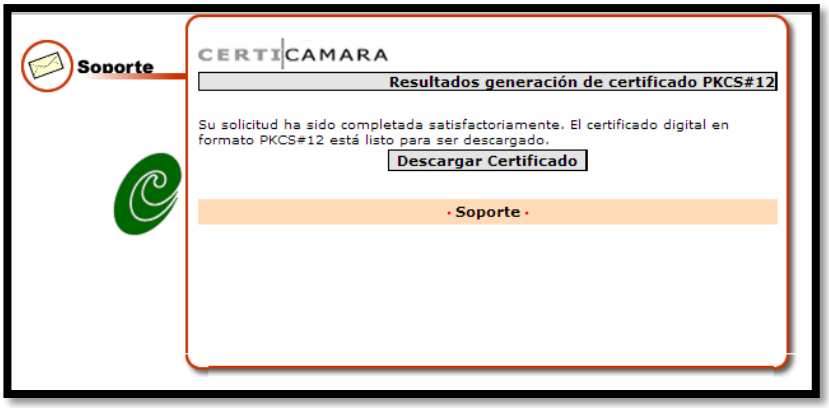


Fuente: Autores del proyecto

[30] RSA LABORATORIES, PKCS #12: Personal information exchange syntax standard [en línea]. < http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm> [citado 14 de febrero de 2014].

El formulario mostrará un mensaje informando que se generó satisfactoriamente el certificado de firma digital en formato "**PKCS#12**". (Véase la figura 23).

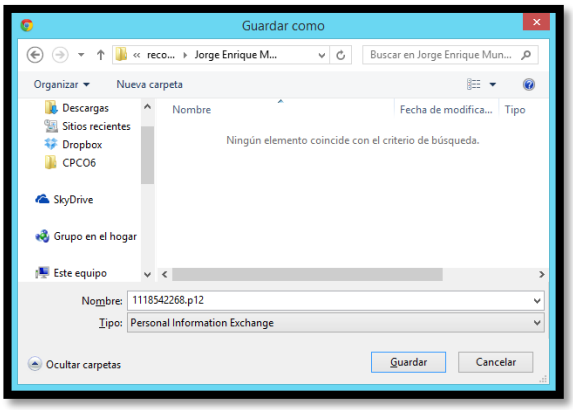
Figura 23. Resultado de generación de certificado PKCS#12



Fuente: Autores del proyecto

Procedemos a hacer clic en el botón "**Descargar**" para realizar la descarga del certificado en nuestro equipo de cómputo. Le navegador mostrara un cuadro de dialogo para seleccionar la ruta donde deseamos almacenar el certificado con extensión "**p12**", seleccionamos una ubicación de fácil recordación y hacemos clic en el botón guardar. (Véase la figura 24).

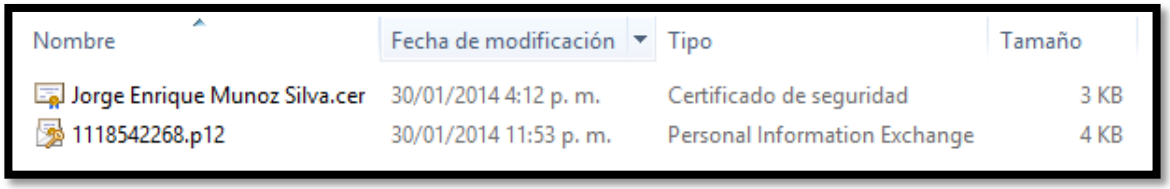
Figura 24. Descarga de certificado de firma digital p12



Fuente: Autores del proyecto

Finalmente tendremos en la ubicación seleccionada el certificado de firma digital con extensión "**p12**" generado y listo para realizar el proceso de firma con cualquier documento electrónico.

Figura 25. Certificado de firma digital p12

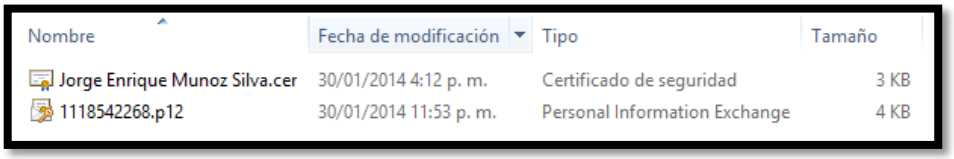


Fuente: Autores del proyecto

9. INSTALACIÓN DE CERTIFICADO DE FIRMA DIGITAL

Para realizar este procedimiento previamente debe haber completado los pasos mencionados en el punto de "**Generación del Certificado de Firma Digital**". Para iniciar haga doble clic sobre el certificado de firma digital generado anteriormente "**NumeroDeIdentificación.p12**" por ejemplo "**1118542268.p12**". (Véase la figura 26).

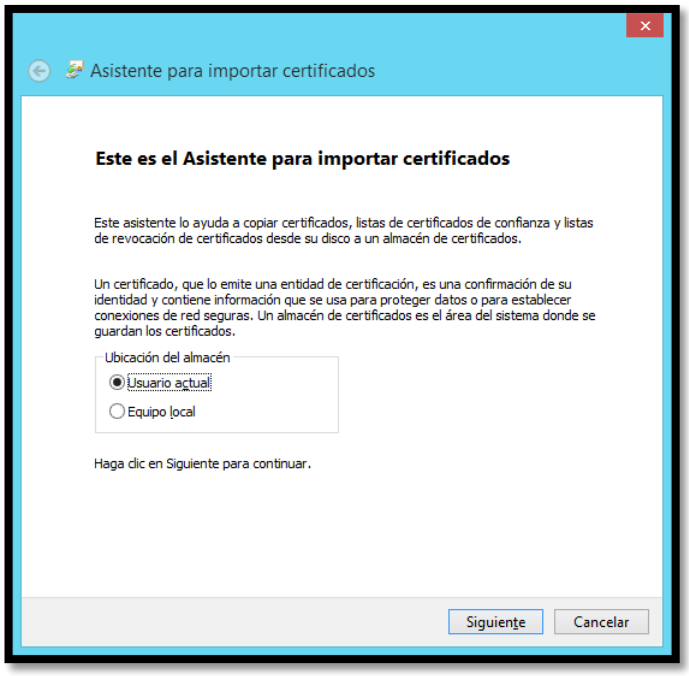
Figura 26. Certificado de firma digital p12



Fuente: Autores del proyecto

Se abrirá un cuadro de dialogo con el "**Asistente para importar certificados**", seleccione la ubicación del almacén en "**Usuario actual**" y haga clic en el botón "**Siguiente**" para continuar. (Véase la figura 27).

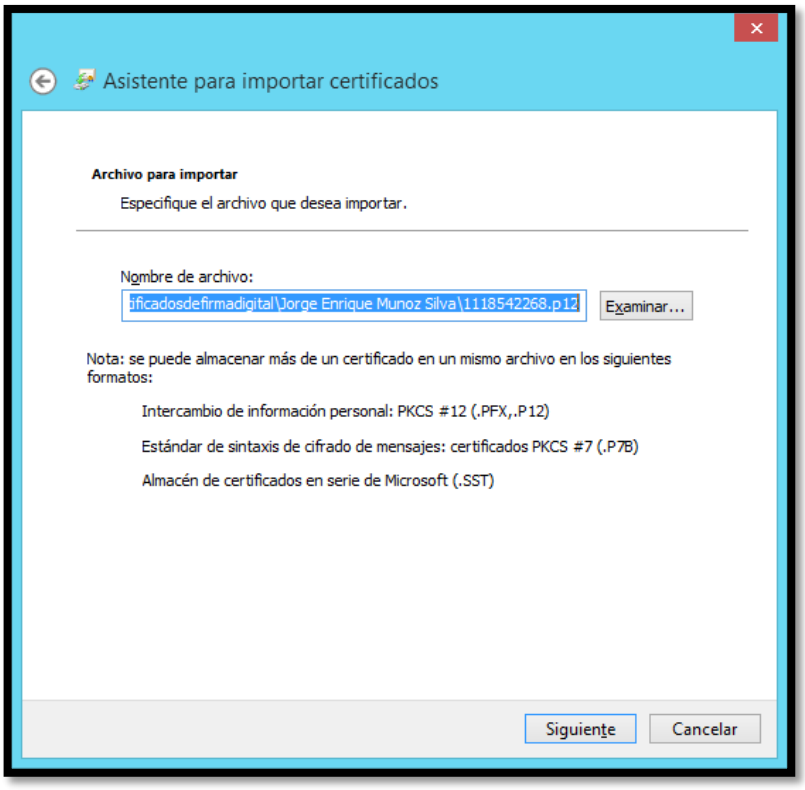
Figura 27. Asistente para importar certificados, selección de almacén



Fuente: Autores del proyecto

El asistente mostrará la ruta del certificado de firma digital a instalar, para continuar con el proceso hacemos clic en el botón "**Siguiente**". (Véase la figura 28).

Figura 28. Asistente para importar certificados, archivo a importar



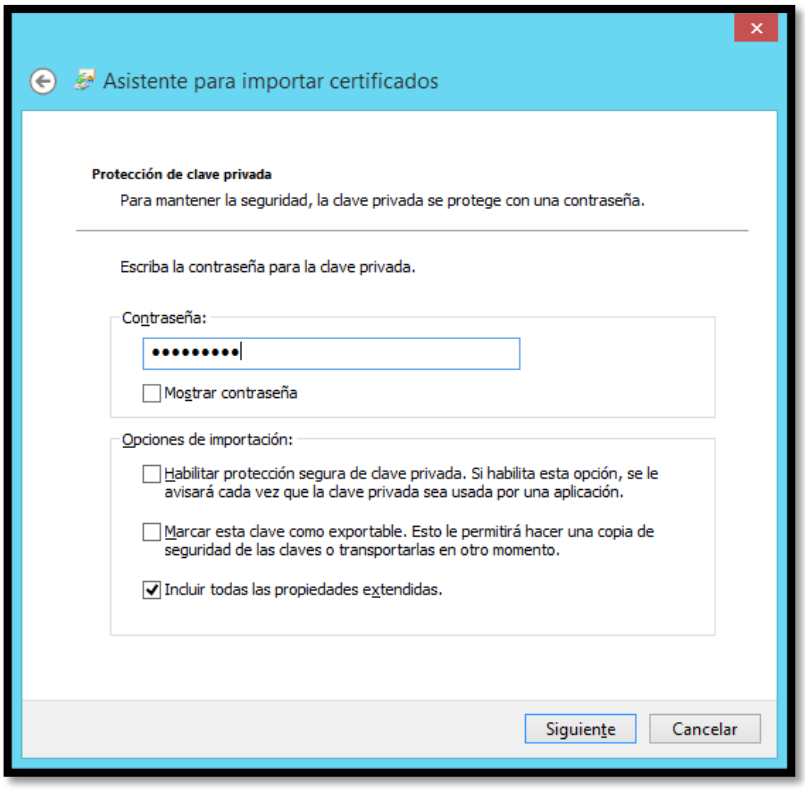
Fuente: Autores del proyecto

A continuación el asistente solicitará la contraseña del certificado de firma digital, el cual fue asignado al momento de la generación y que protege la información de identificación aquí contenida, adicionalmente debemos seleccionar las tres (3) opciones de la importación mencionadas a continuación:

- ✓ Habilitar la protección de la clave privada
- ✓ Marcar esta clave como exportable
- ✓ Incluir todas las propiedades extendidas

Seguidamente hacemos clic en el botón "**Siguiente**". (Véase la figura 29).

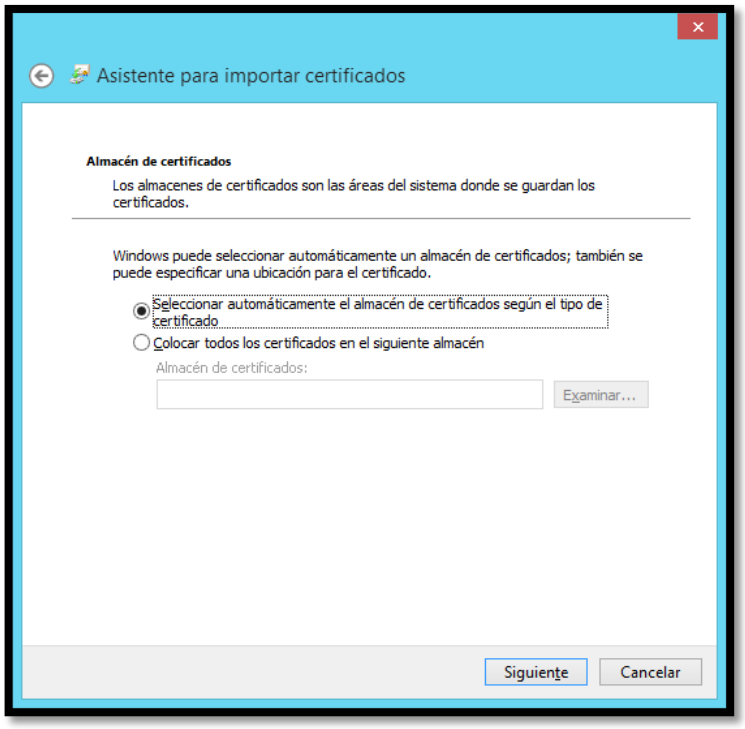
Figura 29. Asistente para importar certificados, protección de clave privada



Fuente: Autores del proyecto

El asistente solicitará el almacén para el certificado, seleccionamos la opción "**Seleccionar automáticamente el almacén de certificados según el tipo de certificado**" y hacemos clic en siguiente para continuar con la instalación del certificado de firma digital. (Véase la figura 30).

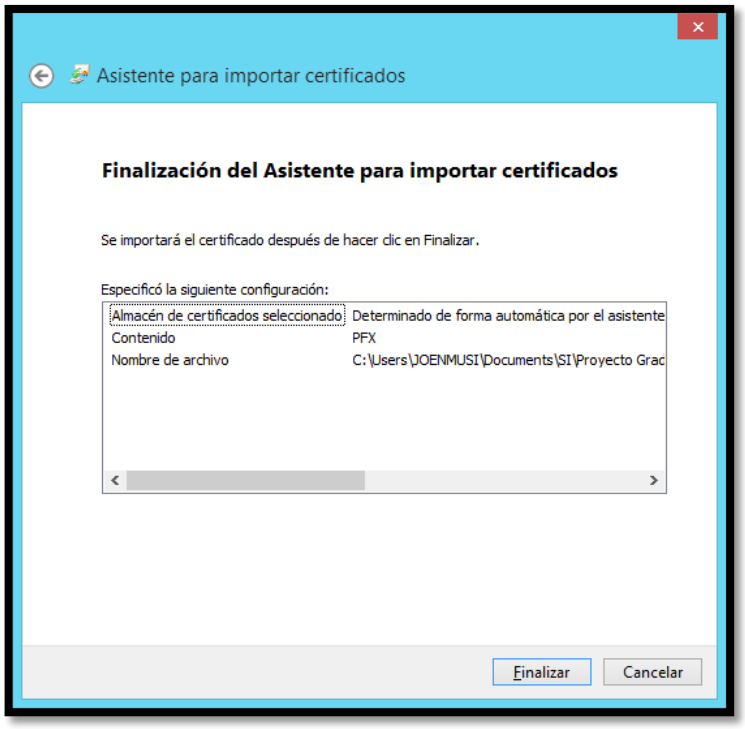
Figura 30. Asistente para importar certificados, selección de almacén de certificados



Fuente: Autores del proyecto

El asistente mostrara un resumen de la importación, hacemos clic en el botón "**Finalizar**".

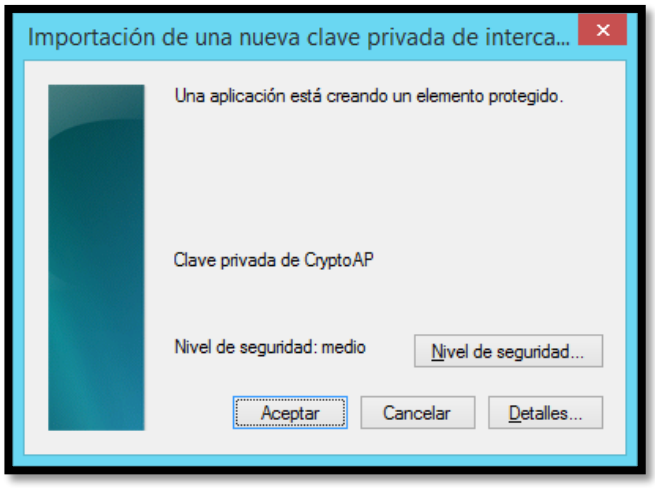
Figura 31. Asistente para importar certificados, resumen de configuración



Fuente: Autores del proyecto

Se abrirá un cuadro de dialogo "**Importación de una nueva clave privada de intercambio**". (Véase la figura 32).

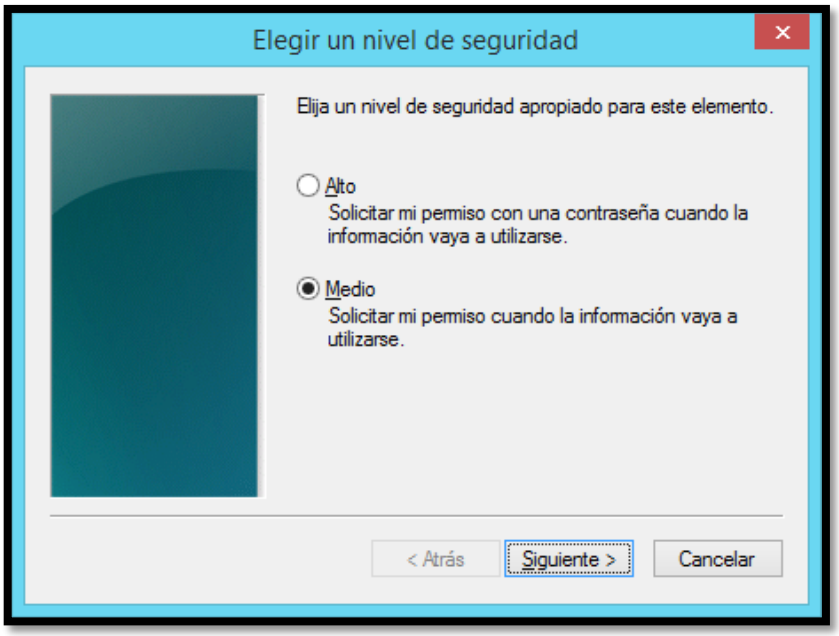
Figura 32. Asistente para selección de nivel de seguridad para certificado importado



Fuente: Autores del proyecto

Hacemos clic en el botón "**Nivel de seguridad…**" y se abrirá otro cuadro de dialogo que nos permite seleccionar el nivel de seguridad asociado a este certificado de firma digital que se está importando, seleccionamos "**Alto**" y hacemos clic en el botón "**Siguiente**" para continuar. (Véase la figura 33).

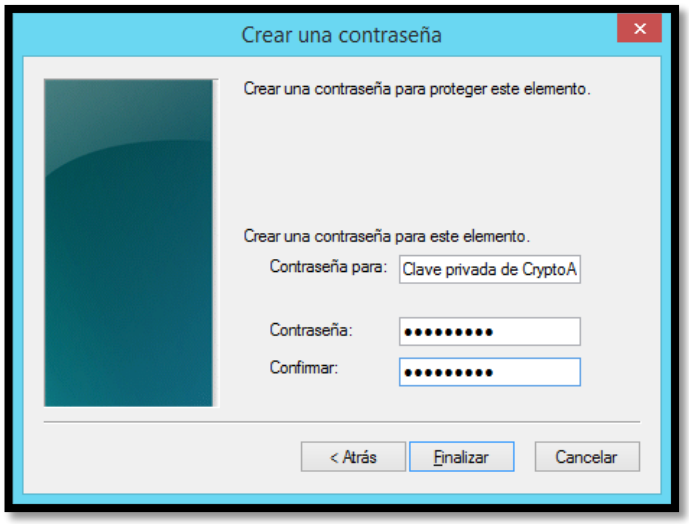
Figura 33. Elección del nivel de seguridad para el uso del certificado digital



Fuente: Autores del proyecto

Un nuevo cuadro de dialogo denominado "**Crear una contraseña**" se abrirá, aquí debemos digitar una contraseña de protección de la llave privada y confirmarla. Esta contraseña será solicitada cada vez que se desee firmar digitalmente o cifrar empleando la llave privada correspondiente al certificado digital. Finalmente hacemos clic en el botón "Finalizar". (Véase la figura 34).

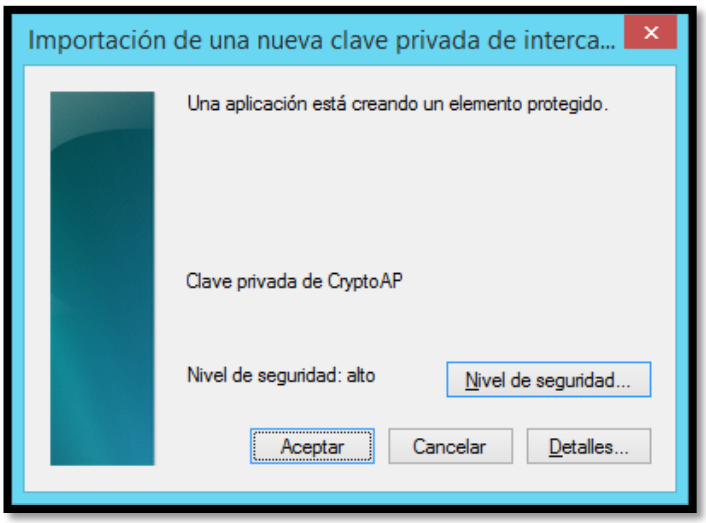
Figura 34. Creación de contraseña para protección de certificado digital



Fuente: Autores del proyecto

Volveremos al cuadro de dialogo "**Importación de una nueva clave privada de intercambio**" y hacemos clic en el botón aceptar "**Aceptar**". (Véase la figura 35).

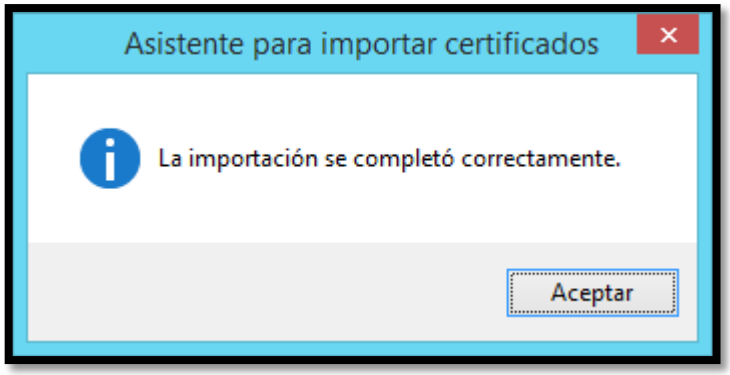
Figura 35. Asistente para selección de nivel de seguridad de certificado digital



Fuente: Autores del proyecto

El “**Asistente para importar certificados**” informara que la importación se realizó correctamente, procedemos a hacer clic en el botón “**Aceptar**” para cerrar el cuadro de dialogo. (Véase la figura 36).

Figura 36. Respuesta de confirmación del proceso de importación de certificados



Fuente: Autores del proyecto

10. INSTALACIÓN CERTIFICADO RAÍZ

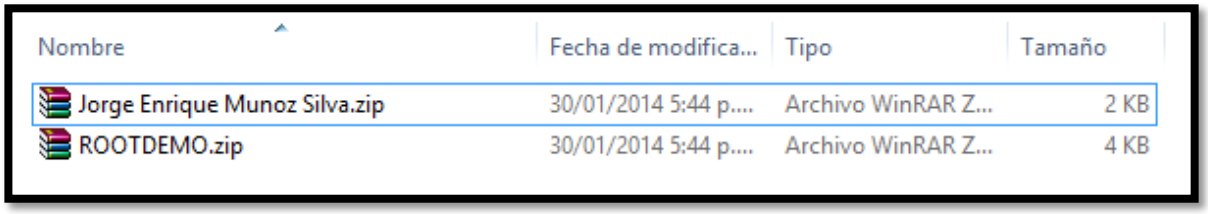
Para realizar este procedimiento previamente debe haber completado los pasos mencionados en el punto de "**Obtención de certificados de firma digital**".

Este procedimiento es complementario al procedimiento de "**Instalación de certificado de firma digital**".

Para realizar la instalación del certificado raíz debe hacer uso del archivo adjunto denominado "**ROOTDEMO.zip**" recibido como respuesta del correo electrónico **ssl@certicamara.com** a su solicitud enviada a "**CERTICÁMARA**".

Si ha seguido los pasos adecuadamente, en el procedimiento "**Generación del certificado de firma digital**" se realizó la descarga del archivo comprimido que contiene el certificado raíz suministrado por la entidad de certificación.

Figura 37. Archivos comprimidos resultado de la solicitud de certificado digital profesional titulado Certicámara



Fuente: Autores del proyecto

Para poder continuar es necesario realizar la descompresión para obtener el certificado raíz; es posible realizar la descompresión con una herramienta gratuita llamada 7zip. Descargar de la siguiente los siguientes enlaces y realizar la instalación que costa de pocos y sencillos pasos.

Figura 38. Enlaces de descarga herramienta 7Zip

7Zip - Arquitecturas 32 bits

- http://downloads.sourceforge.net/sevenzip/7z920.msi

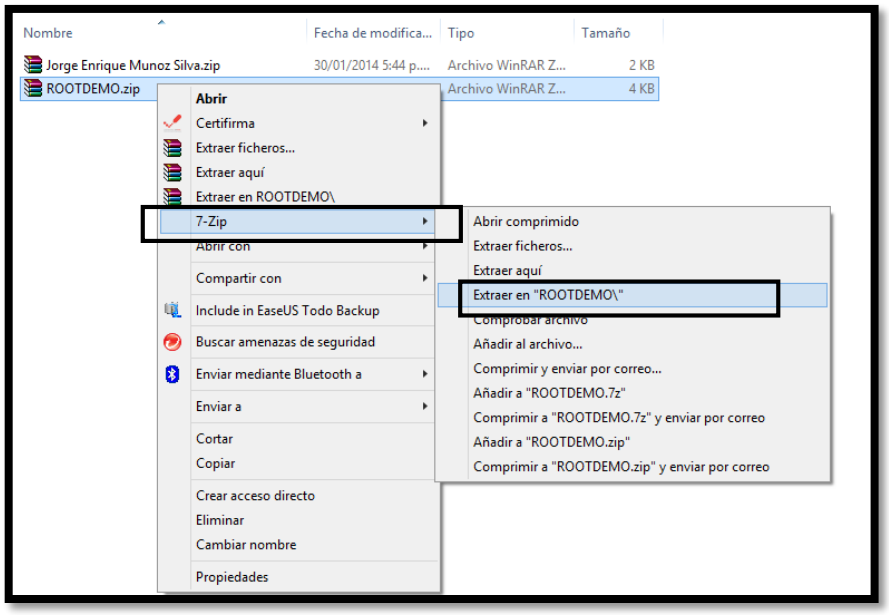
7Zip - Arquitectura 64 Bits

- http://downloads.sourceforge.net/sevenzip/7z920-x64.msi

Fuente: Autores del proyecto

Ejecutamos la descompresión del certificado raíz haciendo clic derecho sobre el archivo descargado denominado "**ROOTDEMO.zip**", buscamos dentro del menú contextual la opción 7-Zip y dentro del submenú la opción Extraer en "**ROOTDEMO**", (Véase la figura 39).

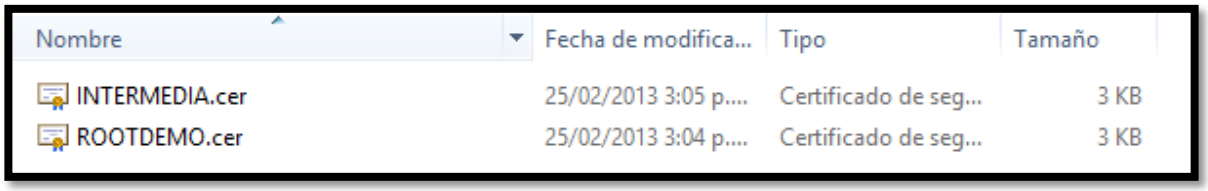
Figura 39. Proceso para realizar descompresión de los archivos



Fuente: Autores del proyecto

Esperamos a que se realice la descompresión del certificado raíz y obtendremos la carpeta, nos desplazamos en ellas hasta ubicar los archivos "**INTERMEDIA.cer**" y "**ROOTDEMO.cer**". (Véase la figura 40).

Figura 40. Certificado raíz emitido por la entidad de certificación

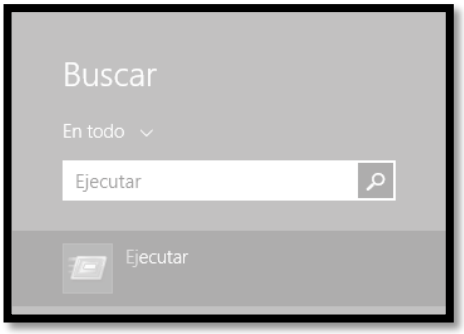


Fuente: Autores del proyecto

10.1. INSTALACIÓN DE CERTIFICADO RAÍZ MEDIANTE CONSOLA DE ADMINISTRACIÓN

En Windows 7 haga clic en el botón "**Inicio**" y seleccione "**Ejecutar**" o En Windows 8 o 8.1 ingrese al "**Inicio**" y escriba la palabra "**Ejecutar**" y se abrirá el cuadro de dialogo ejecutar. (Véase la figura 41).

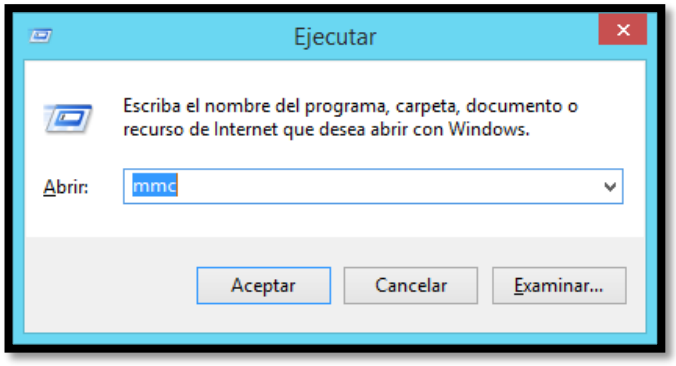
Figura 41. Búsqueda de la herramienta ejecutar



Fuente: Autores del proyecto

En el cuadro de dialogo "**Ejecutar**" escribimos "**mmc**" y hacemos clic en el botón "**Aceptar**" para abrir la "**Consola de administración**". (Véase la figura 42).

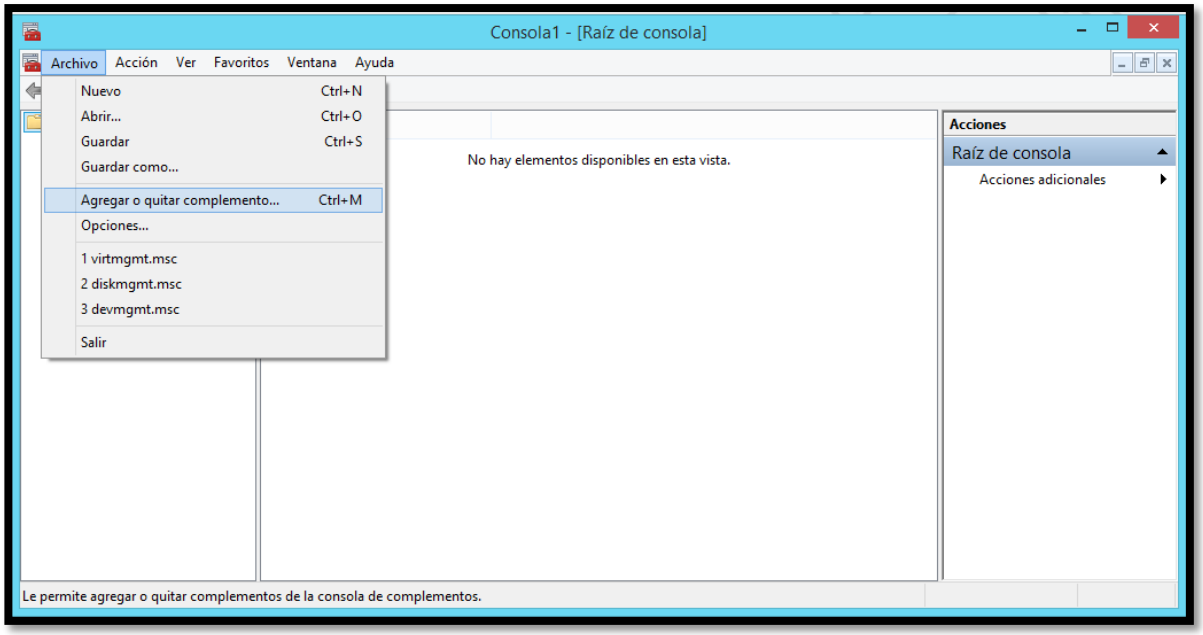
Figura 42. Cuadro de dialogo Ejecutar, abrir consola de administración



Fuente: Autores del proyecto

Se abrirá la consola de administración, para continuar hacemos clic en el menú "**Archivo**" y seleccionamos la opción "**Agregar o quitar complemento**". (Véase la figura 43).

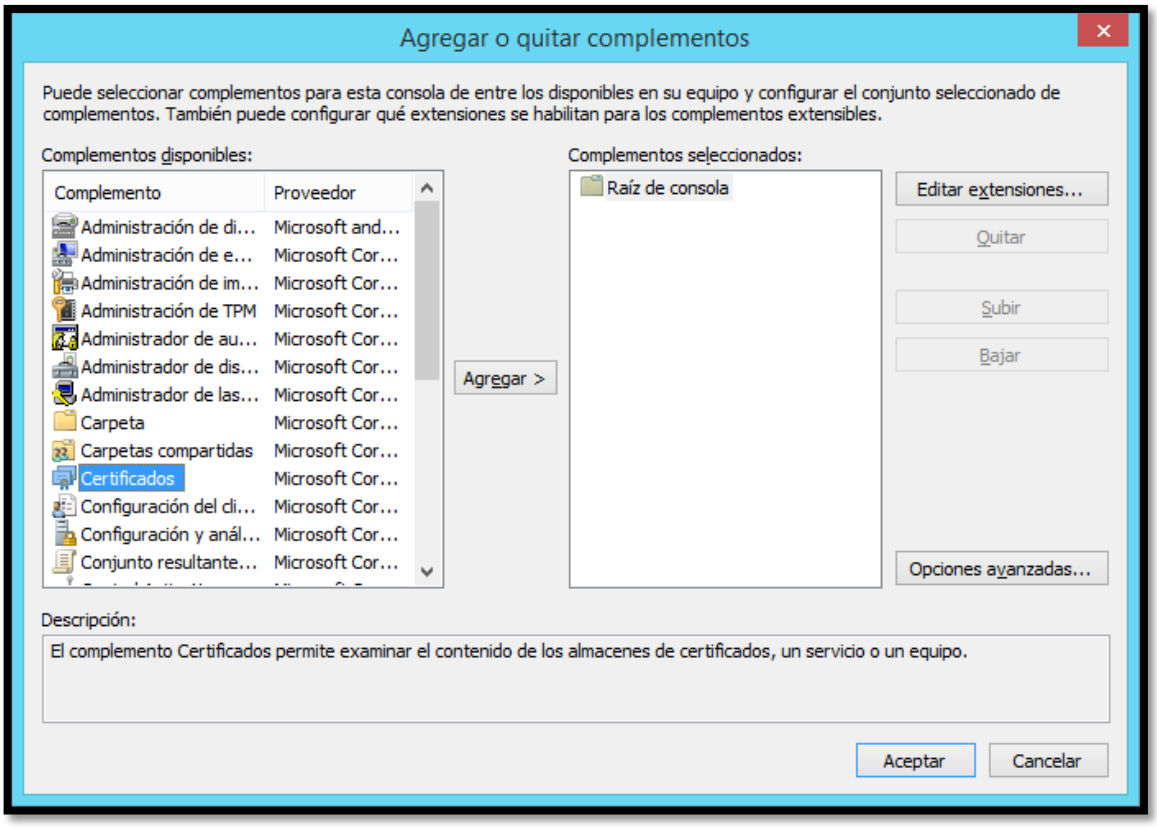
Figura 43. Interfaz de la consola raíz de administración de Windows



Fuente: Autores del proyecto

Seguidamente se abrirá el cuadro de dialogo "**Agregar o quitar complemento**", de la lista de la parte izquierda del cuadro de dialogo seleccionamos "**Certificados**" y hacemos clic en el botón "**Agregar**" de la parte central. (Véase la figura 44).

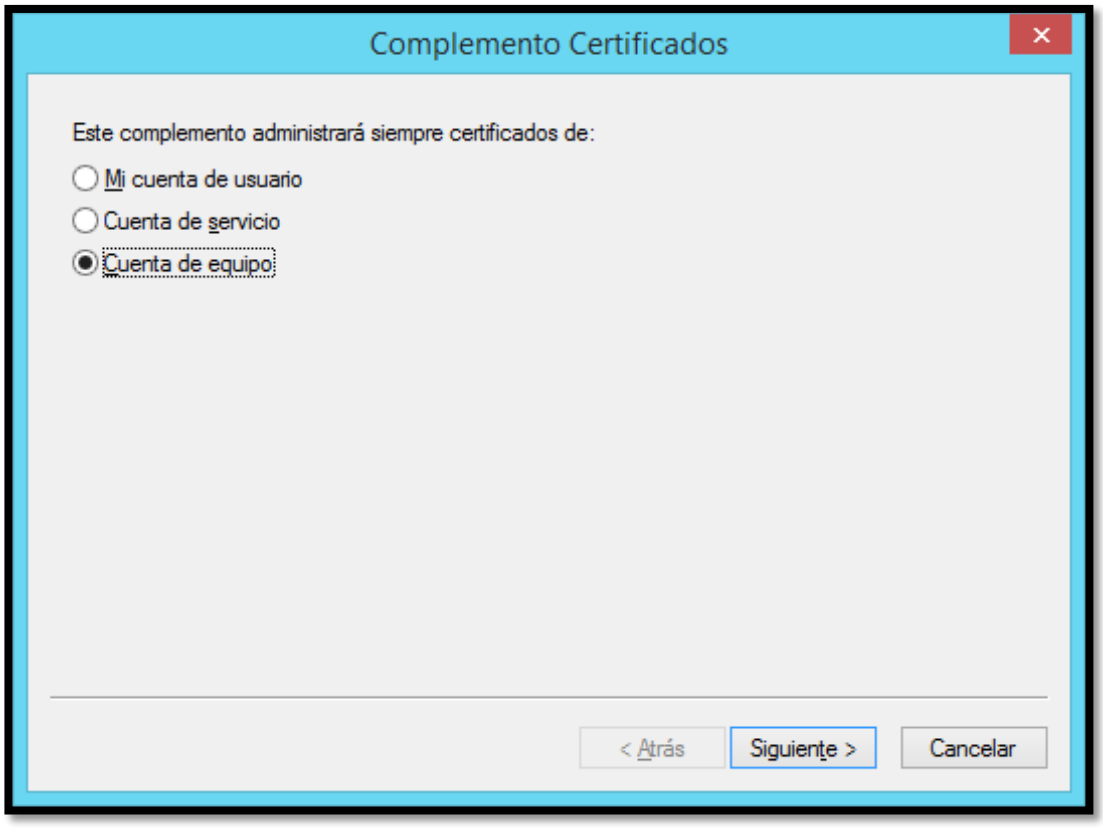
Figura 44. Agregar componente Certificados a la consola de administración



Fuente: Autores del proyecto

El asistente despliega el cuadro de dialogo "**Complemento certificados**" y seleccionamos la opción "**Cuenta de equipo**" y hacemos clic en el botón "**Siguiente**". (Véase la figura 45).

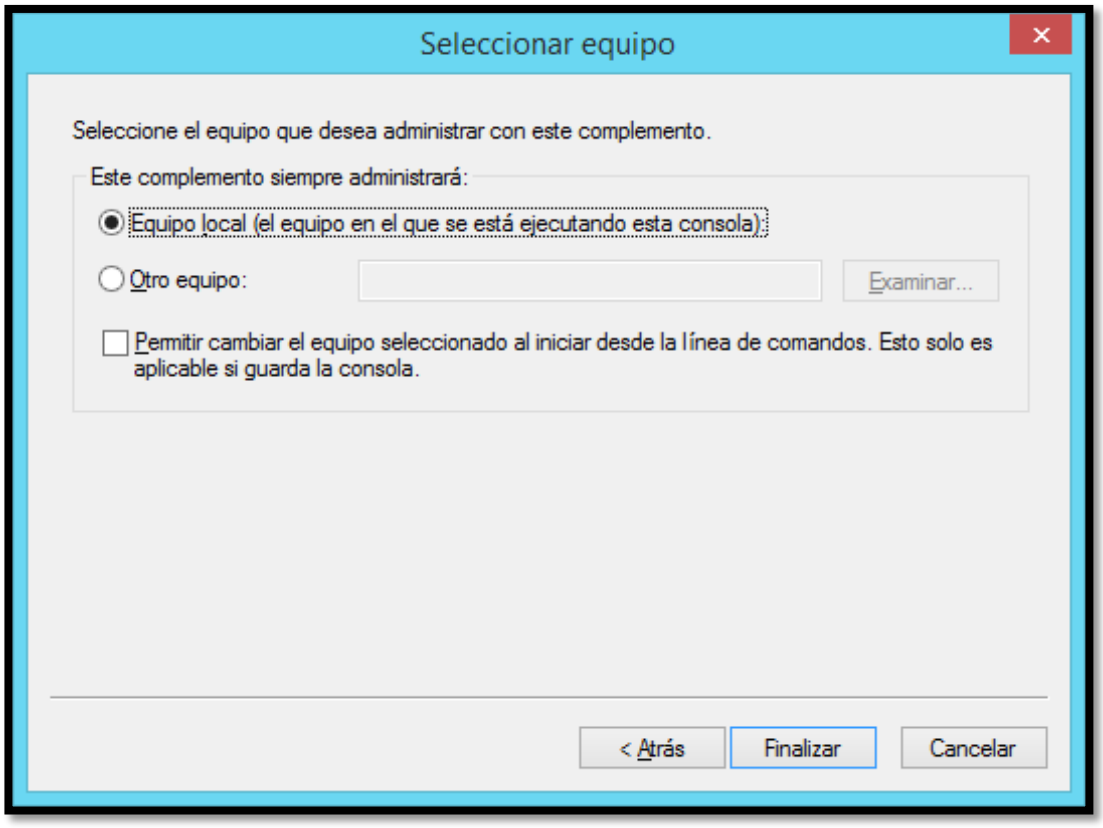
Figura 45. Selección de almacenes de certificados para administración



Fuente: Autores del proyecto

El asistente nos permite seleccionar el equipo que desea administrar el certificado, seleccionamos la opción "**Equipo local (el equipo en el que se está ejecutando la consola)**" y hacemos clic en el botón "**Finalizar**". (Véase la figura 46).

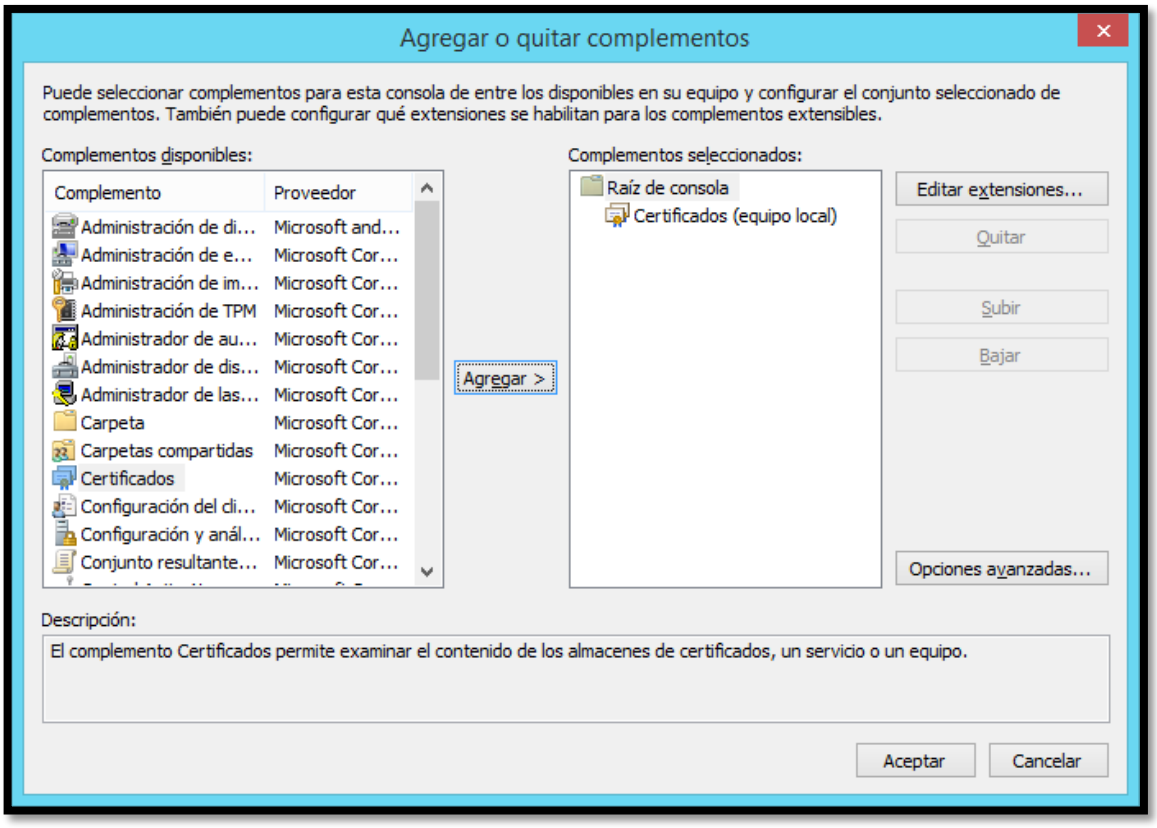
Figura 46. Selección de equipo para administración de certificados



Fuente: Autores del proyecto

Se mostrara el complemento "**Certificados**" agregado correctamente, finalmente hacemos clic en el botón "**Aceptar**".

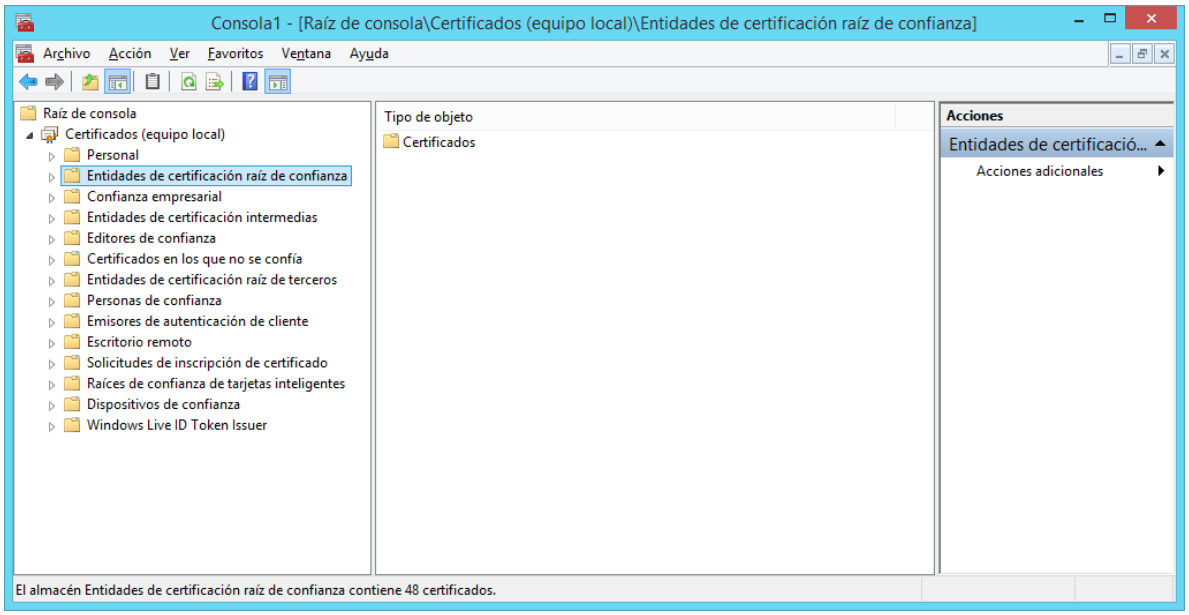
Figura 47. Componente Certificados agregado a la consola de administración



Fuente: Autores del proyecto

En la consola de administración, seleccionamos de la parte izquierda el complemento "**Certificados (Equipo local)**" para expandir y observar las subcategorías. (Véase la figura 48).

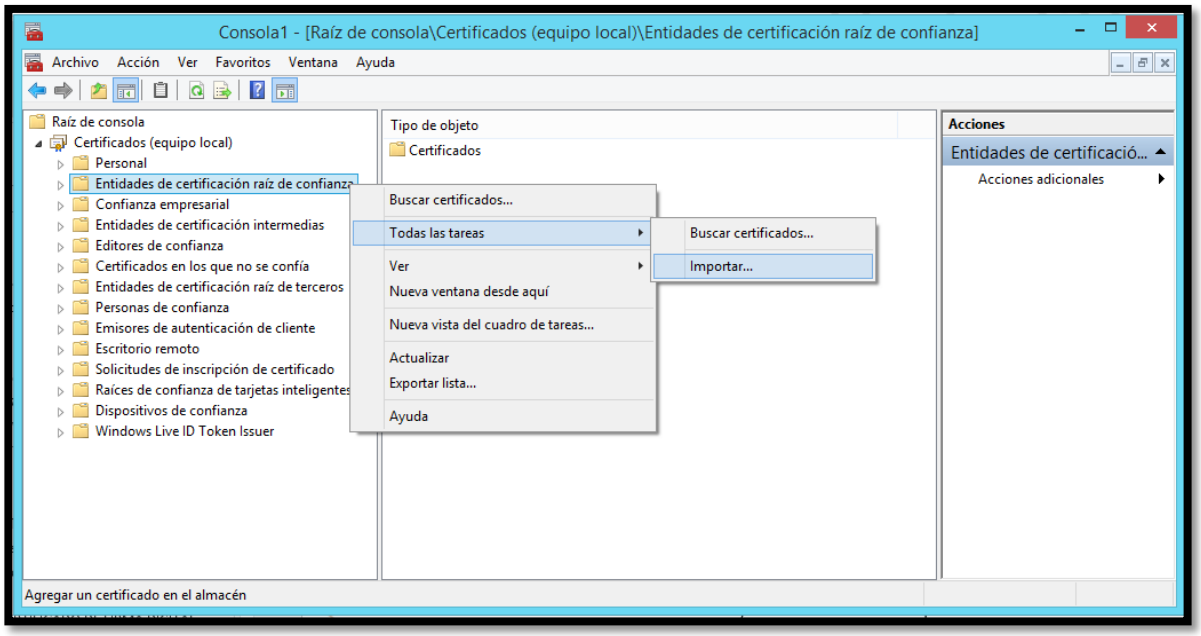
Figura 48. Consola de administración de Windows para la gestión de certificados



Fuente: Autores del proyecto

Hacemos clic derecho sobre la subcategoría denominada "**Entidades de certificación de confianza**" y seleccionamos "**Todas las tareas**" y luego la opción "**Importar**". (Véase la figura 49).

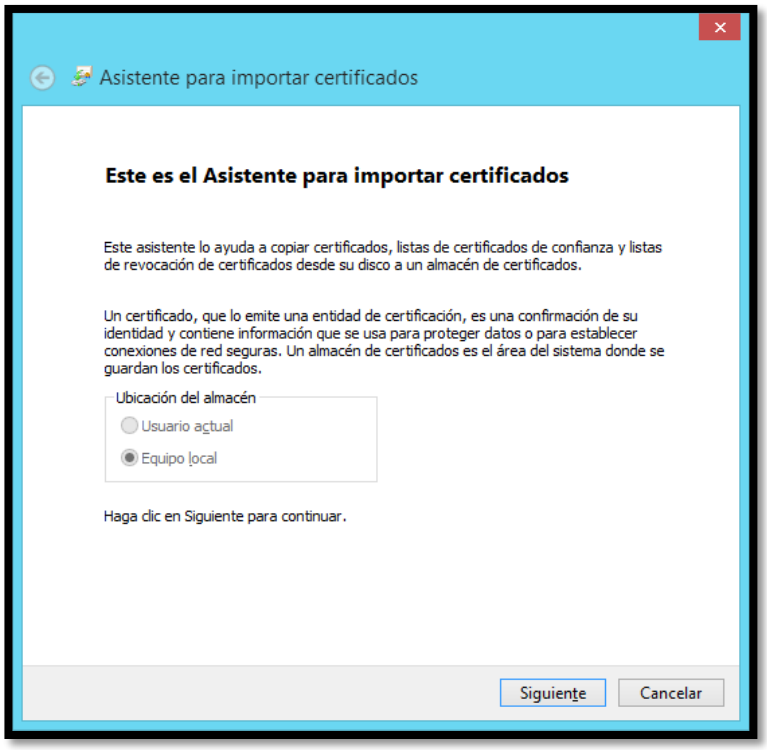
Figura 49. Proceso para importar certificados de entidades de certificación raíz de confianza



Fuente: Autores del proyecto

Se abrirá el cuadro de dialogo "**Asistente para importar certificados**", indicando que el almacén para el certificado será "**Equipo local**", hacemos clic en el botón "**Siguiente**" para continuar. (Véase la figura 50).

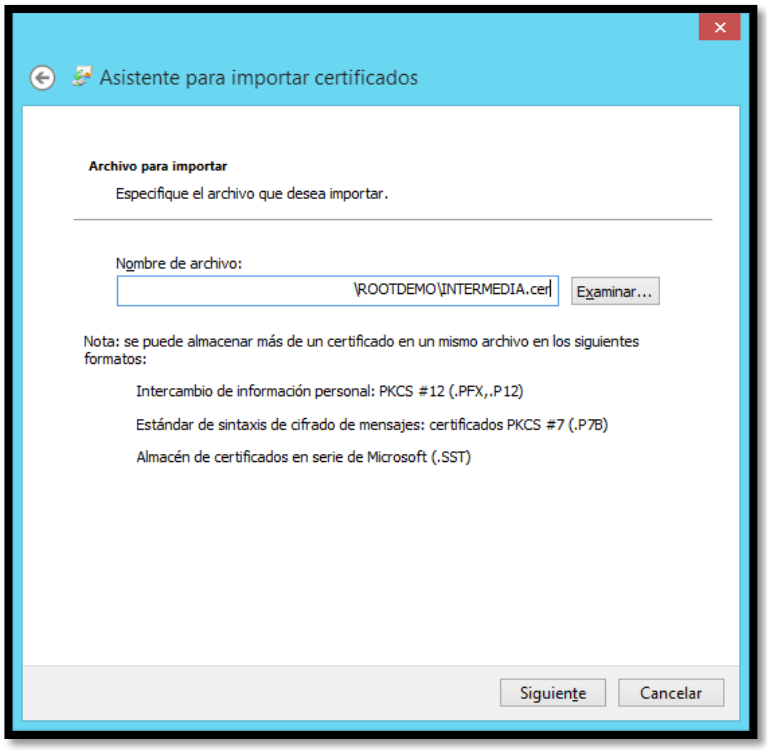
Figura 50. Asistente para importar certificados



Fuente: Autores del proyecto

El asistente solicita la ruta del archivo a importar, para seleccionar el archivo hacemos clic en el botón "**Examinar**" y nos desplazamos por el explorador hasta la carpeta que contiene el certificado, una vez localizado lo seleccionamos y hacemos clic en el botón "**Abrir**", finalmente para continuar clic en el botón "**Siguiente**". (Véase la figura 51).

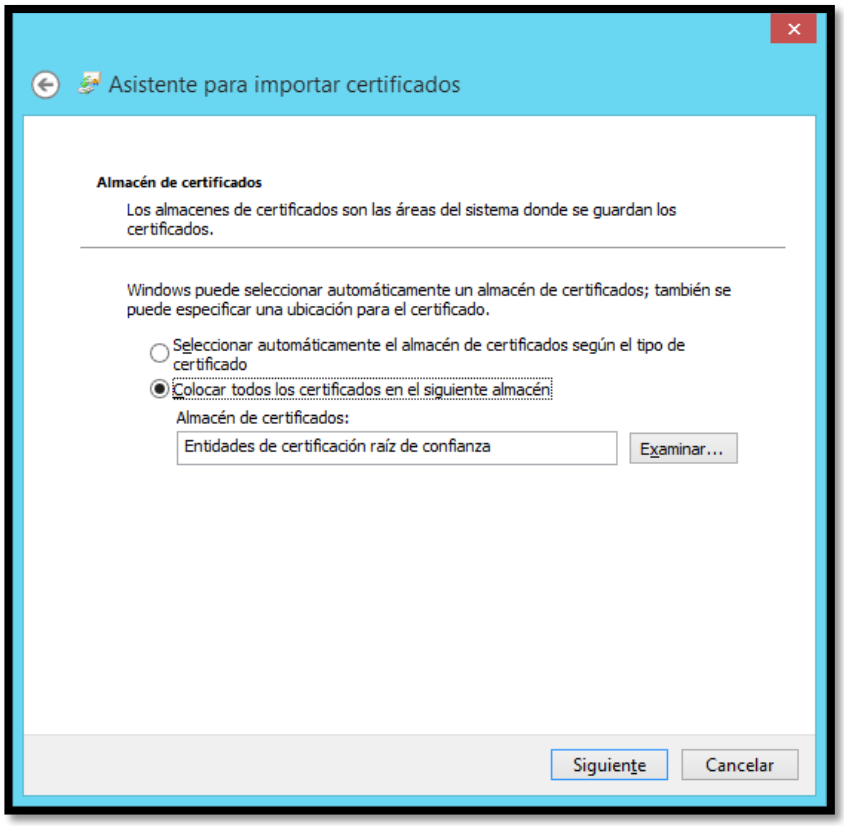
Figura 51. Asistente para importar certificados, selección de archivo para importar



Fuente: Autores del proyecto

El asistente automáticamente seleccionara el almacén donde se almacenara el certificado raíz, este es "**Entidades de certificación raíz de confianza**" y hacemos clic en el botón "**Siguiente**". (Véase la figura 52).

Figura 52. Asistente para importar certificados, selección de almacén Entidades de certificación raíz de confianza

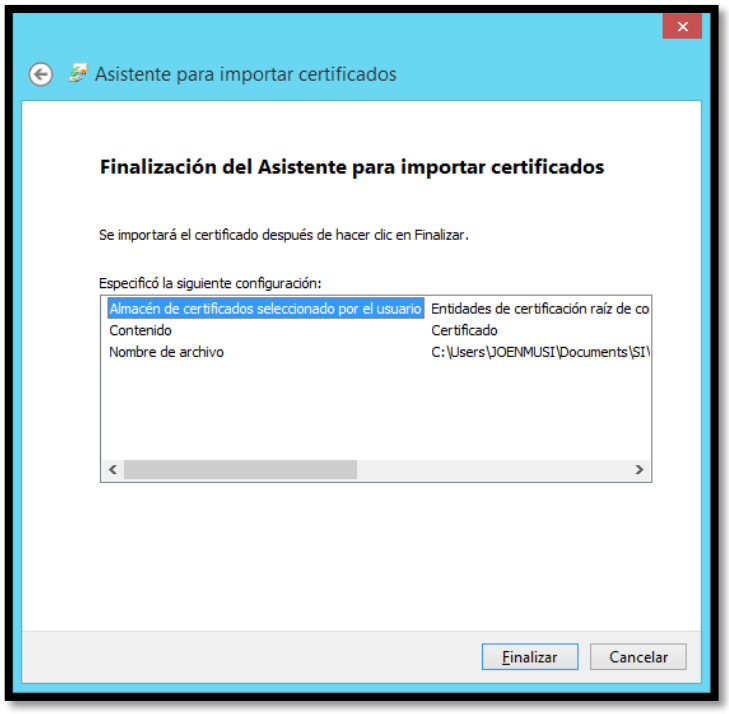


Fuente: Autores del proyecto

Advertencia: Para el correcto funcionamiento del certificado raíz de vital que no se modifique el almacén que selecciona el asistente.

El asistente muestra un resumen de la importación del certificado raíz, procedemos a hacer clic en el botón "**Finalizar**". (Véase la figura 53).

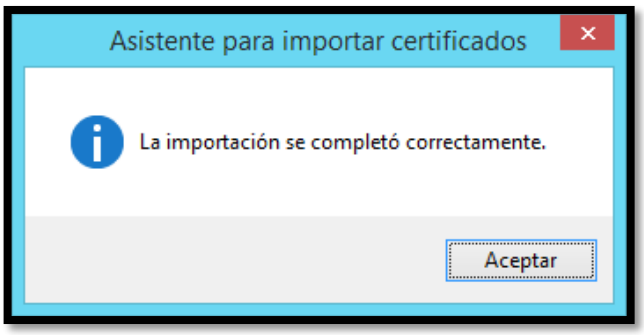
Figura 53. Asistente para importar certificados, resumen de configuración



Fuente: Autores del proyecto

El asistente informa que "**La importación se completó correctamente**", hacemos clic en "**Aceptar**" para cerrar el cuadro de dialogo.

Figura 54. Respuesta de confirmación del proceso de importación de certificados



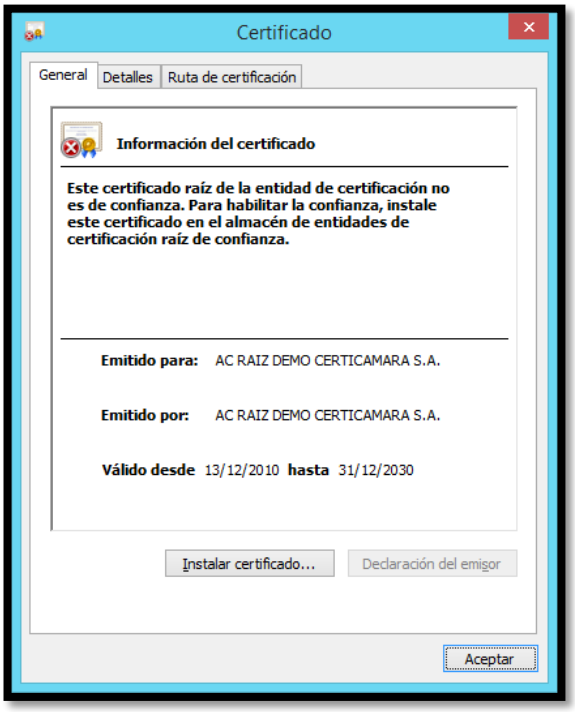
Fuente: Autores del proyecto

Nota: El procedimiento se debe realizar con los dos certificados raíz suministrados por la entidad de certificación, se puede utilizar los dos métodos propuestos.

10.2. MEDIANTE ASISTENTE PARA IMPORTAR CERTIFICADOS

Sobre el certificado raíz denominado "**ROOTDEMO.cer**" y se abrirá un cuadro de dialogo con información del certificado. (Véase la figura 55).

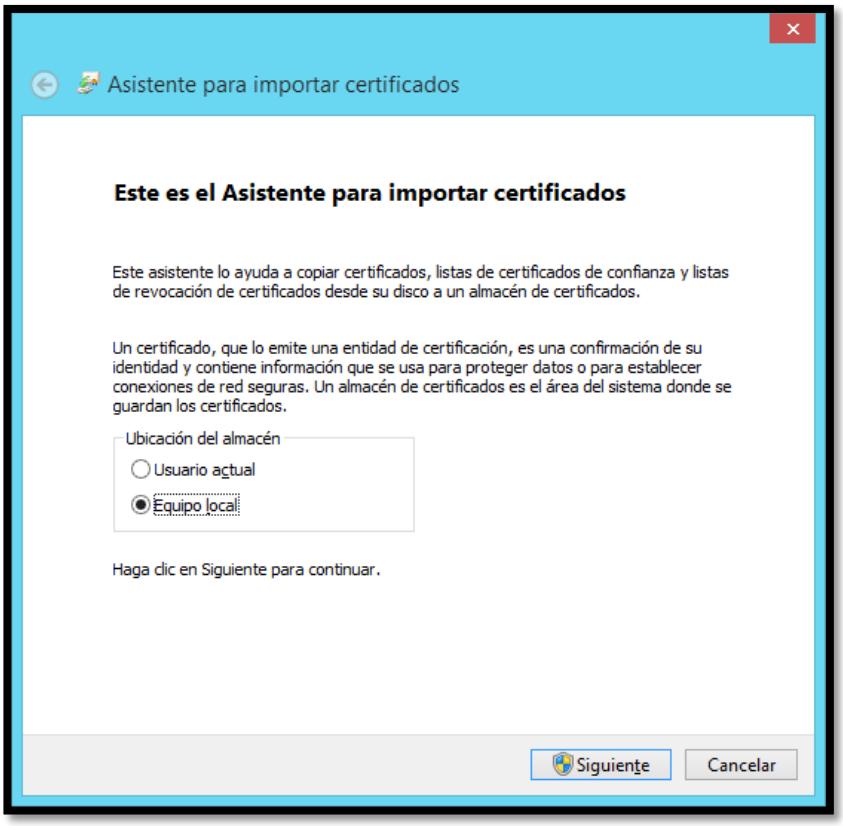
Figura 55. Información general y detalles de certificado raíz



Fuente: Autores del proyecto

Para continuar con el proceso hacemos clic en el botón de la parte inferior "**Instalar certificado…**", se abrirá un cuadro de dialogo con el "**Asistente para importar certificados**", seleccione la ubicación del almacén en "**Equipo local**" y haga clic en el botón "**Siguiente**" para continuar. (Véase la figura 56).

Figura 56. Asistente para importar certificados, selección de almacén

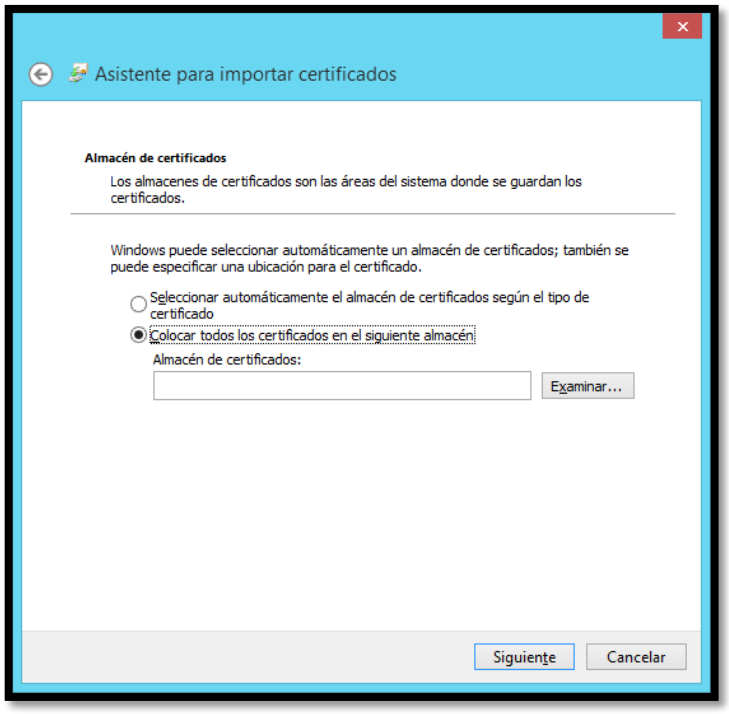


Fuente: Autores del proyecto

Advertencia: Dependiendo de la configuración del equipo de cómputo este procedimiento pedirá autorización para realizar cambios en su sistema, debe aceptar haciendo clic en el botón "**Si**" para que se realice exitosamente.

El asistente solicitara la ubicación del almacén para guardar el certificado, seleccione la opción "**Colocar todos los certificados en el siguiente almacén**". (Véase la figura 57).

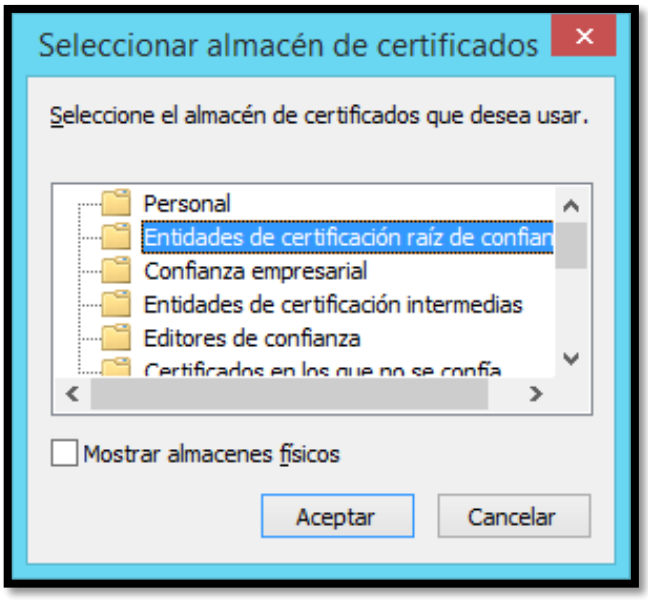
Figura 57. Asistente para importar certificados, selección de almacén



Fuente: Autores del proyecto

Para continuar haga clic en el botón "**Examinar**", se abrirá el cuadro de dialogo "**Seleccionar almacén de certificados**" seleccionamos la opción "**Entidades de certificación raíz de confianza**" y hacemos clic en el botón "**Aceptar**". (Véase la figura 58).

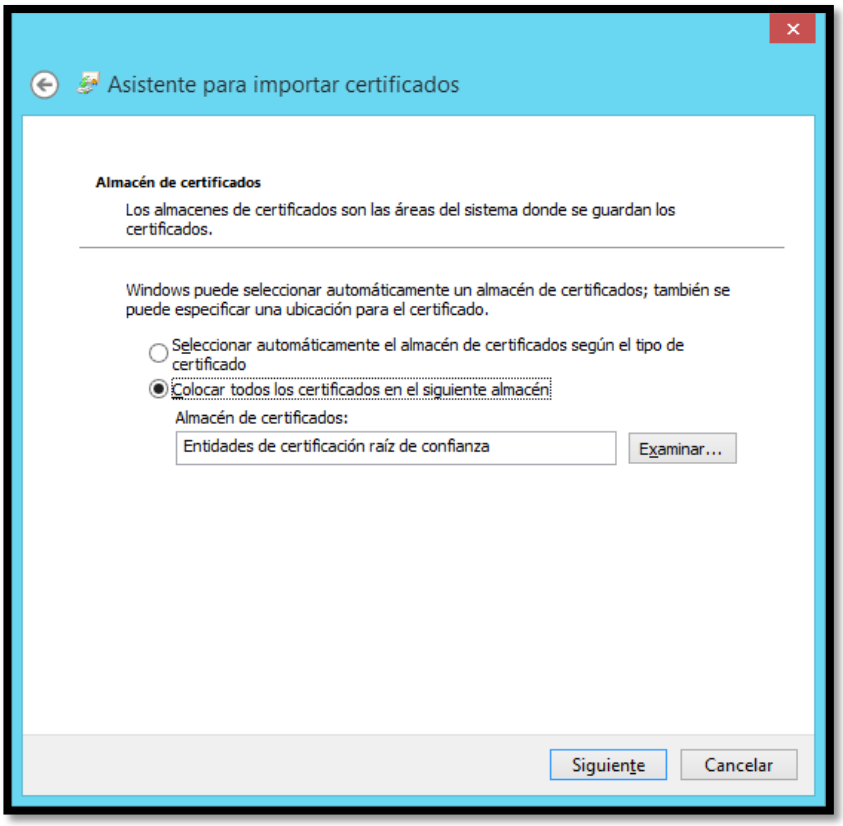
Figura 58. Seleccionar almacén de certificados



Fuente: Autores del proyecto

Una vez seleccionado el almacén donde se almacenara el certificado raíz, este es "**Entidades de certificación raíz de confianza**" y procedemos a hacer clic en el botón "**Siguiente**". (Véase la figura 59).

Figura 59. Asistente para importar certificados, selección de almacén de certificados entidades de certificación de confianza

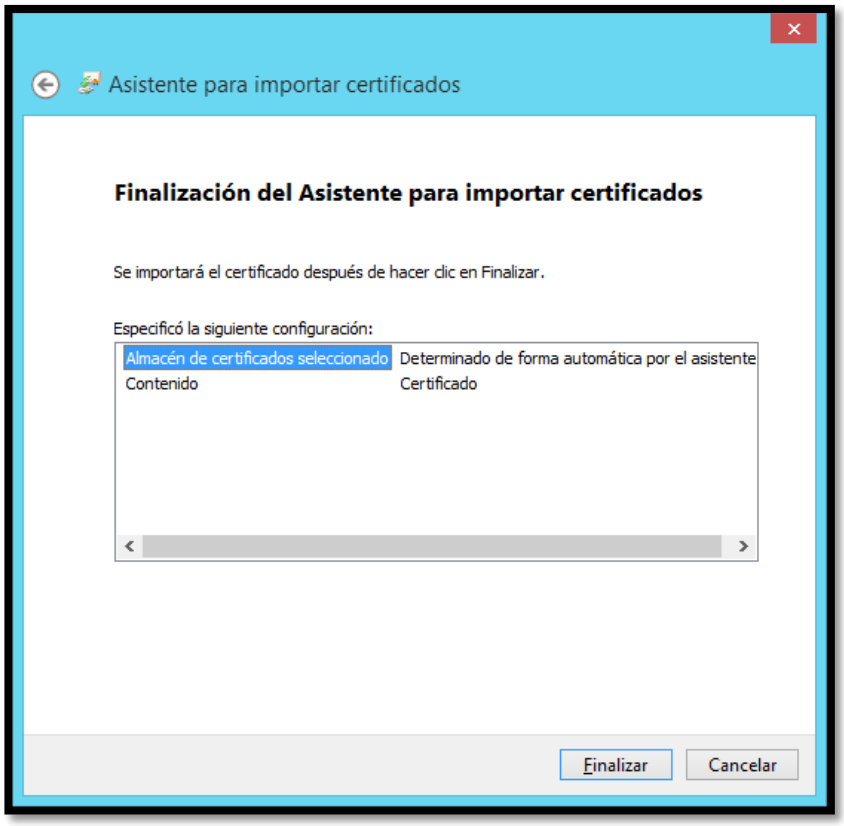


Fuente: Autores del proyecto

Advertencia: Para el correcto funcionamiento del certificado raíz de vital que no se modifique el almacén que selecciona el asistente.

El asistente muestra un resumen de la importación del certificado raíz, procedemos a hacer clic en el botón "**Finalizar**". (Véase la figura 60).

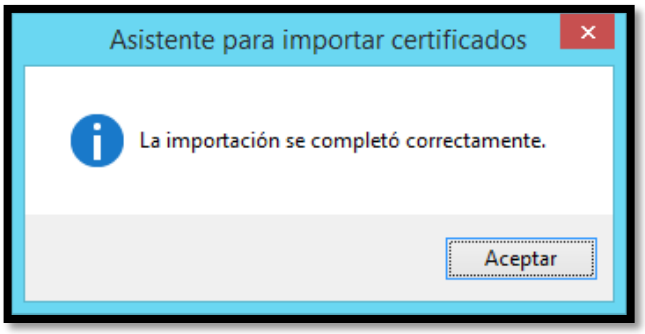
Figura 60. Asistente para importar certificados, resumen de configuración



Fuente: Autores del proyecto

El asistente finalmente mostrara un cuadro de dialogo que indica que "**La importación se completó correctamente**", hacemos clic en el botón "**Aceptar**" para cerrar el cuadro de dialogo. (Véase la figura 61).

Figura 61. Respuesta de confirmación del proceso de importación de certificados



Fuente: Autores del proyecto

Nota: El procedimiento se debe realizar con los dos certificados raíz suministrados por la entidad de certificación, se puede utilizar los dos métodos propuestos.

11. FIRMA DIGITAL

Con el objetivo de incentivar el uso de las nuevas tecnologías, sus beneficios y así mismo contrarrestar los riesgos inherentes a los constantes avances y nuevos desarrollos de la misma, las firmas digitales son una herramienta fundamental en el comercio electrónico de hoy y soporte para todas las transacciones electrónicas con total validez y valor probatorio, NO por ello implica el contar con conocimientos avanzados para su adecuado uso, a continuación se desarrollan los pasos para realizar la instalación de las herramientas software necesarias y los pasos para ejecutar la firma digital sobre todos los documentos electrónicos que así lo requieran.

11.1. CERTITOOL

Es una herramienta desarrollada por CERTICÁMARA con el objetivo de realizar la firma digital de documentos electrónicos.

11.1.1. Requerimientos Técnicos. Para el adecuado funcionamiento de la herramienta se requieren los siguientes requerimientos técnicos:

- ✓ Sistema Operativo:
  - Windows XP Service Pack 3
  - Windows Vista - Arquitecturas de 32 y 64 bits
  - Windows 7 - Arquitecturas de 32 y 64 bits
  - Windows 8 - Arquitecturas de 32 y 64 bits
- ✓ Espacio en Disco duro
  - 20 Mb de espacio disponible en el disco duro
- ✓ Memoria RAM
  - 256 Mb de Memoria RAM

- ✓ Procesador
  - ➢ Procesador con velocidad de 800 MHZ o superior

11.1.2. Proceso de Instalación

La instalación de la herramienta se puede realizar a través de la memoria flash USB suministrada al realizar la inscripción en la plataforma CLIF, también es posible realizar la descarga desde la web de CERTICÁMARA O desde enlace desde el sitio web de la plataforma CLIF.

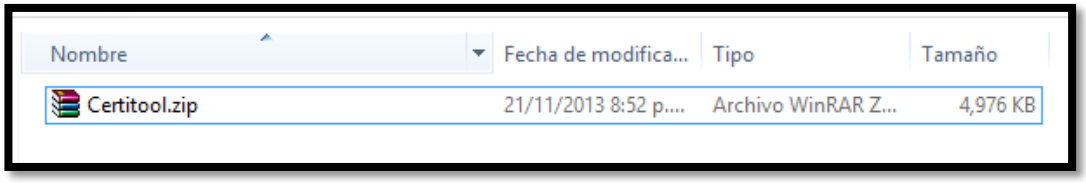
Figura 62. Medios de obtención de la herramienta certitool

USB
• Memoria USB entregada a la hora de la inscripción .
Certicamara
• http://www.certicamara.com/download/CentroDescargas/Certitool.zip.
CLIF
• http://www.clif.co/descargas/firmadigital/certitool.zip

Fuente: Autores del proyecto

Al realizar la descarga en una ubicación fácilmente accesible como "**Escritorio**" se obtendrá un archivo comprimido con el instalador (Véase la figura 63).

Figura 63. Archivo comprimido con el instalador de la herramienta certitool



Fuente: Autores del proyecto

Para poder continuar es necesario realizar la descompresión para obtener el instalador de la herramienta; es posible realizar la descompresión con una herramienta gratuita llamada 7zip. Descargar de la siguiente los siguientes enlaces y realizar la instalación que costa de pocos y sencillos pasos.

Figura 64. Enlaces de descarga herramienta 7Zip

7Zip - Arquitecturas 32 bits

- http://downloads.sourceforge.net/sevenzip/7z920.msi

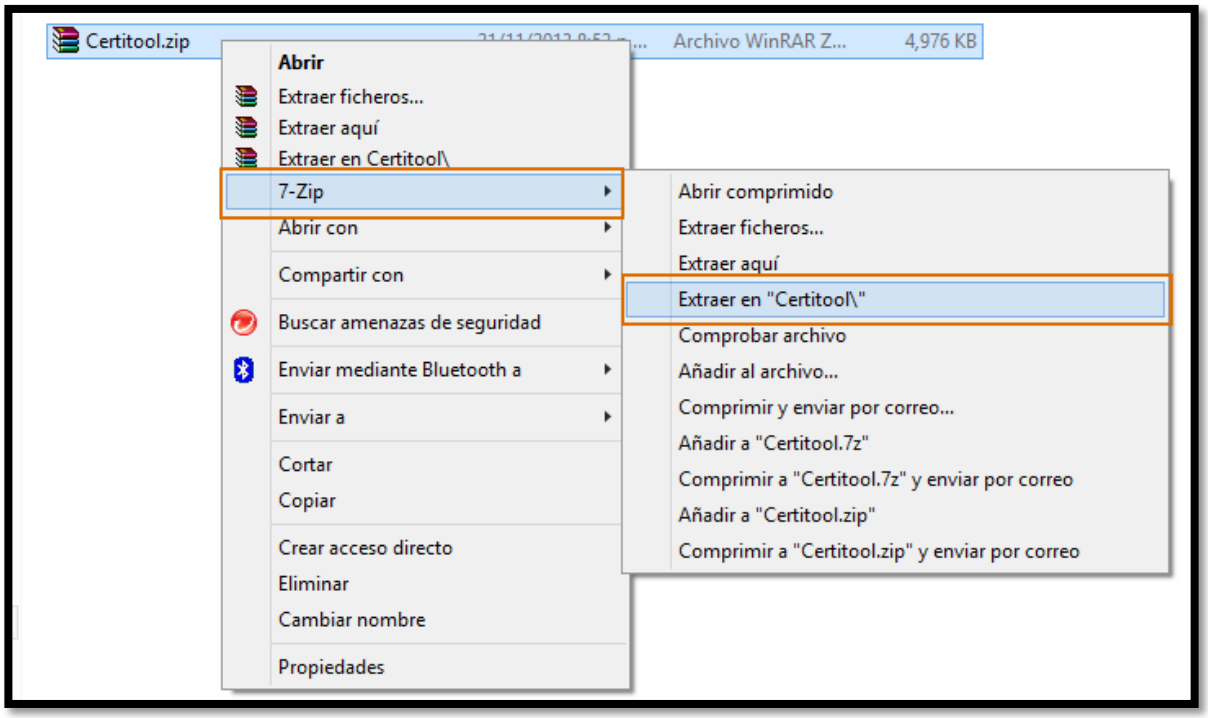
7Zip - Arquitectura 64 Bits

- http://downloads.sourceforge.net/sevenzip/7z920-x64.msi

Fuente: Autores del proyecto

Ejecutamos la descompresión del instalador haciendo clic derecho sobre el archivo descargado denominado "**Certitool.zip**", buscamos dentro del menú contextual la opción 7-Zip y dentro del submenú la opción Extraer en "**Certitool**", (Véase la figura 65).

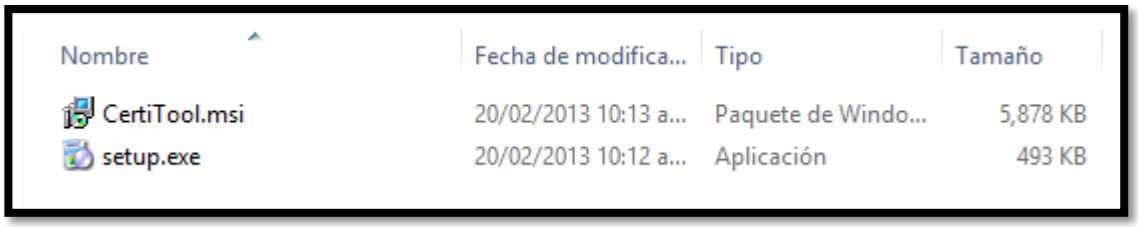
Figura 65. Proceso para realizar descompresión de los archivos mediante 7Zip



Fuente: Autores del proyecto

Esperamos a que se realice la descompresión de la herramienta y obtendremos la carpeta, nos desplazamos en ellas hasta ubicar el instalador de Certitool, (Véase la figura 66).

Figura 66. Archivos de instalación herramienta certitool



Fuente: Autores del proyecto

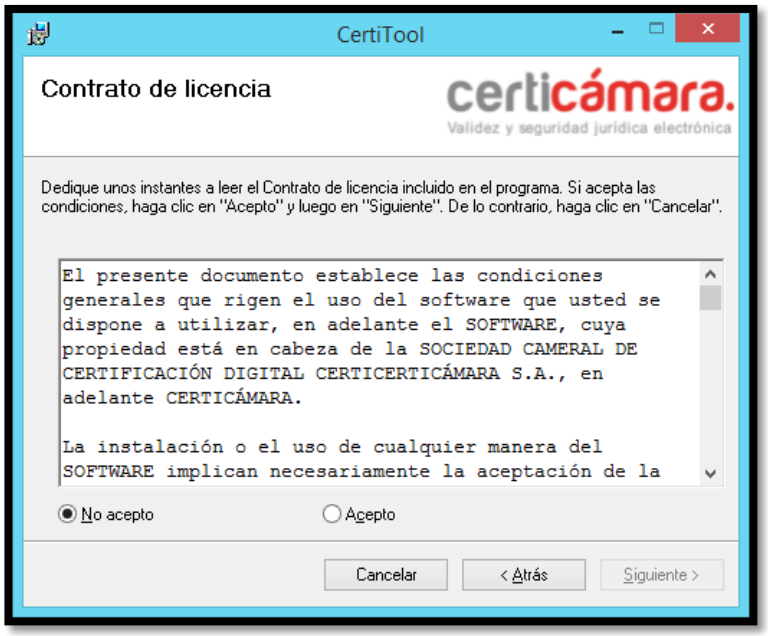
Procedemos con la instalación de la herramienta Certitool haciendo doble clic sobre el archivo "**setup.exe**", esperamos unos segundos a que se muestre el asistente que nos guiara durante el proceso de instalación (Véase la figura 67).

Figura 67. Asistente de instalación certitool

Fuente: Autores del proyecto

Para poder realizar la instalación de la herramienta se debe contar con privilegios de administrador. Procedemos con la instalación haciendo clic en el botón "**Siguiente**". Se muestra el contrato de licencia de uso de la herramienta (Véase la figura 68).

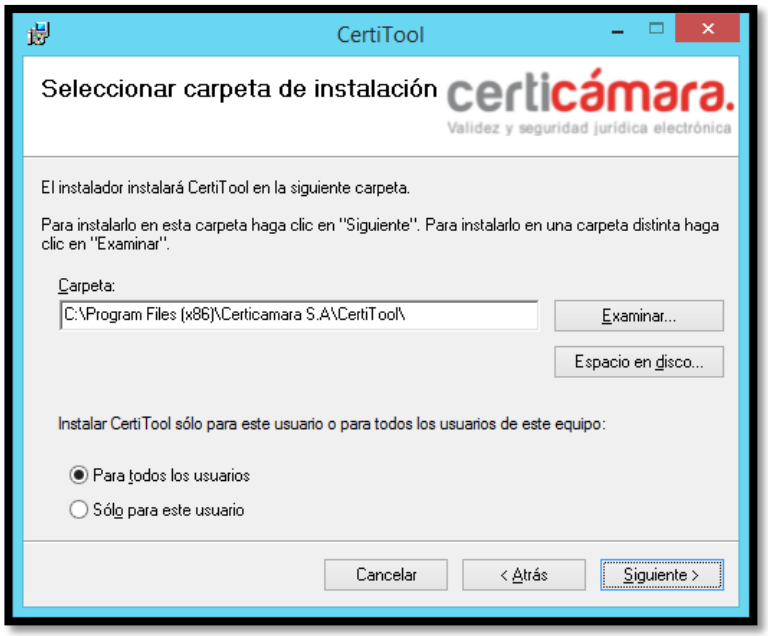
Figura 68. Asistente de instalación certitool, contrato de licencia



Fuente: Autores del proyecto

Procedemos a realizar la lectura del contrato de licencia de uso y si estamos de acuerdo seleccionamos la opción "**Acepto**" y hacemos clic en "**Siguiente**". Si no se acepta el contrato NO es posible realizar la instalación de la herramienta. El asistente de instalación nos muestra la ruta de instalación predeterminada, es posible seleccionar otra instalación si así lo desea, adicionalmente permite seleccionar si la herramienta estará disponible solo para el usuario actual o todos los usuarios del equipo. (Véase la figura 69).

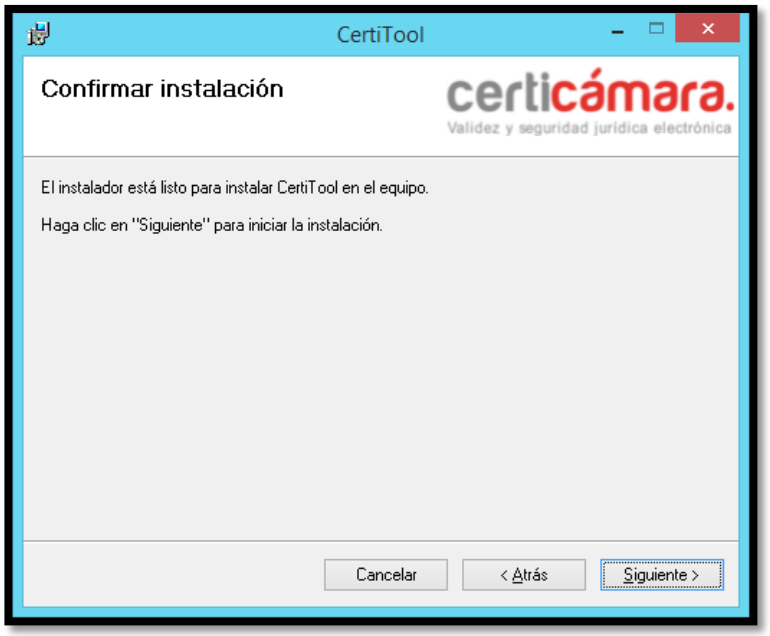
Figura 69. Asistente de instalación certitool, seleccionar carpeta de instalación



Fuente: Autores del proyecto

A continuación realizamos clic en "**Siguiente**", el asistente nos indica que el instalador está listo (Véase la figura 70).

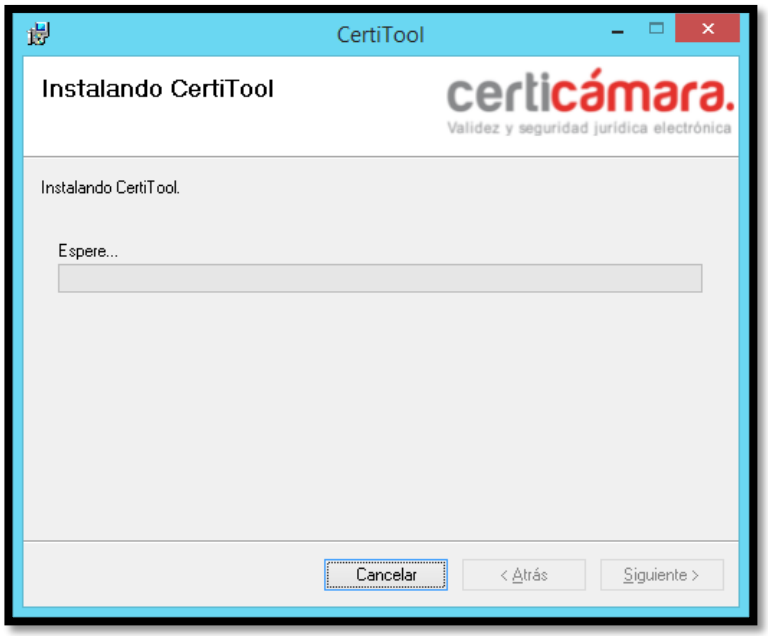
Figura 70. Asistente de instalación certitool, confirmar instalación



Fuente: Autores del proyecto

Para iniciar la instalación procedemos en hacer clic en "**Siguiente**". (Véase la figura 71).

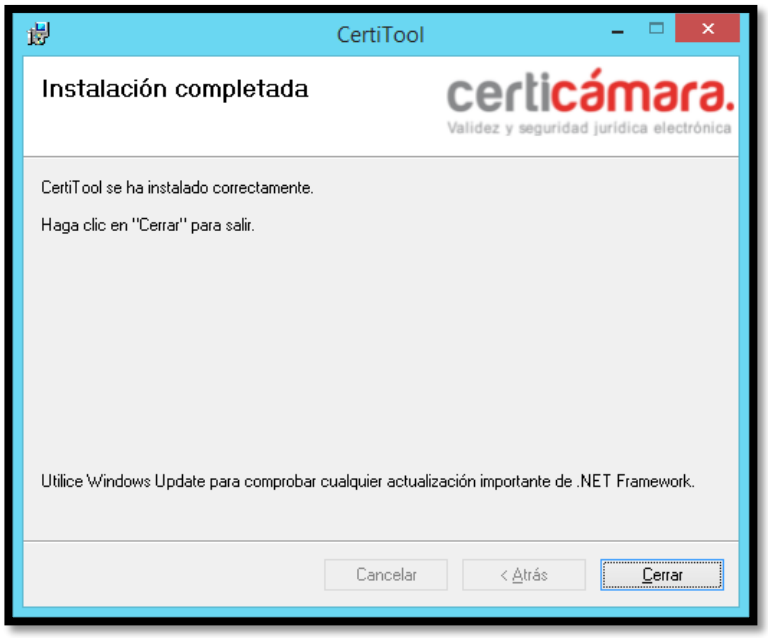
Figura 71. Asistente de instalación certitool, progreso de la instalación



Fuente: Autores del proyecto

Si durante la instalación nos solicita autorización para realizar operaciones relacionadas con Certitool, hacemos clic en SI, para que la instalación se desarrolle sin inconvenientes. Una vez finalice la instalación, el asistente nos informa que se realizó correctamente. (Véase la figura 72).

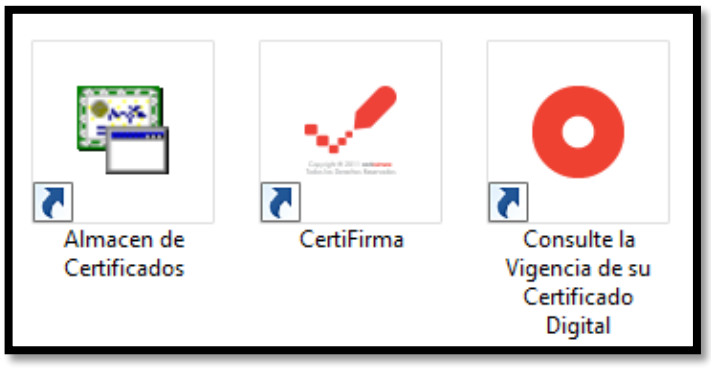
Figura 72. Asistente de instalación certitool, instalación completada



Fuente: Autores del proyecto

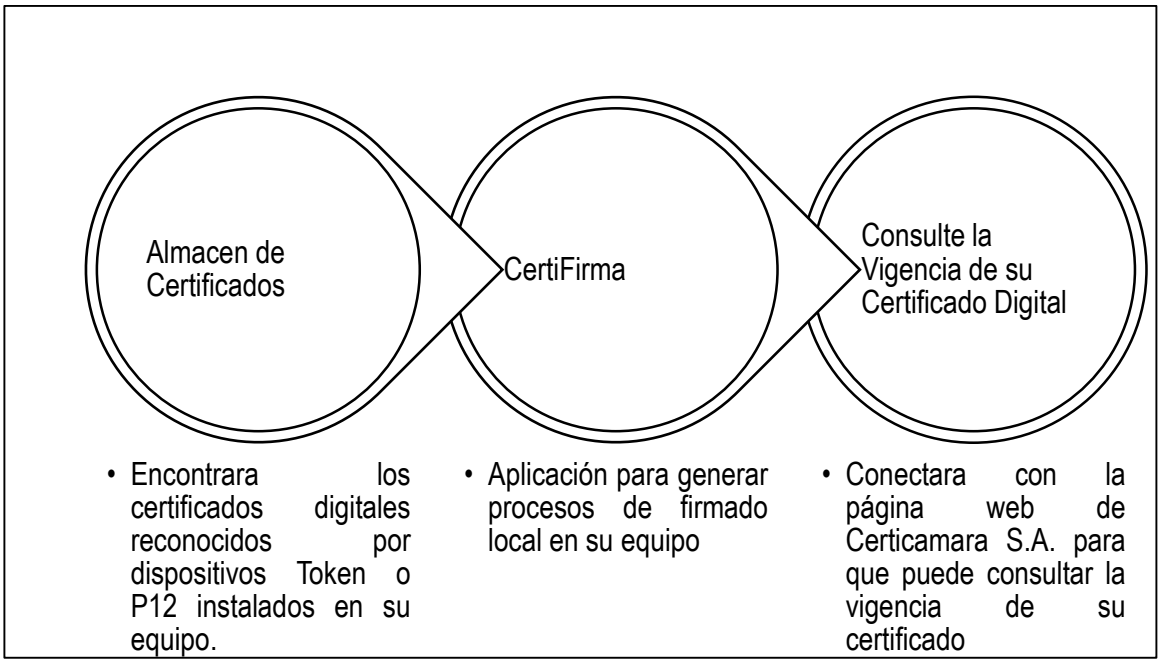
Finalmente hacemos clic en el botón "**Cerrar**" y debemos encontrar en el "**Escritorio**" del equipo 3 accesos directos a las herramientas instaladas por Certitool. (Véase la figura 73).

Figura 73. Accesos directos instalados por la herramienta certitool



Fuente: Autores del proyecto

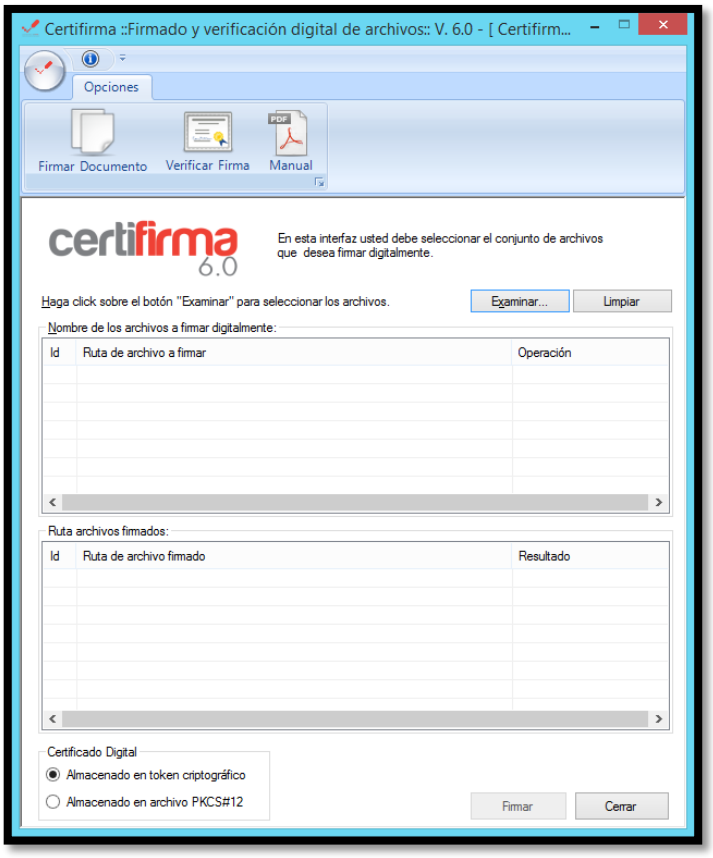
Figura 74. Funciones de las herramientas instaladas por certitool



Fuente: Autores del proyecto

Ejecutando "**Certifirma**" podemos visualizar su interfaz para realizar la firma Digital.

Figura 75. Interfaz de la herramienta certitool

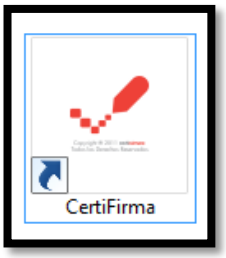


Fuente: Autores del proyecto

11.1.3. Firma digital mediante CertiTool. Para realizar la firma digital de los diferentes documentos electrónicos se deben haber completado previamente los procedimientos para "**Obtención de certificados de firma digital**", "**Generación de certificados de firma digital**", "**Instalación de certificado de firma digital**" e "**Instalación de certificado raíz**", adicionalmente se debe tener instalada la herramienta "**Certitool**" y estar almacenado en el equipo de cómputo el certificado de firma digital en formato "**p12**".

Para iniciar el proceso de firma digital buscamos en el escritorio el acceso directo a la aplicación "**Certifirma**" y hacemos doble clic. (Véase la figura 76).

Figura 76. Icono de acceso directo a certifirma



Fuente: Autores del proyecto

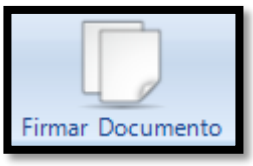
Se abrirá la interfaz de la aplicación, esta está compuesta por dos opciones principales, la primera "**Firmar documento**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información y la segunda "**Verificar firma**" que nos permitirá constatar la firma realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 77).

Figura 77. Interfaz inicial de certitool

Fuente: Autores del proyecto

Procedemos a hacer clic en la opción "**Firmar documento**". (Véase la figura 78).

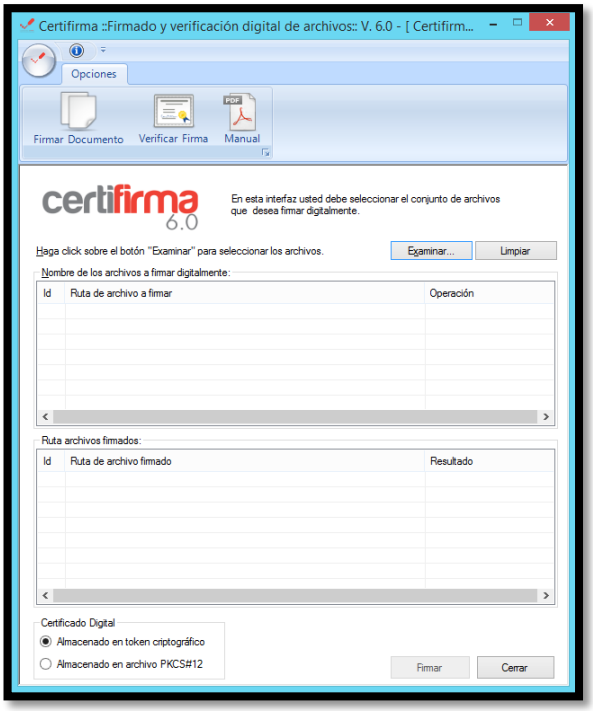
Figura 78. Botón firmar documento de la interfaz de certitool



Fuente: Autores del proyecto

La herramienta "**Certifirma**" muestra su interfaz para realizar la firma digital, compuesta por un botón "**Examinar**" que permitirá seleccionar el o los documentos electrónicos que deseamos firmar digitalmente. (Véase la figura 79).

Figura 79. Interfaz de certitool para firmar digitalmente



Fuente: Autores del proyecto

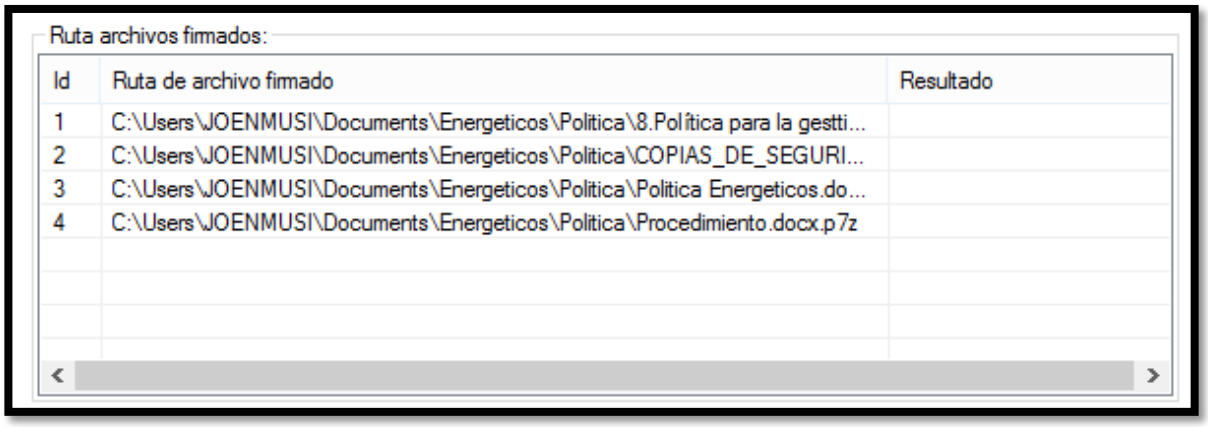
Los documentos agregados se mostraran en una grilla o cuadricula compuesta por un Identificador o consecutivo, una ruta de ubicación de cada uno de los documentos a firmar y una operación deseada para los archivos (Firmar). (Véase la figura 80).

Figura 80. Listado del conjunto de archivos que se desea firmar digitalmente mediante certitool indicando la operación

Fuente: Autores del proyecto

Adicionalmente una segunda grilla o cuadricula mostrara los documentos igualmente con un identificador o consecutivo, una ruta de ubicación de cada uno de los documentos y finalmente una columna que indicará el resultado de la operación de firma digital. (Véase la figura 81).

Figura 81. Listado del conjunto de archivos que se desea firmar digitalmente mediante certitool indicando el resultado de la operación



Fuente: Autores del proyecto

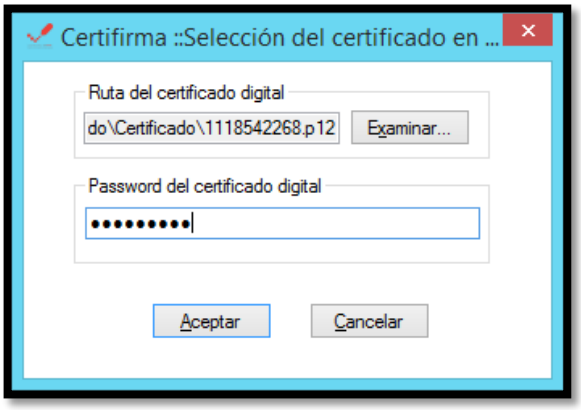
En la parte inferior de la herramienta "**Certifirma**" encontramos dos opciones de donde podemos hacer uso de nuestro certificado de firma digital, para nuestro caso seleccionamos la opción "**Almacenado en archivo PKCS#12**" y hacemos clic en el botón "**Firmar**" para realizar la firma digital de los documentos electrónicos. Si deseamos cerrar la aplicación en cualquier momento podemos hacer clic en el botón "**Cerrar**". (Véase la figura 82).

Figura 82. Selección del tipo de certificado digital en certitool

Fuente: Autores del proyecto

La aplicación "**Certifirma**" desplegará un cuadro de dialogo en el cual hacemos clic en el botón "**Examinar**" y localizamos el certificado de firma digital en formato "**p12**" que deseamos utilizar para realizar la firma de los documentos electrónicos y hacemos clic en el botón abrir para seleccionarlo. (Véase la figura 82).

Figura 83. Cuadro de dialogo para seleccionar la ruta del certificado digital e ingresar la contraseña del mismo

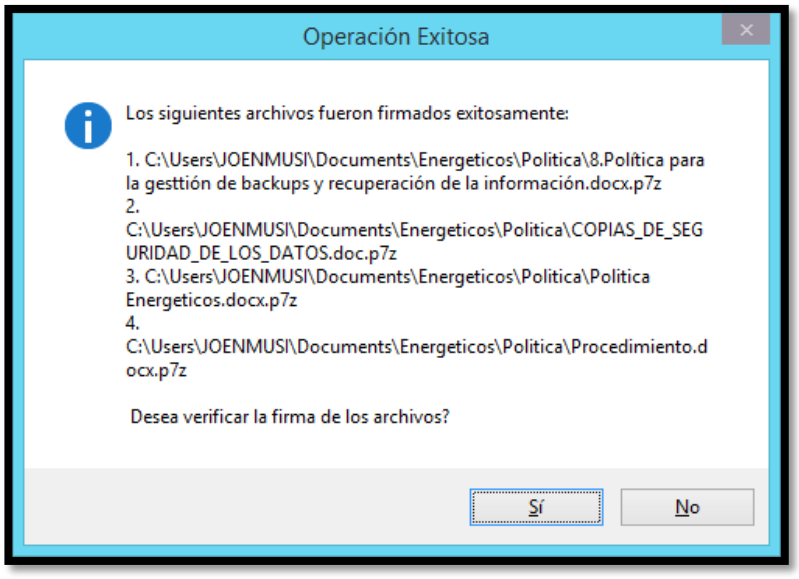


Fuente: Autores del proyecto

Para finalizar el proceso de firma digital ingresamos la contraseña asociada al certificado de firma digital, esta contraseña fue asignada en el procedimiento denominado "**Obtención de certificados de firma digital**" y hacemos clic en el botón "**Aceptar**".

La herramienta "**Certifirma**" genera un cuadro de dialogo que informa que la operación de firma digital fue exitosa y lista la ruta de cada uno de los documentos electrónicos firmados digitalmente. Adicionalmente permite verificar que la firma se aplicó correctamente para ello hacemos clic en el botón "**Si**". (Véase la figura 84).

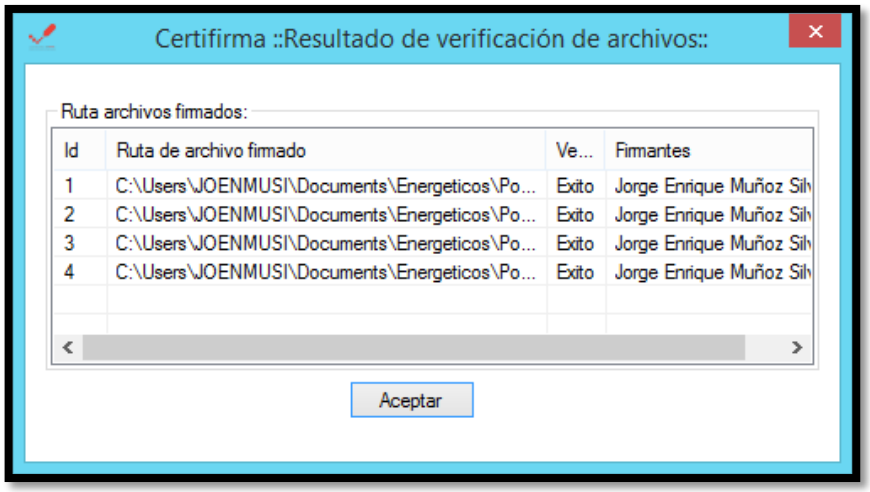
Figura 84. Mensaje de operación de firma digital exitoso de certitool



Fuente: Autores del proyecto

La herramienta genera un cuadro de dialogo con una grilla o cuadricula que muestra un identificador o consecutivo, la ruta de ubicación los documentos electrónicos firmados digitalmente, la verificación de la firma que indica si fue exitosa o no y el titular del certificado digital o firmante. (Véase la figura 85).

Figura 85. Listado de resultados del proceso de firma digital de certitool

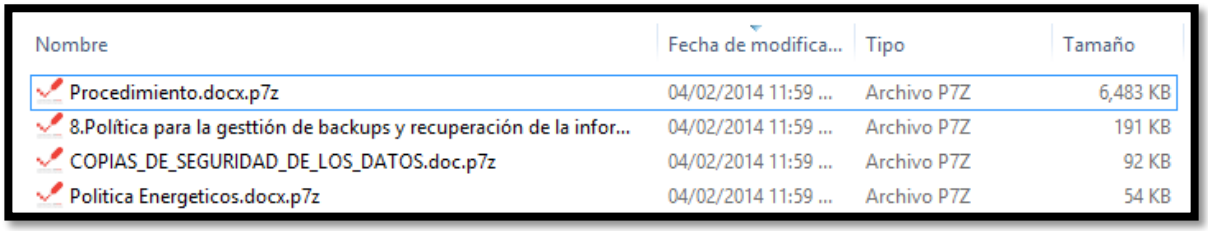


Fuente: Autores del proyecto

Finalmente hacemos clic en el botón "**Aceptar**" para cerrar el cuadro de dialogo "**Resultado de verificación de archivos**".

Podemos observar en la ubicación original de los documentos electrónicos su respectivo documento firmado, con extensión "**p7z**" que indica que el documento está firmado por "**Certifirma**". (Véase la figura 86).

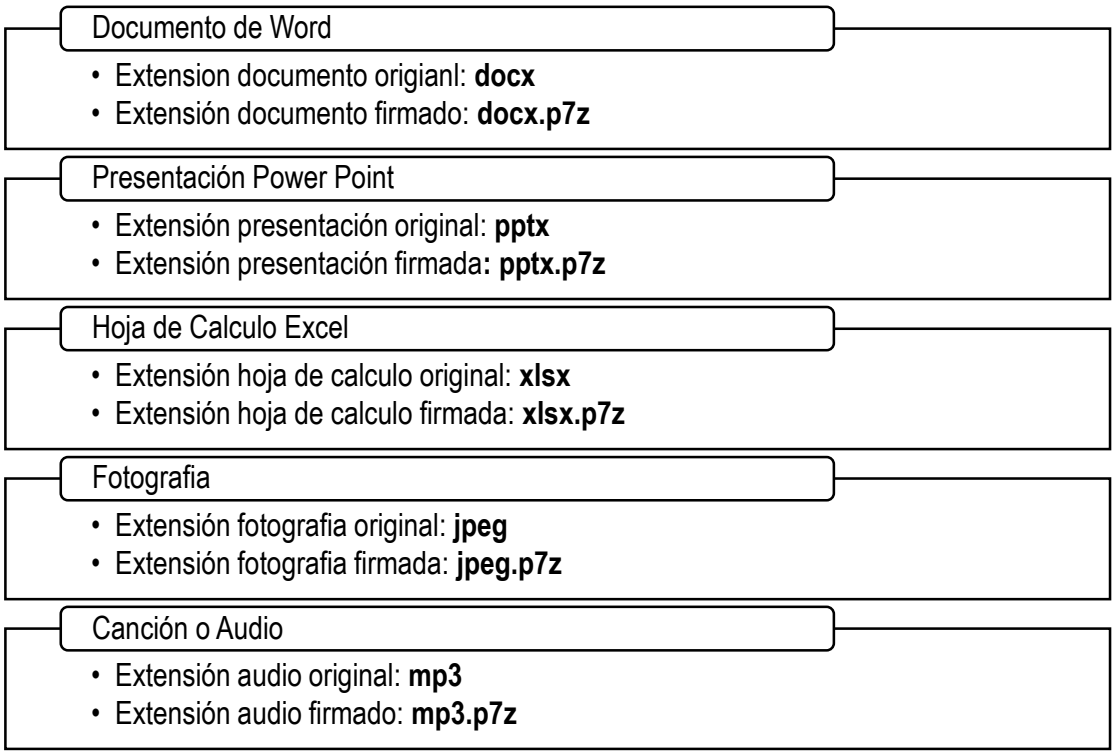
Figura 86. Archivos generados del proceso de firma digital mediante certitool



Fuente: Autores del proyecto

Los archivos al ser firmados digitalmente por la herramienta "**Certifirma**" se les agrega o adiciona una extensión de archivo anexo a la extensión del tipo de archivo que fue firmado, a continuación podemos ver algunos ejemplos de extensiones de documentos electrónicos comunes y sus respectivas extensiones una vez firmados:

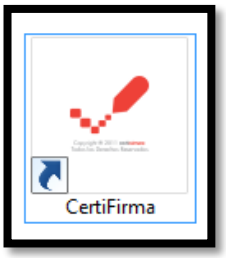
Figura 87. Ejemplos de extensiones de los archivos antes y después del proceso de firma digital mediante certitool



Fuente: Autores del proyecto

11.1.4. Verificar firma digital mediante CertiTool. Para iniciar el proceso de verificación de validez de la firma digital buscamos en el escritorio el acceso directo a la aplicación "**Certifirma**" y hacemos doble clic. (Véase la figura 88).

Figura 88. Icono de acceso directo a certifirma



Fuente: Autores del proyecto

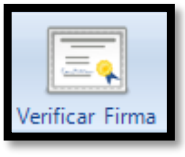
Se abrirá la interfaz de la aplicación, esta está compuesta por dos opciones principales, la primera "**Firmar documento**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información y la segunda "**Verificar firma**" que nos permitirá constatar la firma realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 89).

Figura 89. Interfaz inicial de certitool

Fuente: Autores del proyecto

Procedemos a hacer clic en la opción "**Verificar firma**". (Véase la figura 90)

Figura 90. Botón verificar firma de la interfaz de certitool



Fuente: Autores del proyecto

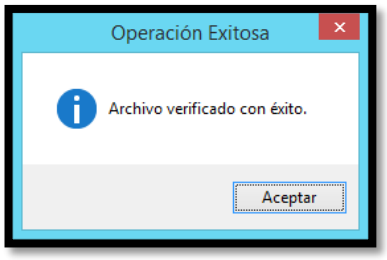
La herramienta "**Certifirma**" muestra su interfaz para realizar la verificación de la firma digital, compuesta por un botón "**Examinar**" que permitirá seleccionar el documento electrónico al que deseamos verificar la validez de la firma digital.

Figura 91. Interfaz de certitool para verificar firma digital

Fuente: Autores del proyecto

Al abrir el archivo la herramienta "**Certifirma**" genera un cuadro de dialogo que informa que el archivo fue verificado con éxito, es decir que este sigue manteniendo su integridad y validez jurídica. (Véase la figura 92).

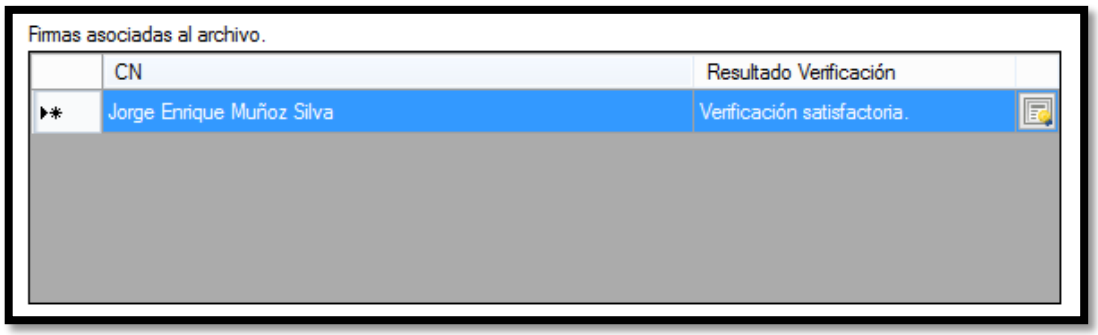
Figura 92. Mensaje de verificación de firma digital exitoso de certitool



Fuente: Autores del proyecto

Las firmas digitales agregadas se mostraran en una grilla o cuadricula compuesta por un el nombre del firmante y un resultado de verificación que indica el estado de la firma en el documento electrónico. (Véase la figura 93).

Figura 93. Listado y valides de las firmas asociadas al archivo firmado con certitool

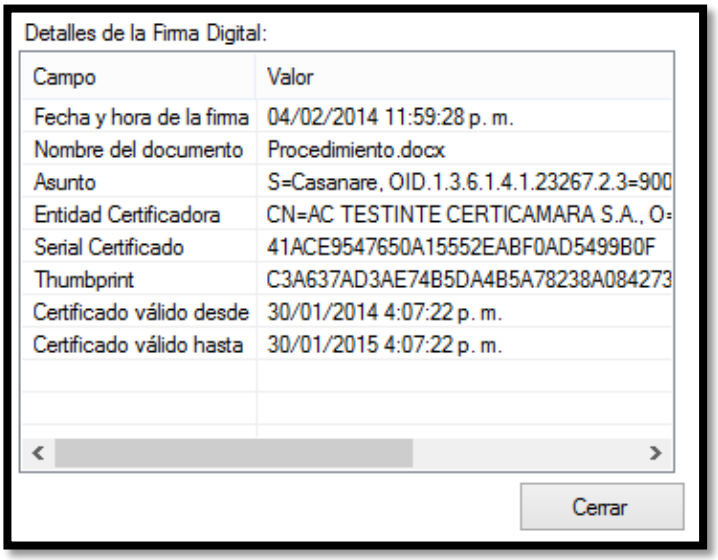


Fuente: Autores del proyecto

Al seleccionar cualquiera de las firmas agregadas al documento electrónico, en la parte inferior derecha de la herramienta “Certifirma” se mostrara la información correspondiente al certificado de firma digital que contra campos que ayudan a soportar la integridad y validez jurídica del documento, algunos de estos campos son:

- ✓ Fecha y hora de la firma
- ✓ Nombre del documento
- ✓ Asunto
- ✓ Entidad certificadora
- ✓ Serial del certificado
- ✓ Fechas de valides del certificado de firma digital

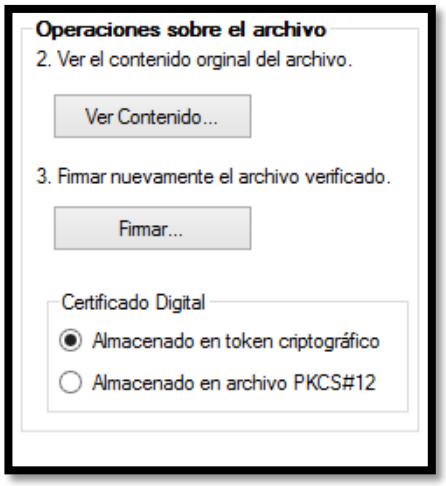
Figura 94. Detalles de la firma digital certitool



Fuente: Autores del proyecto

Adicionalmente la herramienta "**Certifirma**" nos ofrece operaciones sobre el archivo como la posibilidad de "**Ver el contenido original del archivo**" al hacer clic en el botón "**Ver contenido…**" y "**Firmar nuevamente el archivo verificado**" al hacer clic en el botón "**Firmar…**" en caso que el documento que se está verificando requiera firmas adicionales, este proceso se deberá llevar a cabo por cada uno de los firmantes con sus respectivos certificados de firma digital y su contraseña de protección. (Véase la figura 95)

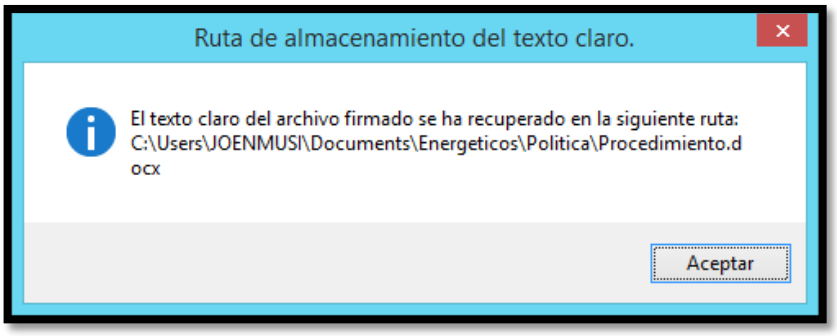
Figura 95. Operaciones disponibles sobre el archivo firmado digitalmente



Fuente: Autores del proyecto

Al hacer clic en el botón "**Ver contenido**" la herramienta "**Certifirma**" genera un cuadro de dialogo informando que el documento electrónico original se ha recuperado e indicando la ruta exacta del documento electrónico, esta ruta será la misma en donde se tenga almacenado el archivo firmado digitalmente con formado "**p7z**". (Véase la figura 96).

Figura 96. Mensaje de operación de extraer el archivo original exitoso después de verificar firma digital mediante certitool

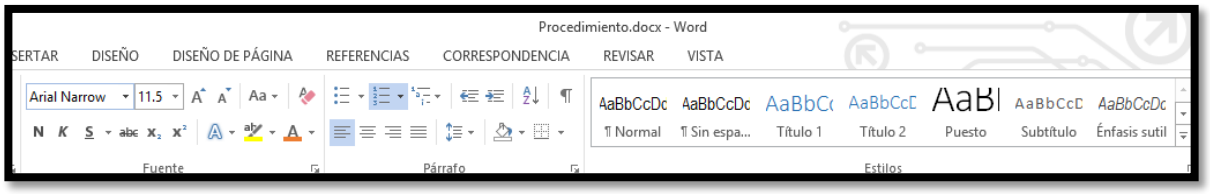


Fuente: Autores del proyecto

Nota: La opción de ver el contenido realiza el proceso inverso a la hora de firmar el documento electrónico referente a que se retira la extensión "**p7z**" dejando el documento en su extensión estándar, por ejemplo "**docx**". Para mayor información revisar la tabla de extensiones comunes en el procedimiento de "**Firma digital mediante CertiTool**".

Una vez observada la ruta del documento electrónico procedemos a hacer clic en el botón "**Aceptar**", seguidamente el documento se abrirá con la aplicación que fue generada, para este ejemplo se abrirá la aplicación "**Microsoft Word**" ya que el documento firmado fue generado con este procesador de texto. (Véase la figura 97).

Figura 97. Interfaz de la aplicación con la que se generó el archivo original firmado digitalmente



Fuente: Autores del proyecto

11.2. XOLIDOSIGN

Herramienta gratuita utilizada para la firma electrónica y el sellado de tiempo para asegurar la identidad del firmante y garantizar que tus documentos no han sido modificados desde su firma o sellado.

11.2.1. Requerimientos Técnicos. Para el adecuado funcionamiento de la herramienta se requieren los siguientes requerimientos técnicos

- ✓ Sistema Operativo:
  - ➢ Windows XP Service Pack 3
  - ➢ Windows Vista - Arquitecturas de 32 y 64 bits
  - ➢ Windows 7 - Arquitecturas de 32 y 64 bits
  - ➢ Windows 8 - Arquitecturas de 32 y 64 bits
- ✓ Espacio en Disco duro
  - ➢ 80 Mb de espacio disponible en el disco duro
- ✓ Memoria RAM
  - ➢ 256 Mb de Memoria RAM
- ✓ Procesador
  - ➢ Procesador con velocidad de 800 MHZ o superior

11.2.2. Proceso de Instalación. La instalación de la herramienta se puede realizar a través de la memoria flash USB suministrada al realizar la inscripción en la plataforma CLIF, también es posible realizar la descarga desde la web de XOLIDO o desde enlace desde el sitio web de la plataforma CLIF.

Figura 98. Medios de obtención de la herramienta xolidosign

USB

- Memoria USB entregada a la hora de la inscripción .

Xolido

- http://www.xolido.com/instaladores/SetupXolidoSign.exe

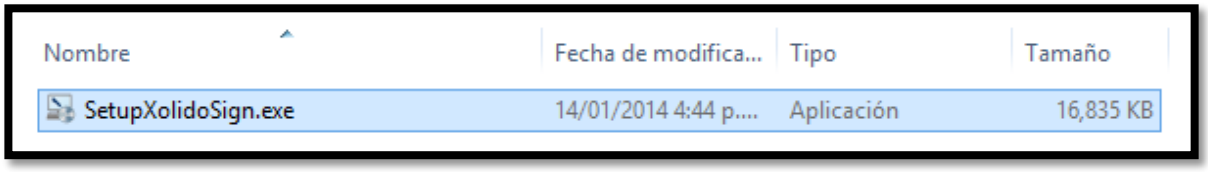
CLIF

- http://www.clif.co/descargas/firmadigital/SetupXolidoSign.exe

Fuente: Autores del proyecto

Al realizar la descarga en una ubicación fácilmente accesible como “Escritorio” se obtendrá un archivo con el instalador. (Véase la figura 99).

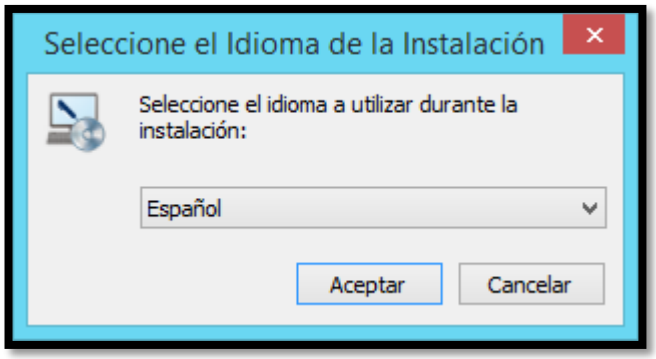
Figura 99. Archivos de instalación herramienta xolidosign



Fuente: Autores del proyecto

Procedemos con la instalación de la herramienta XolidoSign haciendo doble clic sobre el archivo “**SetupXolidoSign.exe**”, esperamos unos segundos a que se muestre el asistente que nos permitirá seleccionar el idioma del proceso de instalación (Véase la figura 100).

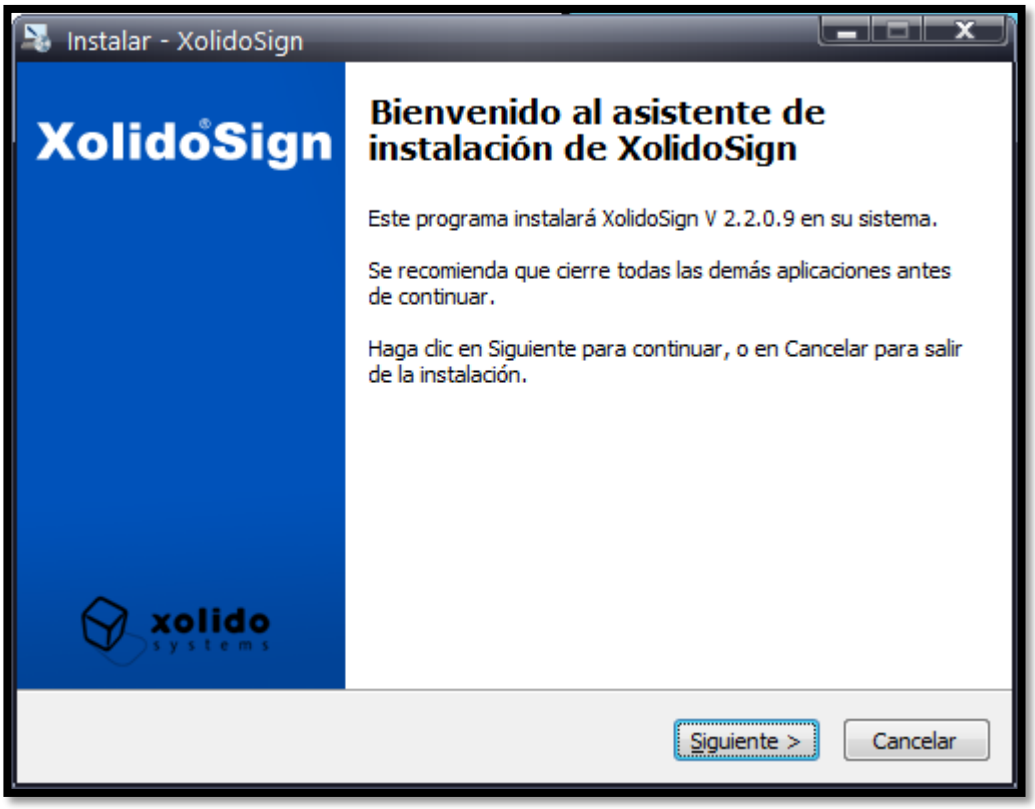
Figura 100. Asistente de instalación xolidosign, selección de idioma



Fuente: Autores del proyecto

Seleccionamos el idioma que deseamos, en este caso mantendremos el predeterminado que es "**Español**" y haremos clic en "**Aceptar**", a continuación de nos muestra el asistente que nos guiara durante el proceso de instalación (Véase la figura 101).

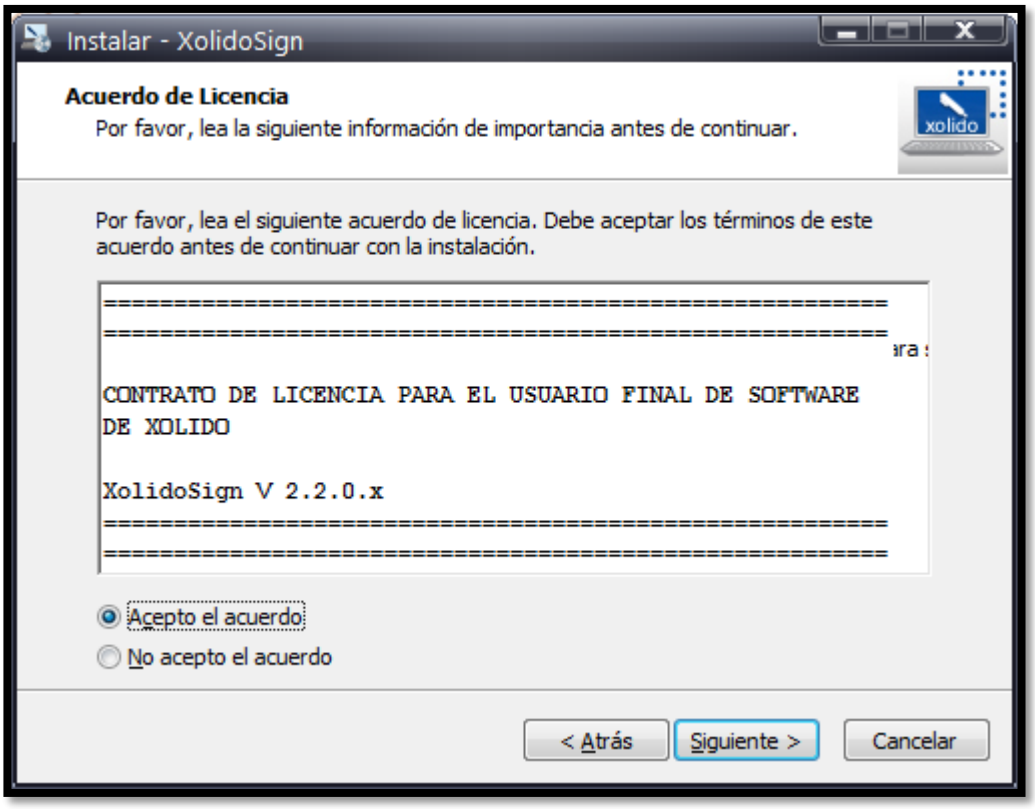
Figura 101. Asistente de instalación xolidosign



Fuente: Autores del proyecto

Para continuar hacemos clic en el botón "**Siguiente**" y se muestra el contrato de licencia de uso de la herramienta (Véase la figura 102).

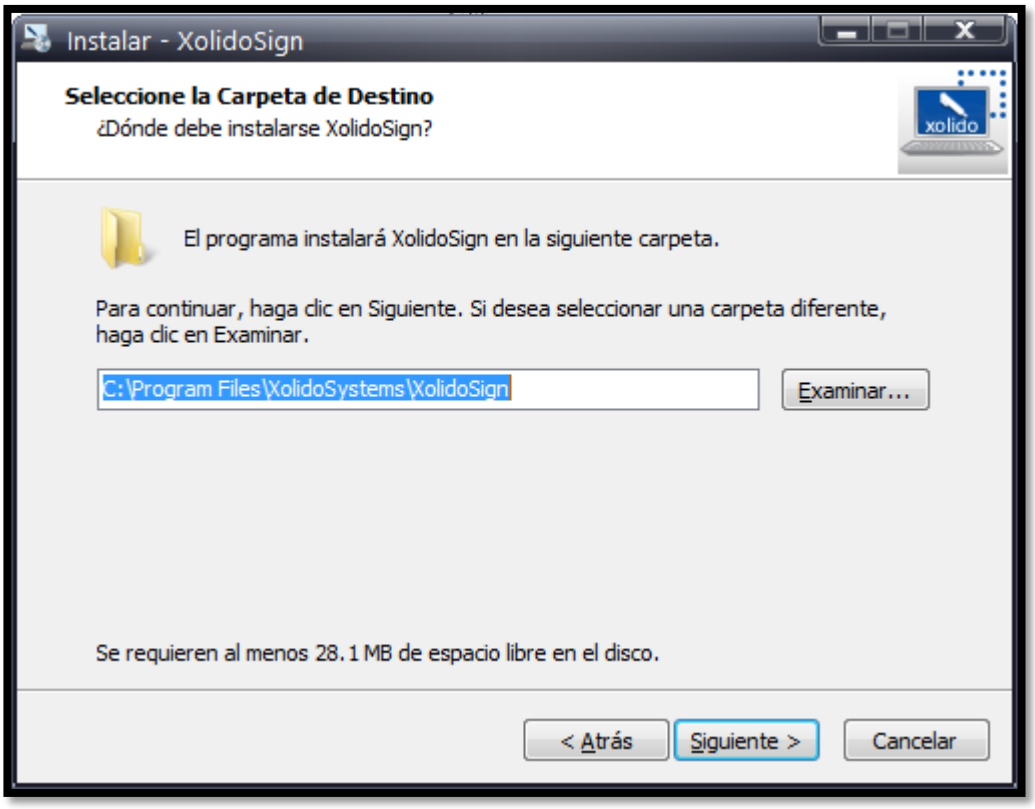
Figura 102. Asistente de instalación xolidosign, contrato de licencia



Fuente: Autores del proyecto

Procedemos a realizar la lectura del contrato de licencia de uso y si estamos de acuerdo seleccionamos la opción "**Acepto el acuerdo**" y hacemos clic en "**Siguiente**". Si no se acepta el contrato NO es posible realizar la instalación de la herramienta. El asistente de instalación nos muestra la ruta de instalación predeterminada, es posible seleccionar otra instalación si así lo desea. (Véase la figura 103).

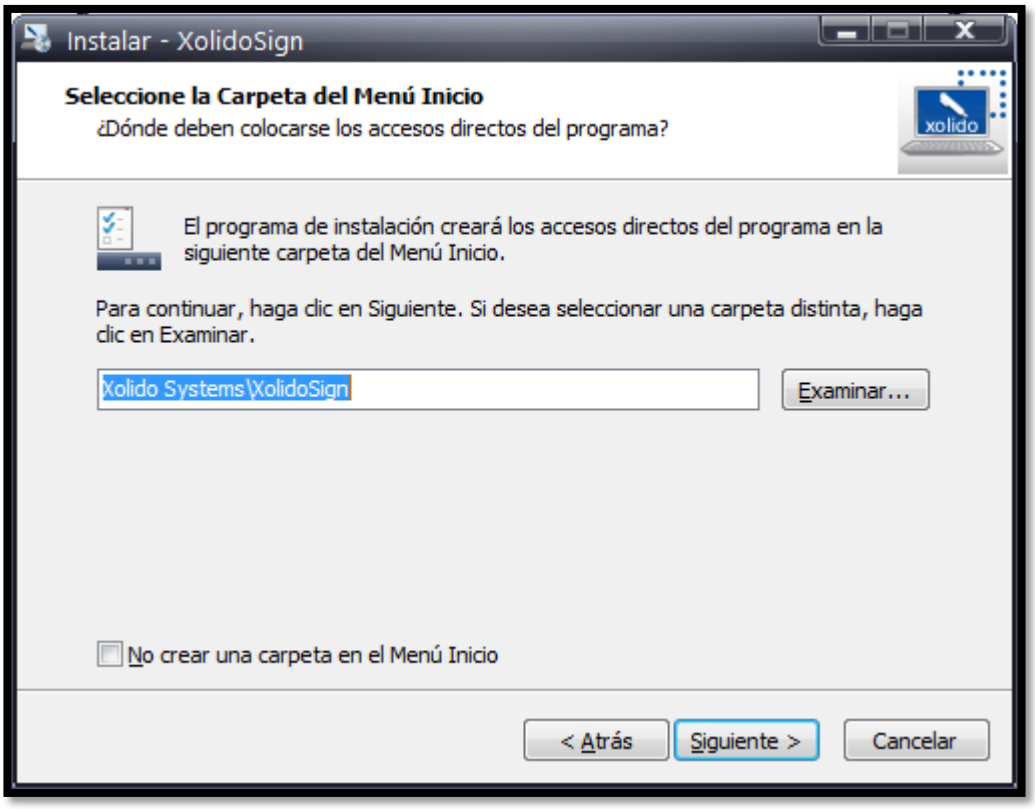
Figura 103. Asistente de instalación xolidosign, seleccionar carpeta de instalación



Fuente: Autores del proyecto

A continuación realizamos clic en "**Siguiente**", el asistente nos indica que el instalador creara accesos directos del programa en el menú inicio. (Véase la figura 104).

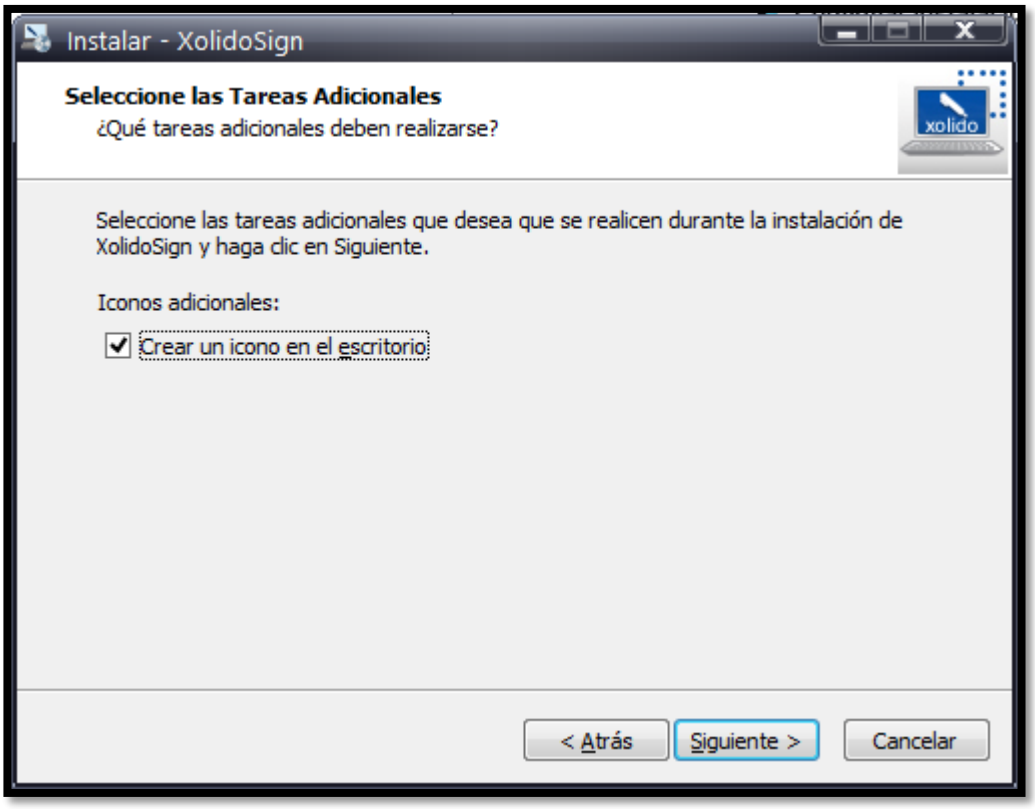
Figura 104. Asistente de instalación xolidosign, seleccionar carpeta del menú inicio



Fuente: Autores del proyecto

Procedemos haciendo clic en "**Siguiente**" y el asistente nos indica que se crearan accesos directos para acceder a la aplicación. (Véase la figura 105)

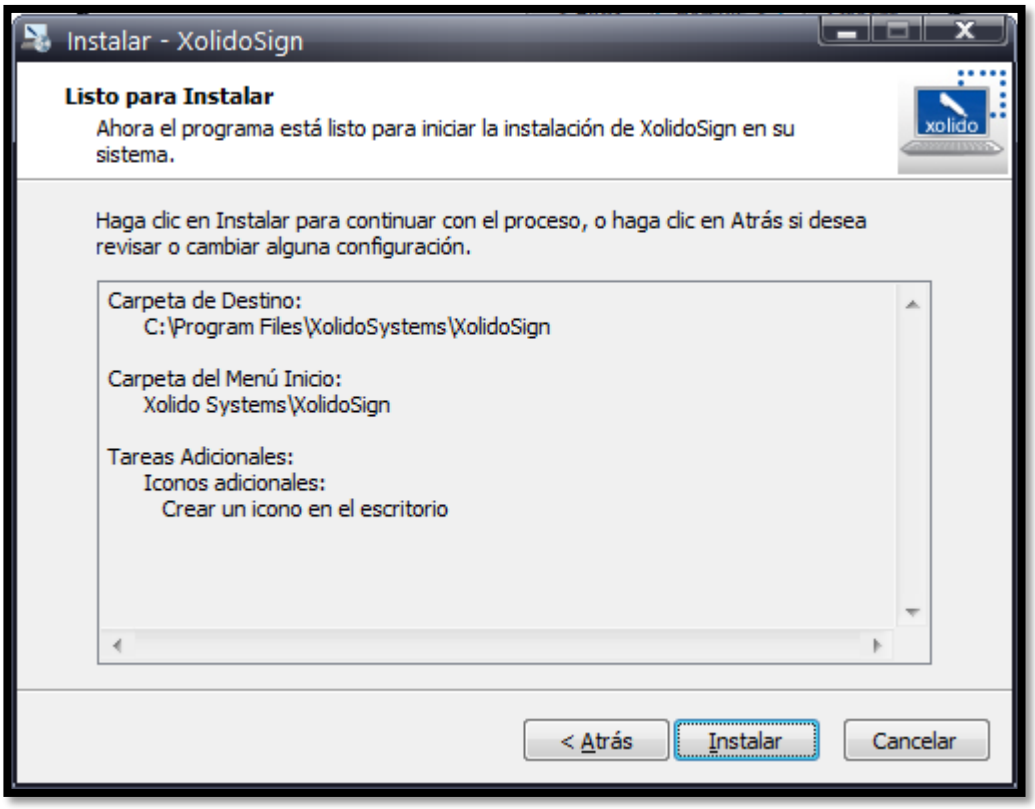
Figura 105. Asistente de instalación xolidosign, seleccionar tareas adicionales



Fuente: Autores del proyecto

A continuación realizamos clic en "**Siguiente**", el asistente nos indica que el instalador está listo. (Véase la figura 106).

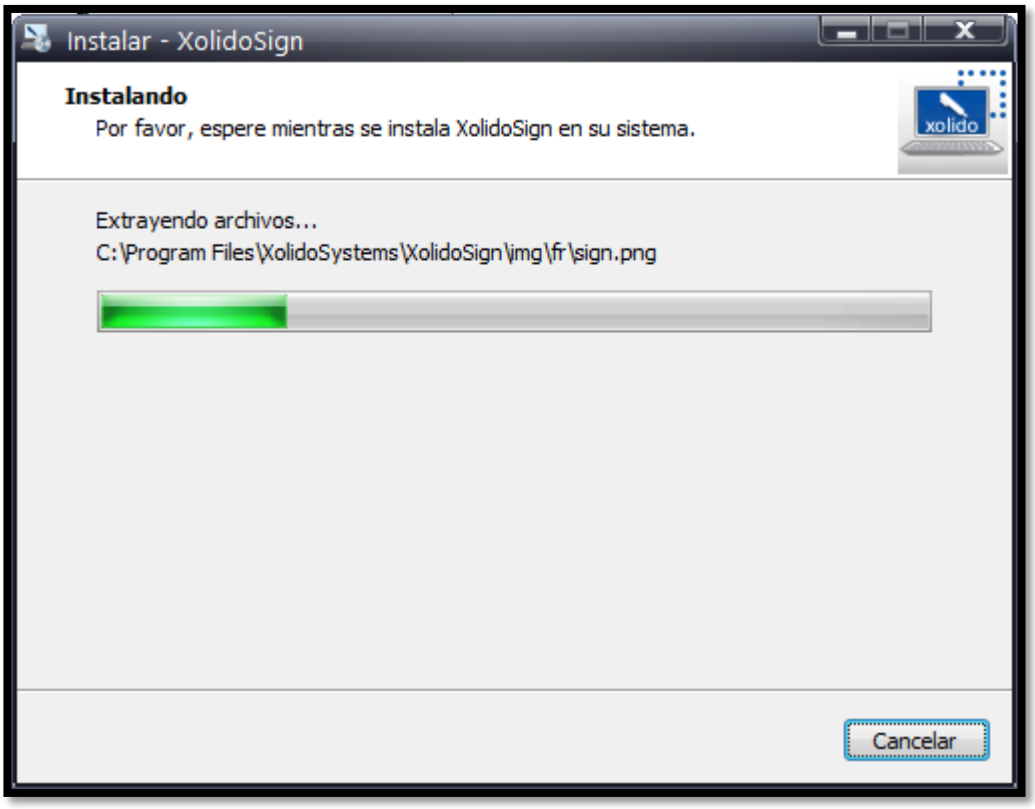
Figura 106. Asistente de instalación xolidosign, resumen de configuraciones de instalación



Fuente: Autores del proyecto

Para iniciar la instalación procedemos en hacer clic en "**Instalar**". (Véase la figura 107).

Figura 107. Asistente de instalación xolidosign, proceso de instalación



Fuente: Autores del proyecto

Si durante la instalación nos solicita autorización para realizar operaciones relacionadas con XolidoSign, hacemos clic en "**SI**", para que la instalación se desarrolle sin inconvenientes. Una vez finalice la instalación, el asistente nos informa que se realizó correctamente. (Véase la figura 108).

Figura 108. Asistente de instalación xolidosign, instalación completada

Fuente: Autores del proyecto

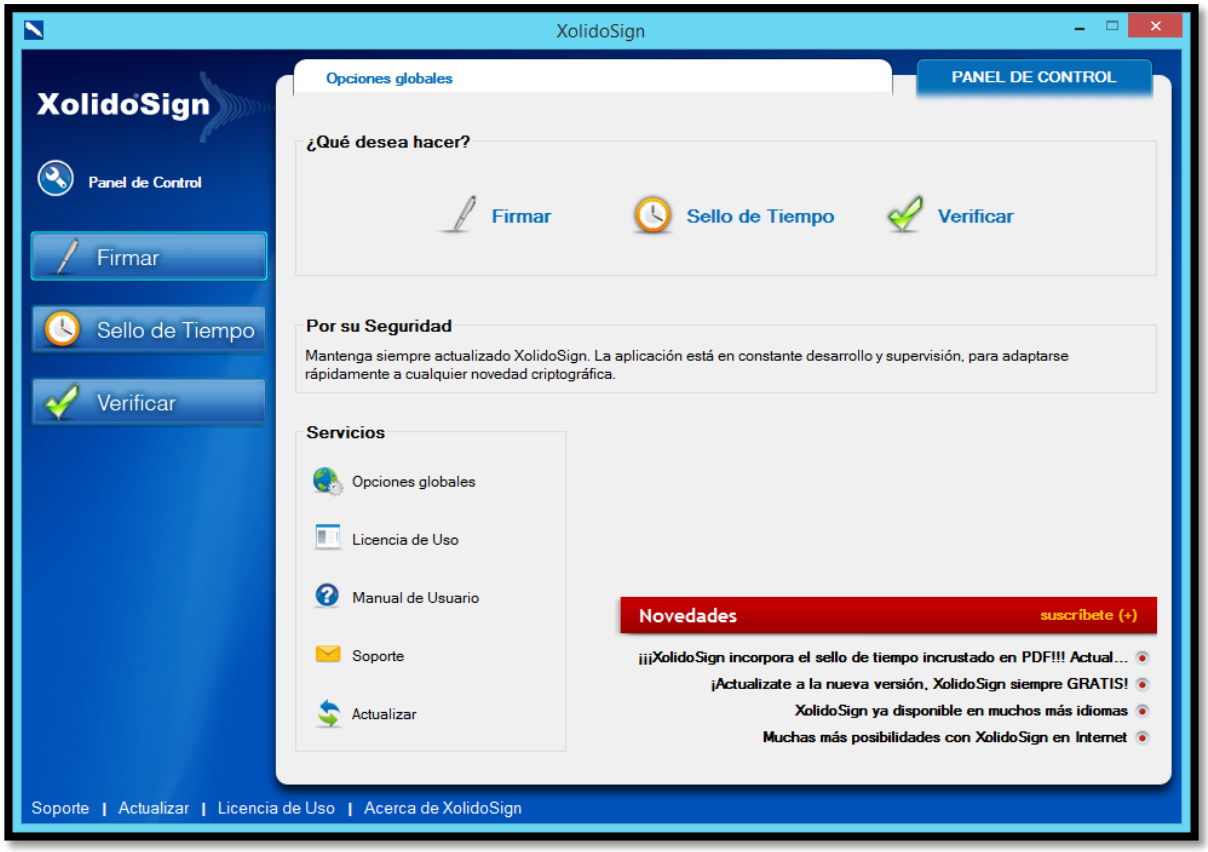
Finalmente hacemos clic en el botón "**Finalizar**" y debemos encontrar en el "**Escritorio**" del equipo un acceso directo a la herramienta instalada. (Véase la figura 108).

Figura 109. Acceso directo instalado por la herramienta xolidosign

Fuente: Autores del proyecto

Ejecutando "**XolidoSign**" podemos visualizar su interfaz para realizar firmado Digital. (Véase la figura 110).

Figura 110. Interfaz de la herramienta xolidosign



Fuente: Autores del proyecto

11.2.3. Firma Digital Mediante XolidoSign. Para realizar la firma digital de los diferentes documentos electrónicos se deben haber completado previamente los procedimientos para "**Obtención de certificados de firma digital**", "**Generación de certificados de firma digital**", "**Instalación de certificado de firma digital**" e "**Instalación de certificado raíz**", adicionalmente se debe tener instalada la herramienta "**XolidoSign**" y debe estar instalado en el equipo de cómputo el certificado de firma digital.

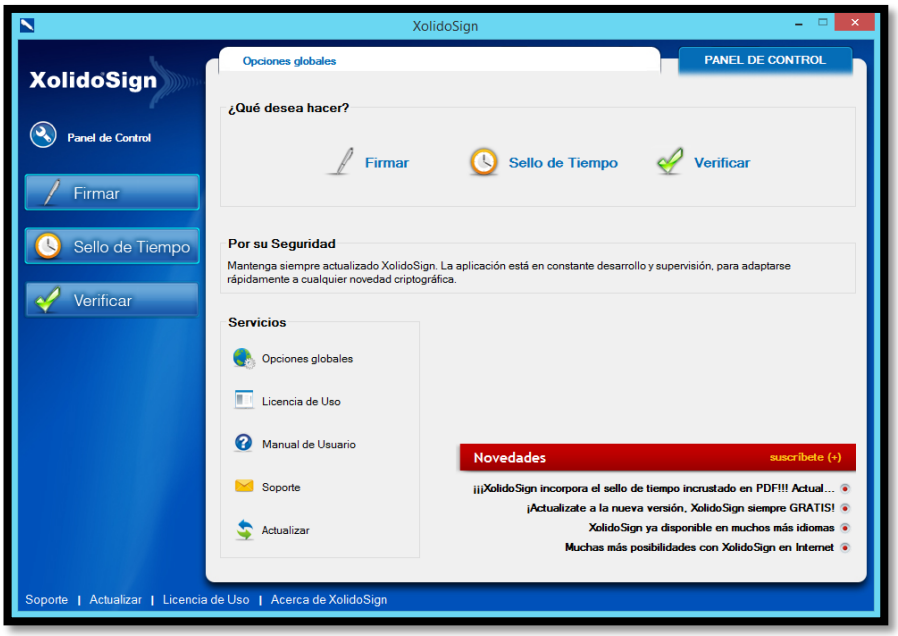
Para iniciar el proceso de firma digital buscamos en el escritorio el acceso directo a la aplicación "**XolidoSign**" y hacemos doble clic. (Véase la figura 111).

Figura 111. Acceso directo instalado por la herramienta xolidosign

Fuente: Autores del proyecto

Se abrirá la interfaz de la aplicación, esta está compuesta por tres opciones principales, la primera "**Firmar**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información, la segunda "**Sello de tiempo**" que nos permitirá dejar constancia de la existencia de un documento en un instante de tiempo determinado (No es necesario un certificado de firma digital, solo seleccionar los archivos e iniciar la operación) y la tercera "**Verificar**" que nos permitirá constatar la firma y sello de tiempo o estampa cronológica realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 112).

Figura 112. Interfaz de la herramienta xolidosign



Fuente: Autores del proyecto

Procedemos a hacer clic en la opción "**Firmar**". (Véase la figura 113).

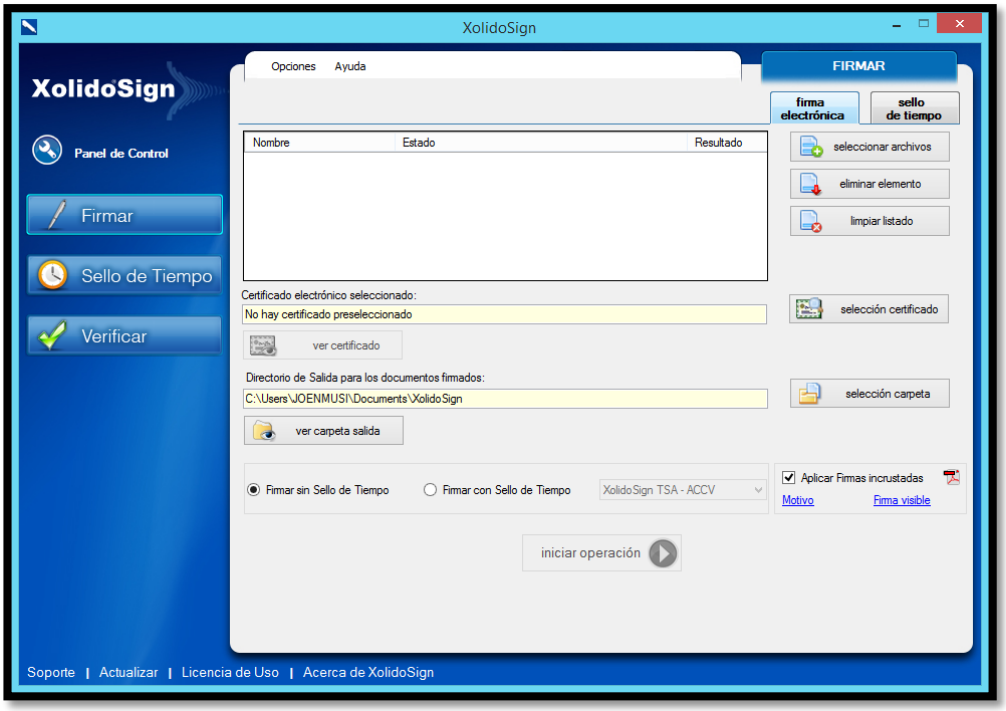
Figura 113. Botón firmar documento de la interfaz de xolidosign

Fuente: Autores del proyecto

La herramienta "**XolidoSign**" muestra su interfaz para realizar la firma digital, compuesta por un botón "**Seleccionar archivos**" que permitirá seleccionar el o los documentos electrónicos que deseamos firmar digitalmente, el botón "**eliminar elemento**" que permitirá eliminar un documento electrónico

seleccionado anteriormente y "**limpiar listado**" que eliminara todos los documentos seleccionados anteriormente para realizar firma digital. (Véase la figura 114).

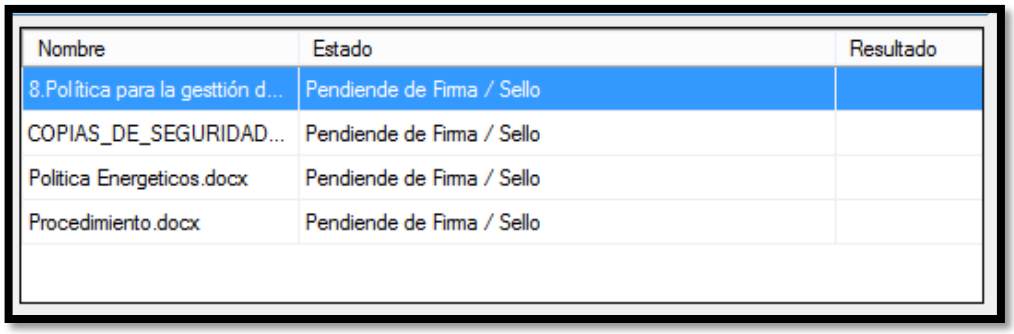
Figura 114. Interfaz de xolidosign para firmar digitalmente



Fuente: Autores del proyecto

Los documentos agregados se mostraran en una grilla o cuadricula compuesta por el nombre de cada uno de los documentos a firmar, el estado del documento "**Pendiente de firma / sello**" y el resultado de la operación. (Véase la figura 115).

Figura 115. Listado del conjunto de archivos que se desea firmar digitalmente mediante xolidosign

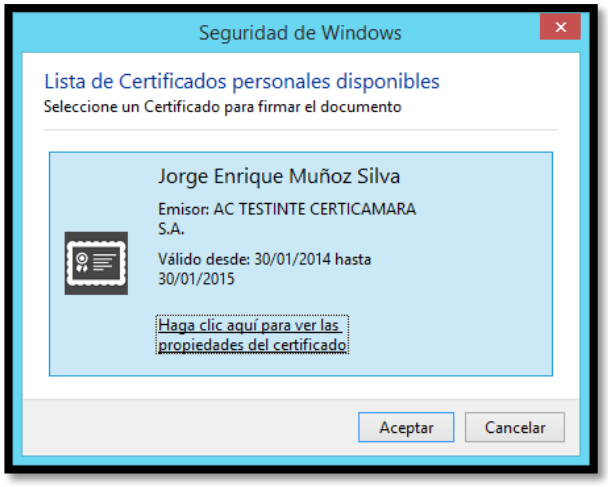


Fuente: Autores del proyecto

En la parte central de la herramienta "**XolidoSign**" encontramos la opción para seleccionar nuestro certificado de firma digital, para nuestro caso seleccionamos la opción "**Selección certificado**" y se abrirá un cuadro de dialogo para seleccionar el certificado de firma digital y seguidamente haremos clic en el botón "**Aceptar**". (Véase la figura 116).

Figura 116. Cuadro de dialogo seleccionar certificado digital instalado en el equipo

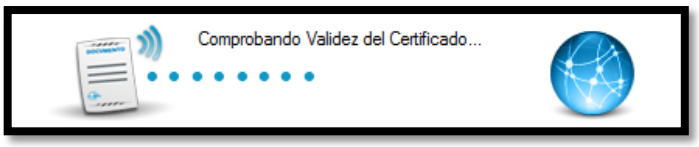
Fuente: Autores del proyecto



Fuente: Autores del proyecto

La herramienta "**XolidoSign**" comprobara la validez del certificado. (Véase la figura 117).

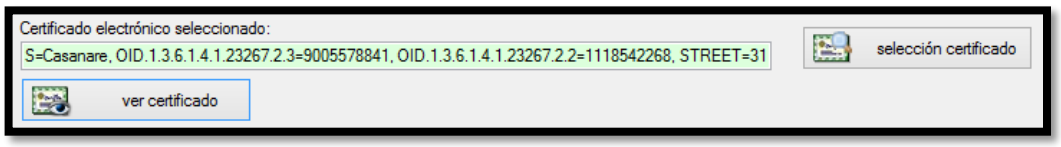
Figura 117. Proceso de comprobación de la validez del certificado de firma digital



Fuente: Autores del proyecto

Posteriormente se mostrara la información del certificado de firma digital seleccionado. (Véase la figura 118).

Figura 118. Información del certificado de firma digital seleccionado en xolidosign



Fuente: Autores del proyecto

Seguidamente la herramienta permite seleccionar la ruta de salida de los documentos firmados digitalmente, se puede dejar la carpeta por defecto o definir la que desee al hacer clic en el botón "**selección carpeta**". (Véase la figura 119).

Figura 119. Seleccionar carpeta para los documentos firmados por xolidosign

Fuente: Autores del proyecto

La herramienta permite seleccionar si adicionara ("**Firmar con Sello de Tiempo**") o no ("**Firmar sin Sello de Tiempo**") sello de tiempo o estampa cronológica a los archivos que firmará digitalmente, esta característica garantiza la existencia del documento electrónico en un instante de tiempo al agregar un sello con la fecha y hora en la que se realiza el procedimiento tomado de un servidor externo destinado para tal fin (Véase la figura 120), puede seleccionar entre dos opciones para asignar sello de tiempo que son:

- ✓ XolidoSign TSA – ACCV
- ✓ XolidoSign TSA - IZENPE

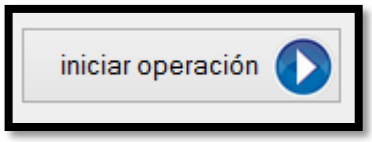
Seleccione el que desee, esto no interfiere en el proceso de sello de tiempo.

Figura 120. Selección de servidor de sello de tiempo en xolidosign

Fuente: Autores del proyecto

Finalmente hacemos clic en el botón "**Iniciar operación**" para iniciar la firma de los documentos electrónicos seleccionados. (Véase la figura 121).

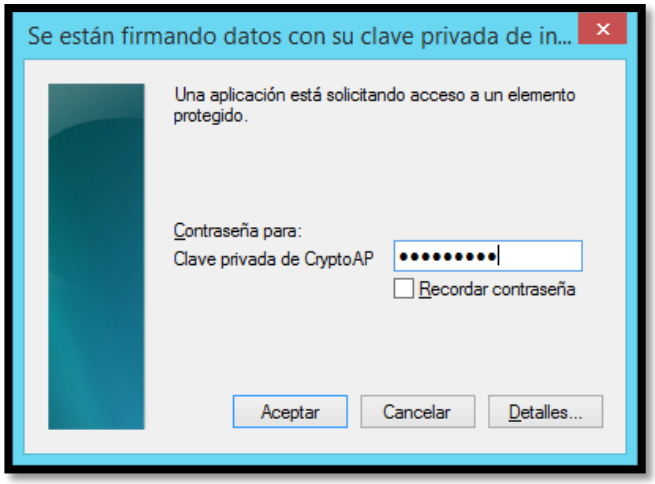
Figura 121. Botón iniciar operación de firma digital en xolidosign



Fuente: Autores del proyecto

La aplicación "**XolidoSign**" desplegará un cuadro de dialogo en el cual debemos ingresar la contraseña de **USO** del certificado de firma digital asignada en el procedimiento "**Instalación de certificado de firma digital**" y hacemos clic en el botón "**Aceptar**". (Véase la figura 122).

Figura 122. Solicitud de contraseña de uso del certificado de firma digital en xolidosign



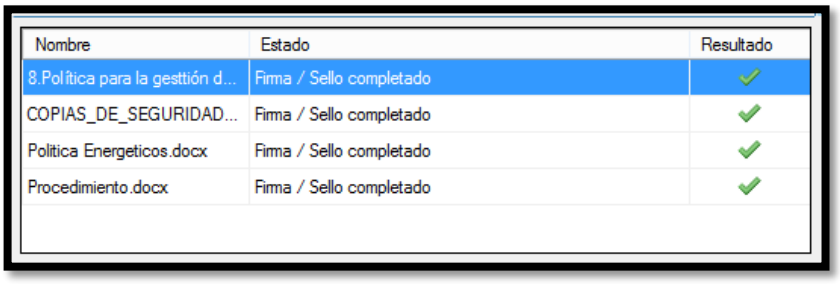
Fuente: Autores del proyecto

Advertencia: La contraseña de **USO** asignada en el procedimiento "**Instalación de certificado de firma digital**" puede ser distinta a la contraseña de **PROTECCIÓN** del certificado de firma digital asignada en el procedimiento "**Obtención de certificados de firma digital**". Por seguridad es recomendable que **NO** se active la casilla "**Recordar contraseña**" para evitar que el certificado de

firma digital pueda ser utilizado sin su consentimiento, teniendo en cuenta que este cuenta con total validez jurídica.

La herramienta actualiza la grilla o cuadricula compuesta por el nombre de cada uno de los documentos a firmar, el estado del documento "**Firma / Sello completado**" y el resultado de la operación (Visto bueno en color verde (√) o una X roja). (Véase la figura 123).

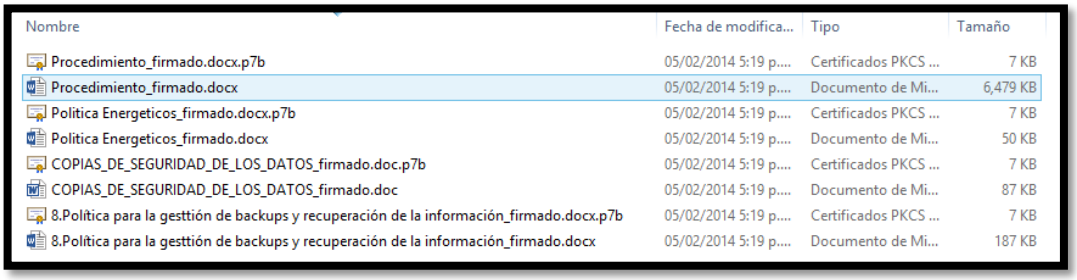
Figura 123. Listado del conjunto de archivos firmados digitalmente mediante xolidosign



Fuente: Autores del proyecto

Podemos observar en la ubicación seleccionada los documentos electrónicos firmados digitalmente (extensión original) y su respectivo certificado de validación con extensión "**p7b**" que indica que el documento está firmado por "**XolidoSign**". (Véase la figura 124).

Figura 124. Archivos generados del proceso de firma digital mediante xolidosign



Fuente: Autores del proyecto

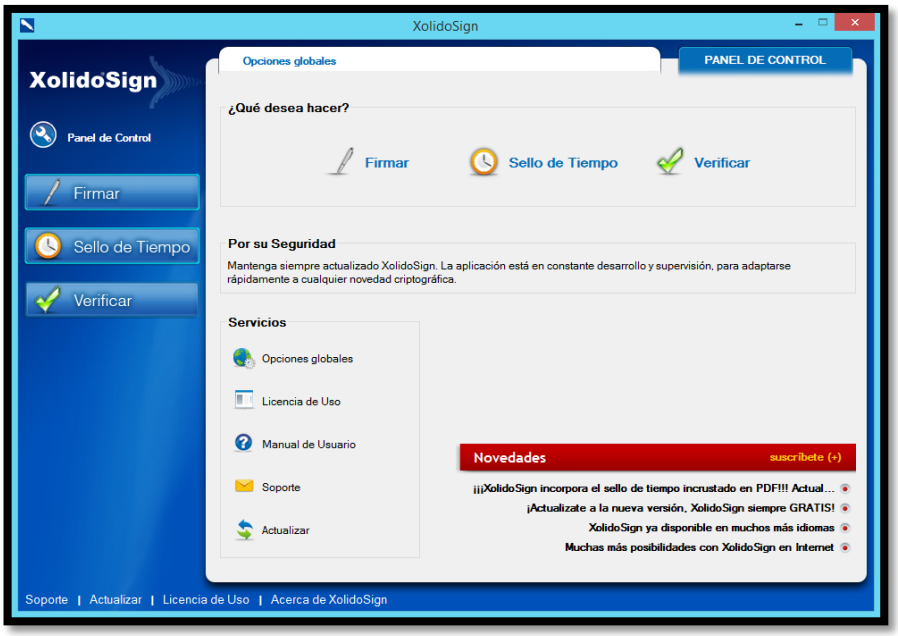
11.2.4. Verificar firma digital mediante XolidoSign. Para iniciar el proceso de verificación de validez de la firma digital buscamos en el escritorio el acceso directo a la aplicación "**XolidoSign**" y hacemos doble clic. (Véase la figura 125).

Figura 125. Acceso directo instalado por la herramienta xolidosign

Fuente: Autores del proyecto

Se abrirá la interfaz de la aplicación, esta está compuesta por tres opciones principales, la primera "**Firmar**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información, la segunda "**Sello de tiempo**" que nos permitirá dejar constancia de la existencia de un documento en un instante de tiempo determinado (No es necesario un certificado de firma digital, solo seleccionar los archivos e iniciar la operación) y la tercera "**Verificar**" que nos permitirá constatar la firma y sello de tiempo o estampa cronológica realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 126).

Figura 126. Interfaz de la herramienta xolidosign



Fuente: Autores del proyecto

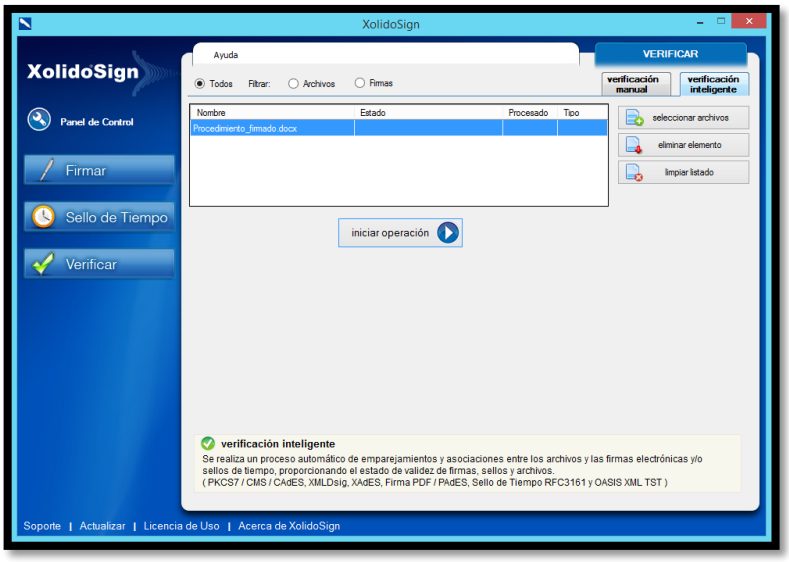
Procedemos a hacer clic en la opción "**Verificar**". (Véase la figura 127)

Figura 127. Botón verificar documento interfaz de xolidosign

Fuente: Autores del proyecto

La herramienta "**XolidoSign**" muestra su interfaz para realizar la verificación de la firma digital, compuesta por un botón "**Seleccionar archivos**" que permitirá seleccionar el documento electrónico al que deseamos verificar la validez de la firma digital. (Véase la figura 128).

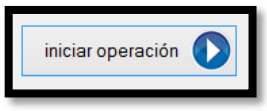
Figura 128. Interfaz de xolidosign para verificar firma digital



Fuente: Autores del proyecto

Para iniciar el proceso de verificación de la firma digital hacemos clic en el botón "**Iniciar operación**". (Véase la figura 129).

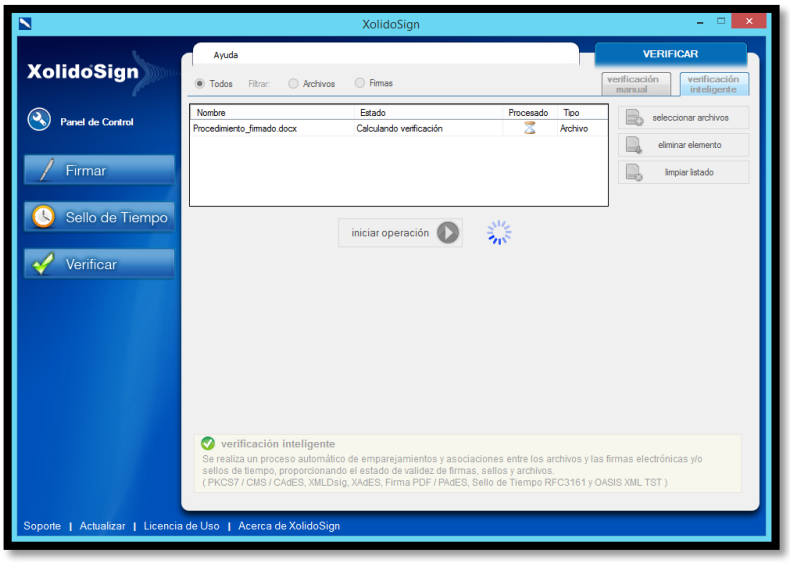
Figura 129. Botón iniciar operación de verificación de firma digital en xolidosign



Fuente: Autores del proyecto

La herramienta "**XolidoSign**" inicia el proceso de comprobación, esta operación tarda unos segundos dependiendo del tamaño y cantidad de archivos. (Véase la figura 130).

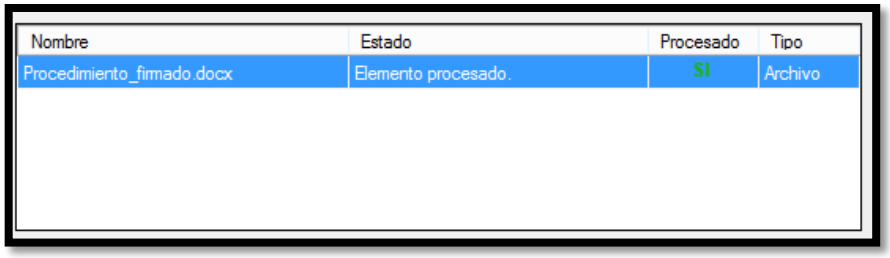
Figura 130. Proceso de comprobación de firma digital de xolidosign



Fuente: Autores del proyecto

Una vez comprobada la validez de la firma digital la herramienta muestra la grilla o cuadricula compuesta por el nombre del documento electrónico, el estado, indicador de procesado y el tipo. (Véase la figura 131).

Figura 131. Listado del conjunto de archivos verificados mediante xolidosign



Fuente: Autores del proyecto

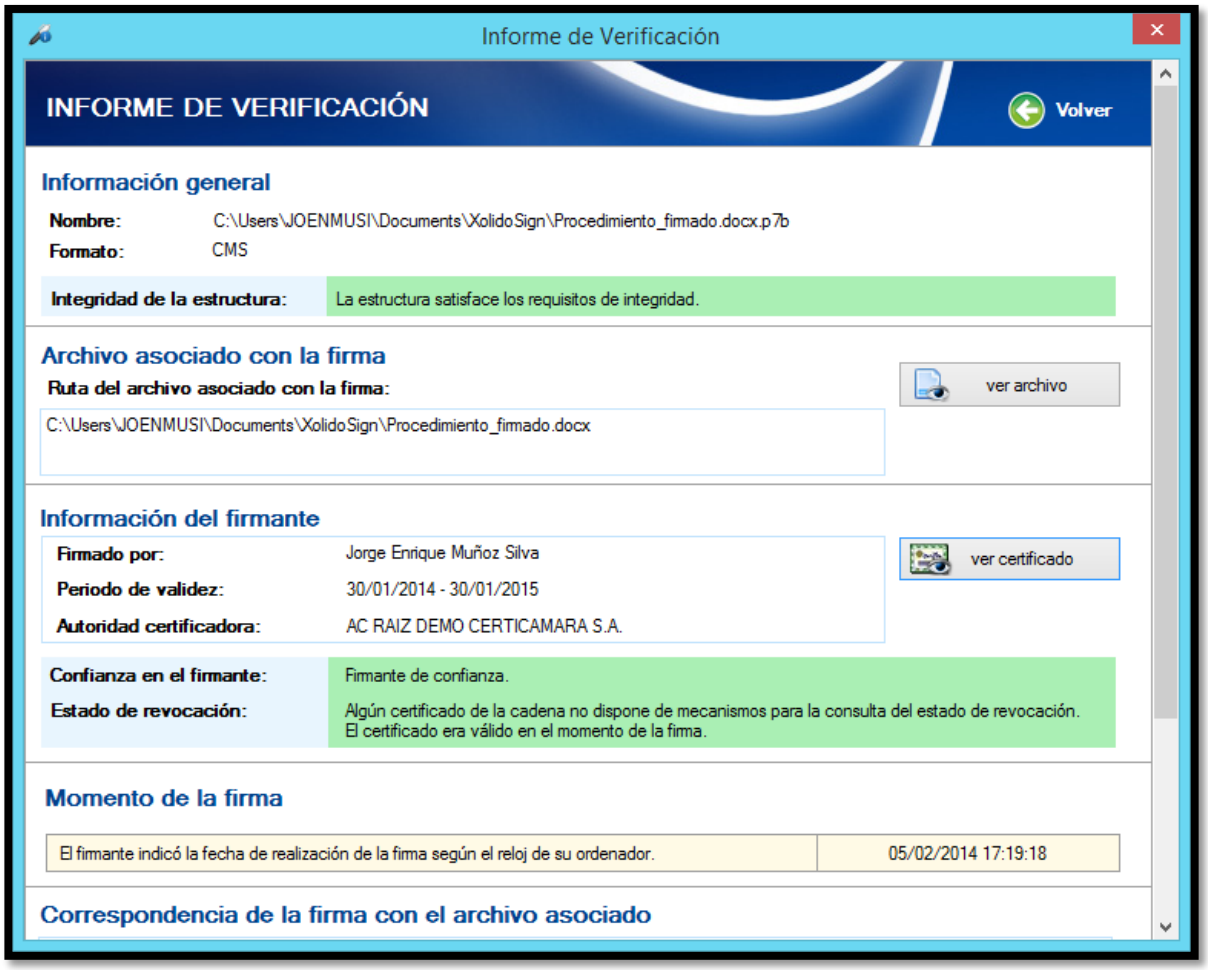
Adicionalmente "**XolidoSign**" muestra información relevante como el nombre del documento firmado, el directorio o ruta donde se encuentra almacenado, el nombre de quien lo firmo digitalmente, la autoridad de certificación, confianza del firmante, información de revocación del firmante, integridad del documento y correspondencia entre la firma y el documento, fecha y hora del ordenador a la hora de realizó la firma. (Véase la figura 132).

Figura 132. Información relevante del documento firmado mediante xolidosign

Fuente: Autores del proyecto

Para obtener mayor información podemos hacer clic en el botón de la parte inferior derecha "**ver informe**". (Véase la figura 133).

Figura 133. Informe de verificación de firma digital de xolidosign

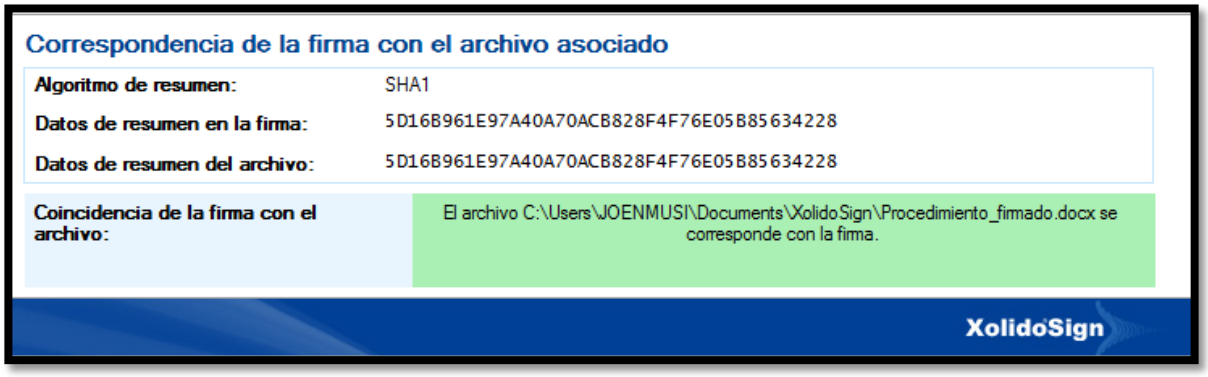


Fuente: Autores del proyecto

El informe de verificación muestra la ruta donde se encuentra almacenado el archivo de firma en formato "**p7b**", adicionalmente la ruta donde se encuentra almacenado el documento asociado a la firma "**docx**", seguidamente información del firmante, periodo de validez del certificado, autoridad certificadora, también suministra fecha y hora del ordenador a la hora de realizar la firma.

La correspondencia de la firma con el archivo asociado muestra el algotirmo de resumen o hash utilizado por la herramienta "**XolidoSign**", los datos de resumen contenida en la firma y datos de resumen del archivo firmado, al ser iguales estos valores se garantiza totalmente la integridad del documento electronico. (Véase la figura 134).

Figura 134. Correspondencia de la firma digital con el archivo asociado



Fuente: Autores del proyecto

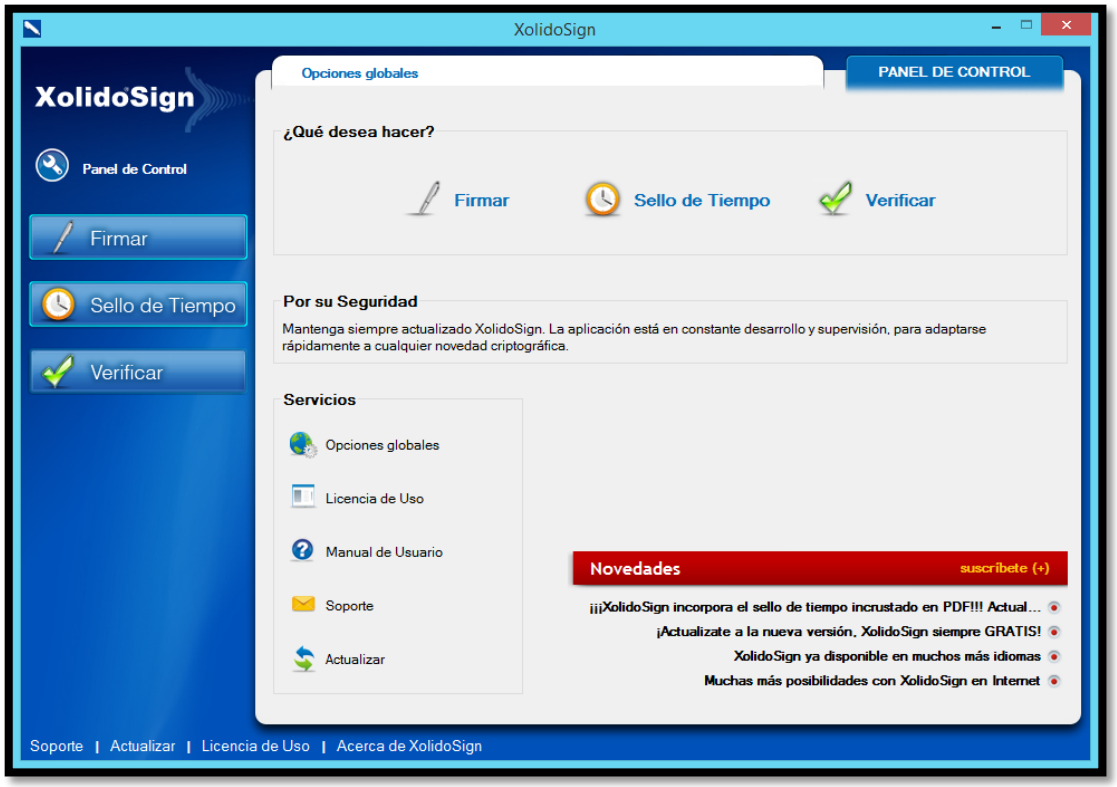
11.2.5. Sello de tiempo mediante XolidoSign. Para iniciar el proceso de sello de tiempo buscamos en el escritorio el acceso directo a la aplicación "**XolidoSign**" y hacemos doble clic. (Véase la figura 135).

Figura 135. Acceso directo instalado por la herramienta xolidosign

Fuente: Autores del proyecto

Se abrirá la interfaz de la aplicación, esta está compuesta por tres opciones principales, la primera "**Firmar**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información, la segunda "**Sello de tiempo**" que nos permitirá dejar constancia de la existencia de un documento en un instante de tiempo determinado (No es necesario un certificado de firma digital, solo seleccionar los archivos e iniciar la operación) y la tercera "**Verificar**" que nos permitirá constatar la firma y sello de tiempo o estampa cronológica realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 136).

Figura 136. Interfaz de la herramienta xolidosign



Fuente: Autores del proyecto

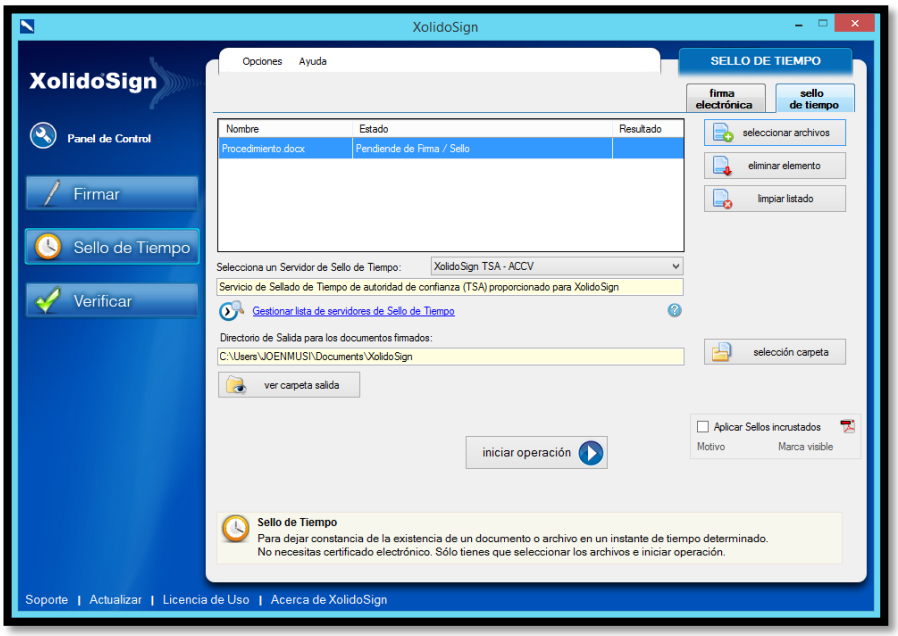
Procedemos a hacer clic en la opción "**Sello de tiempo**". (Véase la figura 137).

Figura 137. Botón sello de tiempo de documentos de la interfaz de xolidosign

Fuente: Autores del proyecto

La herramienta "**XolidoSign**" muestra su interfaz para realizar la firma digital, compuesta por un botón "**Seleccionar archivos**" que permitirá seleccionar el o los documentos electrónicos a los que deseamos aplicar el sello de tiempo, el botón "**eliminar elemento**" que permitirá eliminar un documento electrónico seleccionado anteriormente y "**limpiar listado**" que eliminará todos los documentos seleccionados anteriormente para aplicar el sello de tiempo. (Véase la figura 138).

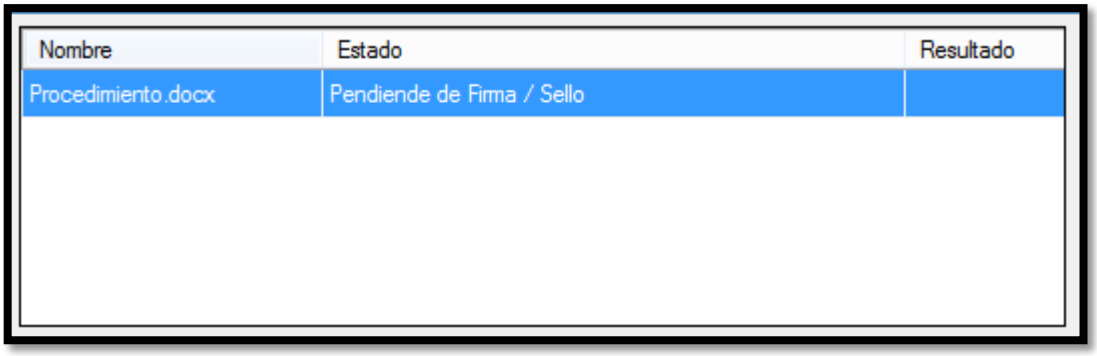
Figura 138. Interfaz de xolidosign para sello de tiempo



Fuente: Autores del proyecto

Los documentos agregados se mostraran en una grilla o cuadricula compuesta por el nombre de cada uno de los documentos a los cuales se les aplicará sello de tiempo, el estado del documento "**Pendiente de firma / sello**" y el resultado de la operación. (Véase la figura 139).

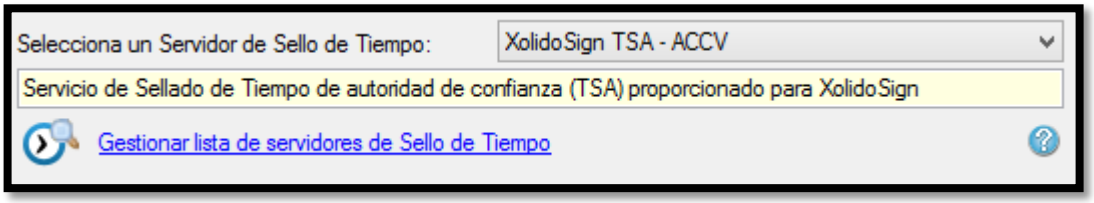
Figura 139. Listado del conjunto de archivos que se desea aplicar sello de tiempo mediante xolidosign



Fuente: Autores del proyecto

Posteriormente se mostrara la información del servidor de sello de tiempo seleccionado, existen disponibles dos y se pueden agregar si así se requieren. (Véase la figura 140).

Figura 140. Selección de servidor de sello de tiempo de xolidosign



Fuente: Autores del proyecto

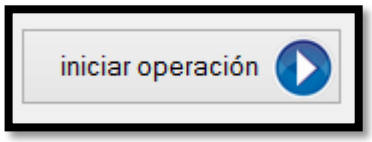
Seguidamente la herramienta permite seleccionar la ruta de salida de los documentos a los cuales se les aplicó sello de tiempo, se puede dejar la carpeta por defecto o definir la que desee al hacer clic en el botón "**selección carpeta**". (Véase la figura 141).

Figura 141. Seleccionar carpeta para los documentos firmados por xolidosign

Fuente: Autores del proyecto

Finalmente hacemos clic en el botón "**Iniciar operación**" para iniciar la firma de los documentos electrónicos seleccionados. (Véase la figura 142).

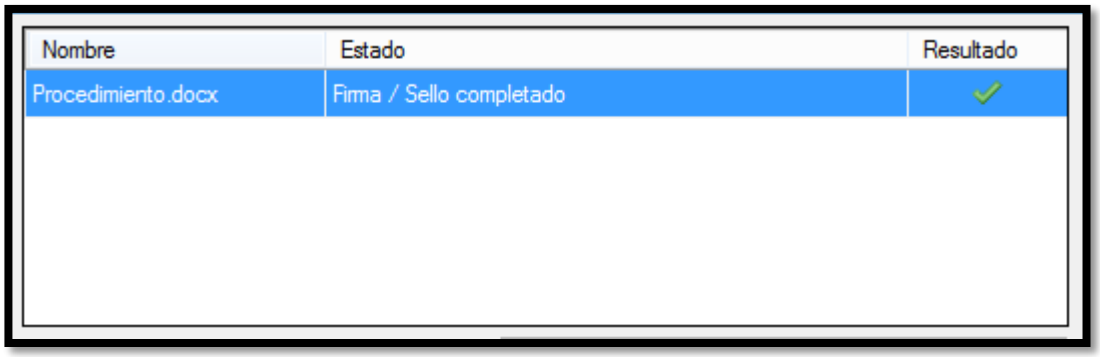
Figura 142. Botón iniciar operación de sello de tiempo en xolidosign



Fuente: Autores del proyecto

La herramienta actualiza la grilla o cuadricula compuesta por el nombre de cada uno de los documentos a firmar, el estado del documento "**Firma / Sello completado**" y el resultado de la operación (Visto bueno en color verde (√) o una X roja). (Véase la figura 143).

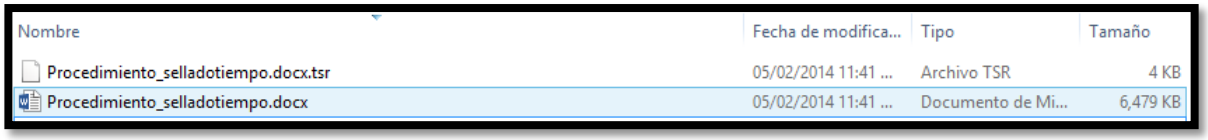
Figura 143. Listado del conjunto de archivos a los que se les aplico sello de tiempo mediante xolidosign



Fuente: Autores del proyecto

Podemos observar en la ubicación seleccionada los documentos electrónicos a los que se les aplico el sello de tiempo (extensión original) y su respectivo certificado de validación del sello de tiempo con extensión "**tsr**" que indica que el documento está con sello de tiempo de "**XolidoSign**". (Véase la figura 144).

Figura 144. Archivos generados del proceso de sello de tiempo mediante xolidosign



Fuente: Autores del proyecto

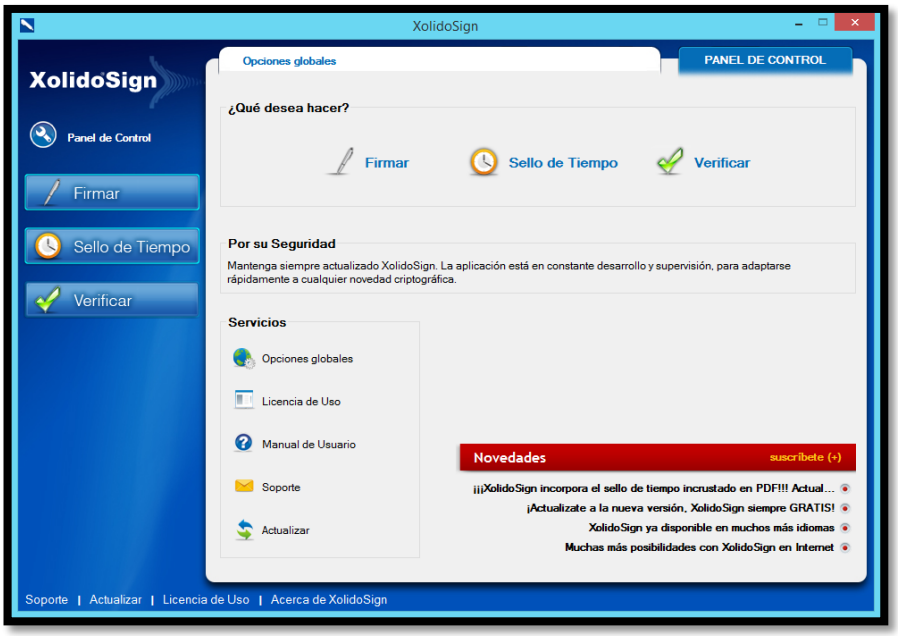
11.2.6. Verificar sello de tiempo mediante XolidoSign. Para iniciar el proceso de verificación de validez del sello de tiempo buscamos en el escritorio el acceso directo a la aplicación "**XolidoSign**" y hacemos doble clic. (Véase la figura 145).

Figura 145. Acceso directo instalado por la herramienta xolidosign

Fuente: Autores del proyecto

Se abrirá la interfaz de la aplicación, esta está compuesta por tres opciones principales, la primera "**Firmar**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información, la segunda "**Sello de tiempo**" que nos permitirá dejar constancia de la existencia de un documento en un instante de tiempo determinado (No es necesario un certificado de firma digital, solo seleccionar los archivos e iniciar la operación) y la tercera "**Verificar**" que nos permitirá constatar la firma y sello de tiempo o estampa cronológica realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 146).

Figura 146. Interfaz de la herramienta xolidosign



Fuente: Autores del proyecto

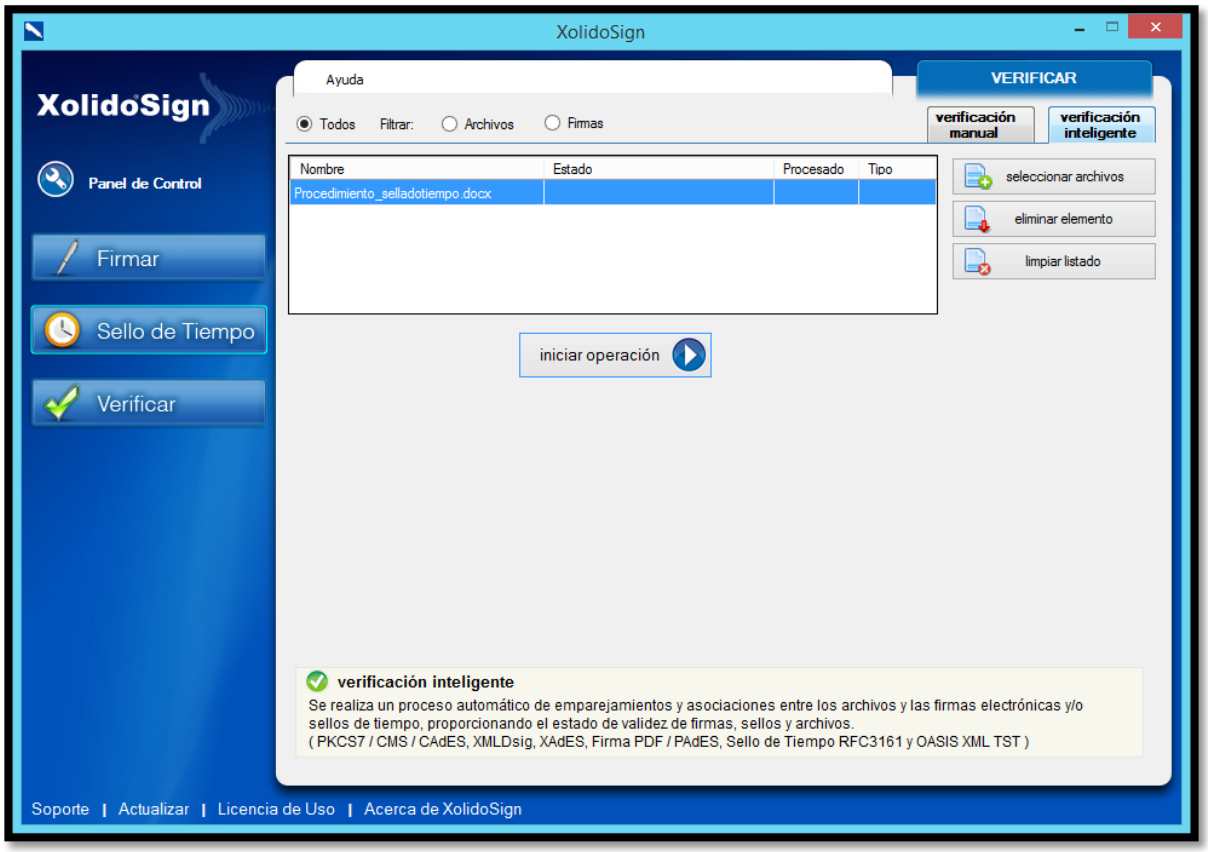
Procedemos a hacer clic en la opción "**Verificar**". (Véase la figura 147).

Figura 147. Botón verificar sello de tiempo interfaz de xolidosign

Fuente: Autores del proyecto

La herramienta "**XolidoSign**" muestra su interfaz para realizar la verificación del sello de tiempo, compuesta por un botón "**Seleccionar archivos**" que permitirá seleccionar el documento electrónico al que deseamos verificar la validez del sello de tiempo. (Véase la figura 148).

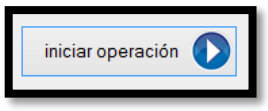
Figura 148. Interfaz de xolidosign para verificar sello de tiempo



Fuente: Autores del proyecto

Para iniciar el proceso de verificación del sello de tiempo hacemos clic en el botón "**Iniciar operación**". (Véase la figura 149).

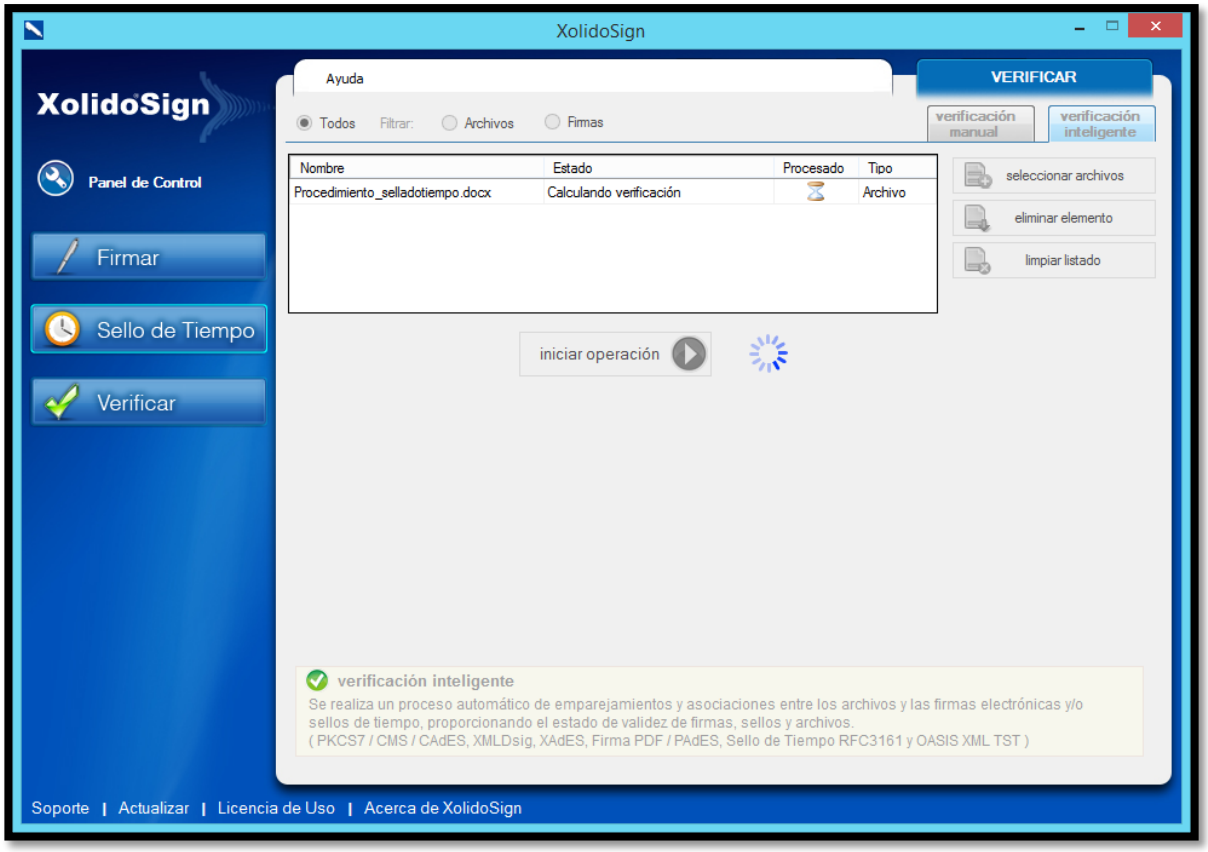
Figura 149. Botón iniciar operación de verificación de sello de tiempo en xolidosign



Fuente: Autores del proyecto

La herramienta "**XolidoSign**" inicia el proceso de comprobación, esta operación tarda unos segundos dependiendo del tamaño y cantidad de archivos. (Véase la figura 150).

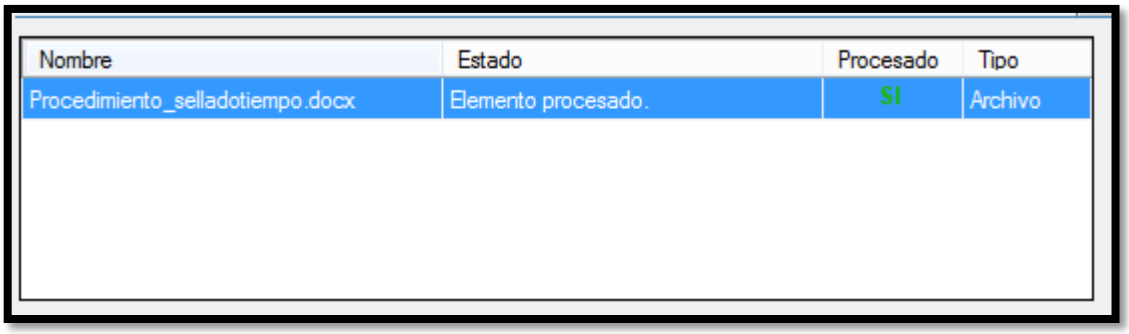
Figura 150. Proceso de comprobación de sello de tiempo de xolidosign



Fuente: Autores del proyecto

Una vez comprobada la validez del sello de tiempo la herramienta muestra la grilla o cuadricula compuesta por el nombre del documento electrónico, el estado, indicador de procesado y el tipo. (Véase la figura 151).

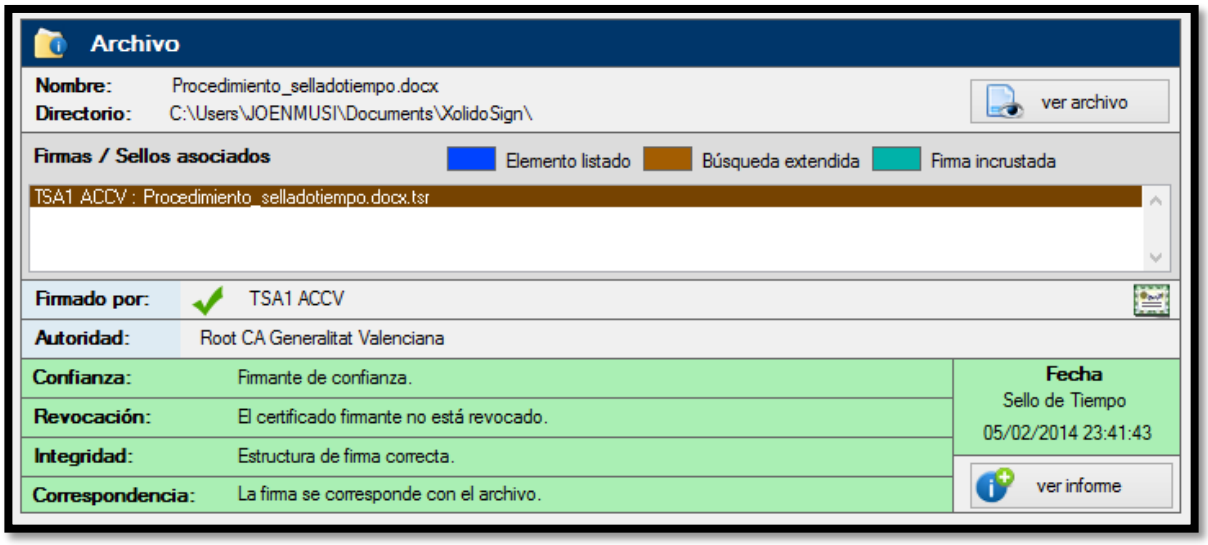
Figura 151. Listado del conjunto de archivos verificados mediante xolidosign



Fuente: Autores del proyecto

Adicionalmente "**XolidoSign**" muestra información relevante como el nombre del documento con el sello de tiempo, el directorio o ruta donde se encuentra almacenado, el nombre de quien aplico el sello de tiempo, la autoridad de certificación, confianza del firmante, información de revocación del firmante, integridad del documento y correspondencia entre la firma y el documento, fecha y hora del ordenador a la hora de realizó el sello de tiempo. (Véase la figura 152).

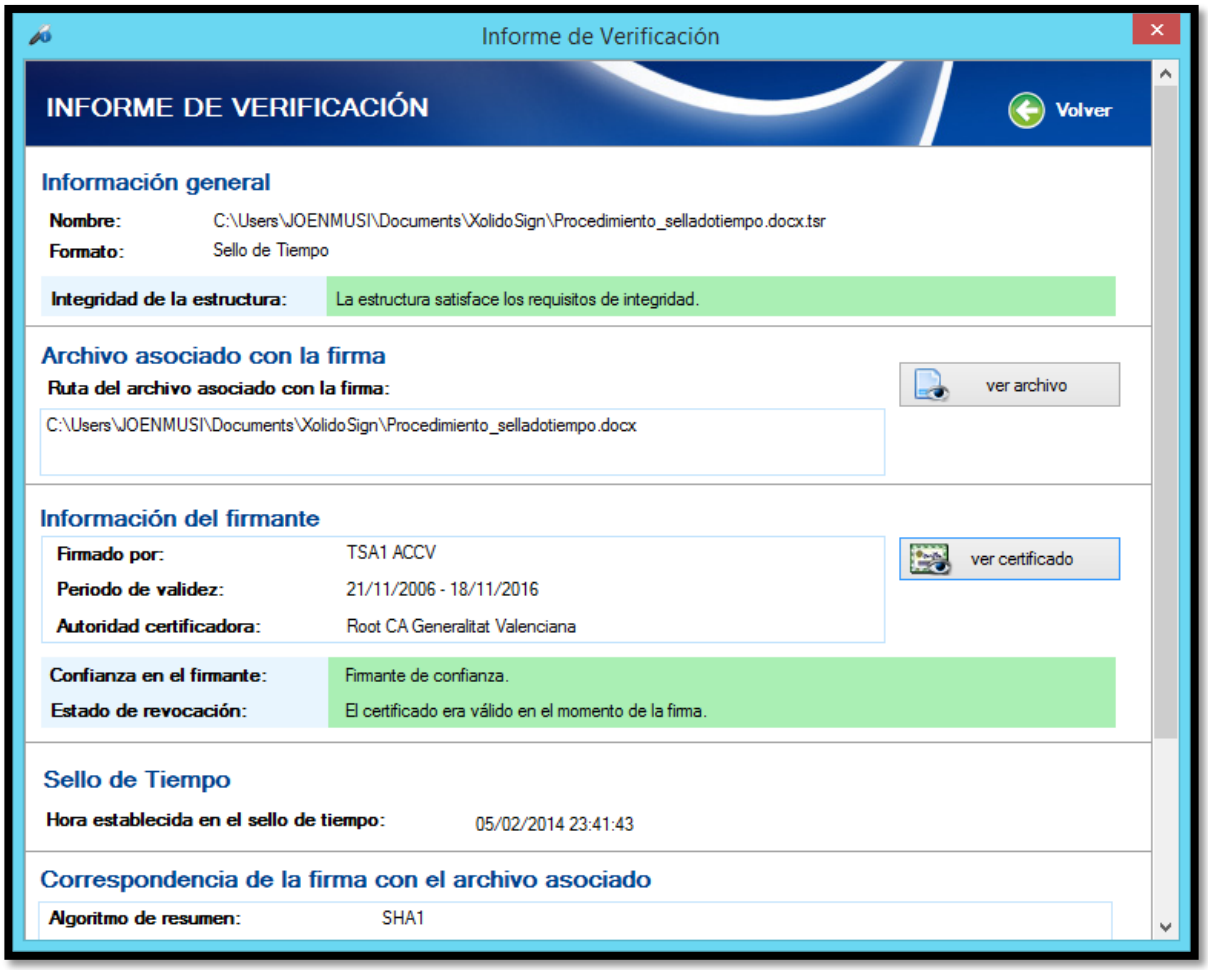
Figura 152. Información relevante del documento con sello de tiempo mediante xolidosign Fuente: Autores del proyecto



Fuente: Autores del proyecto

Para obtener mayor información podemos hacer clic en el botón de la parte inferior derecha "**ver informe**". (Véase la figura 153).

Figura 153. Informe de verificación de sello de tiempo de xolidosign



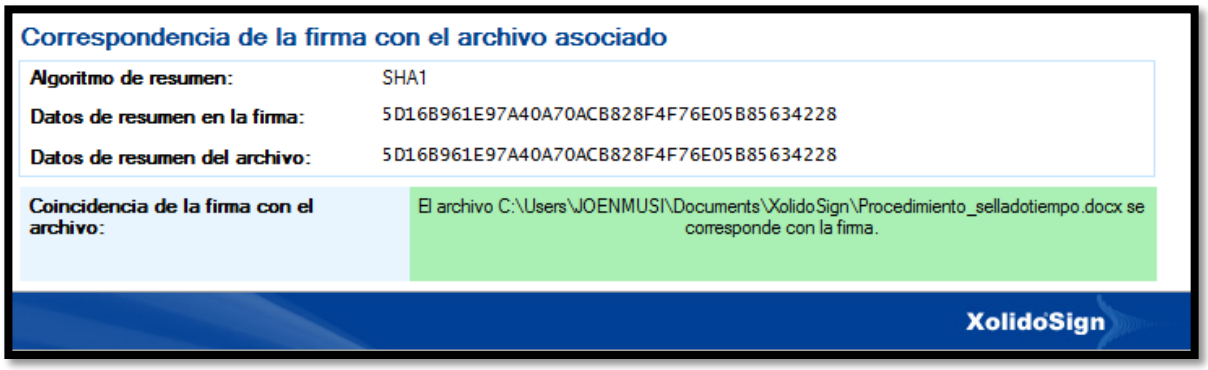
Fuente: Autores del proyecto

El informe de verificación muestra la ruta donde se encuentra almacenado el archivo de sello de tiempo en formato "**tsr**", adicionalmente la ruta donde se encuentra almacenado el documento asociado a la firma "**docx**", seguidamente información del firmante, periodo de validez del certificado, autoridad certificadora, también suministra fecha y hora del sello de tiempo.

La correspondencia de la firma con el archivo asociado muestra el algotirmo de resumen o hash utilizado por la herramienta "**XolidoSign**", los datos de resumen contenida en la firma y datos de

resumen del archivo firmado, al ser iguales estos valores se garantiza totalmente la integridad del sello de tiempo aplicado al documento electronico. (Véase la figura 154).

Figura 154. Correspondencia del sellado de tiempo con el archivo asociado



Fuente: Autores del proyecto

11.3. ANDES SIGNER

Es una herramienta desarrollada por AndesSCD (Andes Servicios de Certificación Digital) con el objetivo de realizar la firma digital de documentos electrónicos.

11.3.1. Requerimientos Técnicos. Para el adecuado funcionamiento de la herramienta se requieren los siguientes requerimientos técnicos:

- ✓ Sistema Operativo:
  - ➢ Windows XP Service Pack 3
  - ➢ Windows Vista - Arquitecturas de 32 y 64 bits
  - ➢ Windows 7 - Arquitecturas de 32 y 64 bits
  - ➢ Windows 8 - Arquitecturas de 32 y 64 bits
- ✓ Espacio en Disco duro
  - ➢ 20 Mb de espacio disponible en el disco duro

- ✓ Memoria RAM
  - ➢ 256 Mb de Memoria RAM
- ✓ Procesador
  - ➢ Procesador con velocidad de 800 MHZ o superior

11.3.2. Proceso de Instalación. La instalación de la herramienta se puede realizar a través de la memoria flash USB suministrada al realizar la inscripción en la plataforma CLIF, también es posible realizar la descarga desde la web de ANDESSCD O desde enlace desde el sitio web de la plataforma CLIF.

Figura 155. Medios de obtención de la herramienta andes signer

USB

- Memoria USB entregada a la hora de la inscripción .

AndesSCD

- https://www.andesscd.com.co/docs/Software/andes%20signer%203.2.zip

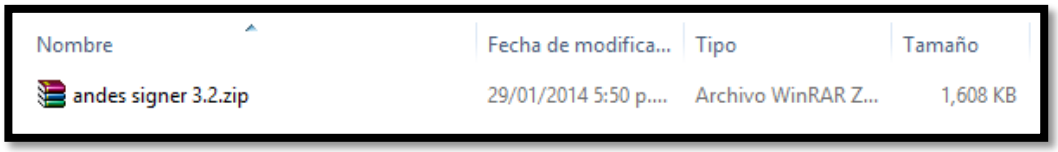
CLIF

- http://www.clif.co/descargas/firmadigital/andessigner.zip

Fuente**:** Autores del proyecto

Al realizar la descarga en una ubicación fácilmente accesible como "**Escritorio**" se obtendrá un archivo comprimido con el instalador (Véase la figura 156).

Figura 156. Archivo comprimido con el instalador de la herramienta andes signer



Fuente**:** Autores del proyecto

Para poder continuar es necesario realizar la descompresión para obtener el instalador de la herramienta; es posible realizar la descompresión con una herramienta gratuita llamada 7zip. Descargar de la siguiente los siguientes enlaces y realizar la instalación que costa de pocos y sencillos pasos.

Figura 157. Enlaces de descarga herramienta 7Zip

7Zip - Arquitecturas 32 bits

- http://downloads.sourceforge.net/sevenzip/7z920.msi

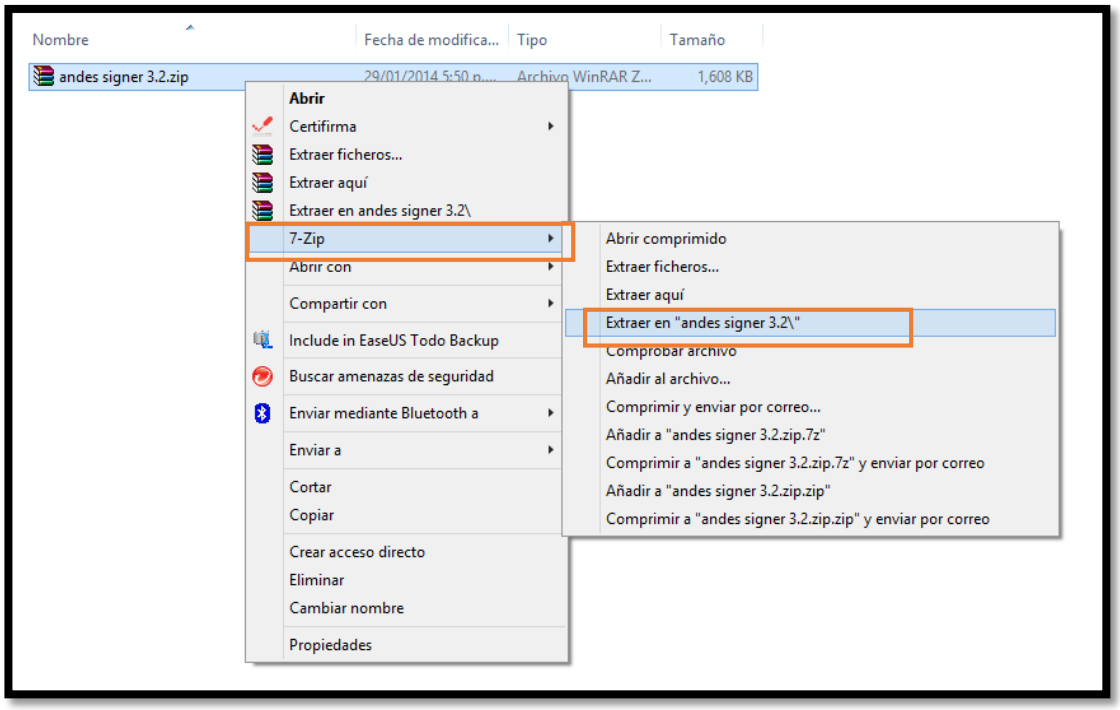
7Zip - Arquitectura 64 Bits

- http://downloads.sourceforge.net/sevenzip/7z920-x64.msi

Fuente: Autores del proyecto

Ejecutamos la descompresión del instalador haciendo clic derecho sobre el archivo descargado denominado "**andes signer 3.2.zip**", buscamos dentro del menú contextual la opción 7-Zip y dentro del submenú la opción Extraer en "**andes signer 3.2**", (Véase la figura 158).

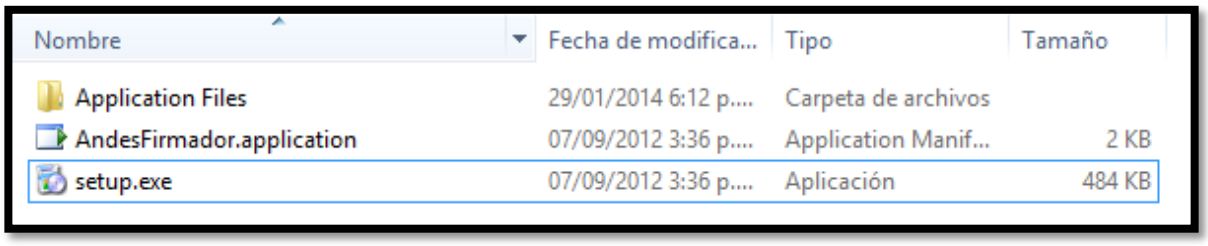
Figura 158. Proceso para realizar descompresión de los archivos mediante 7Zip



Fuente: Autores del proyecto

Esperamos a que se realice la descompresión de la herramienta y obtendremos la carpeta, nos desplazamos en ellas hasta ubicar el instalador de Andes Signer, (Véase la figura 159).

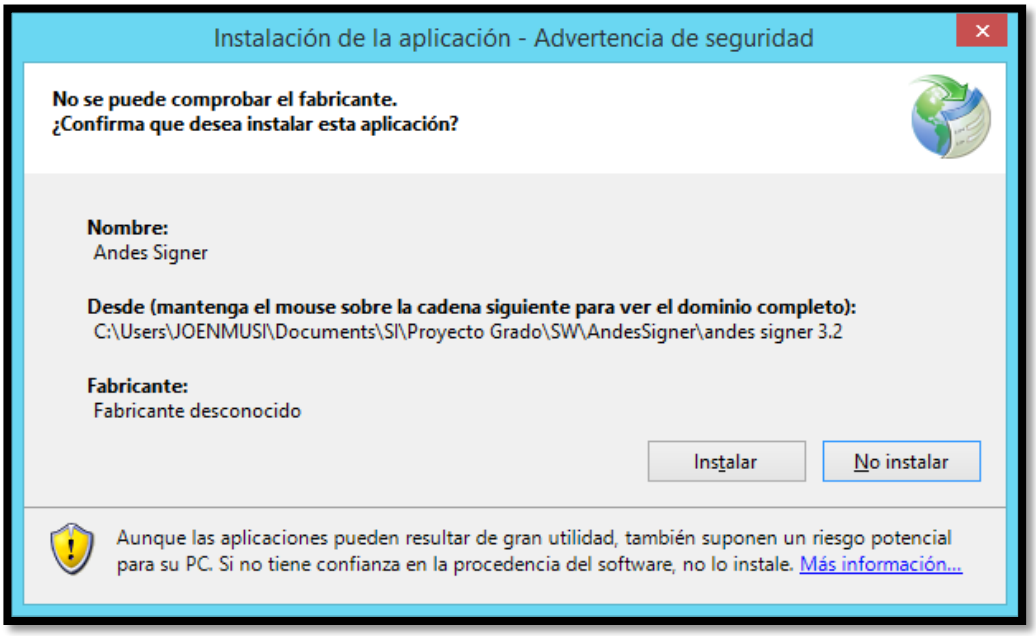
Figura 159. Archivos de instalación herramienta andes Signer



Fuente: Autores del proyecto

Procedemos con la instalación de la herramienta Andes Signer haciendo doble clic sobre el archivo "**setup.exe**", esperamos unos segundos a que se muestre el asistente que nos guiara durante el proceso de instalación. Para poder realizar la instalación de la herramienta se debe contar con privilegios de administrador. Procedemos con la instalación haciendo clic en el botón "**Instalar**". (Véase la figura 160).

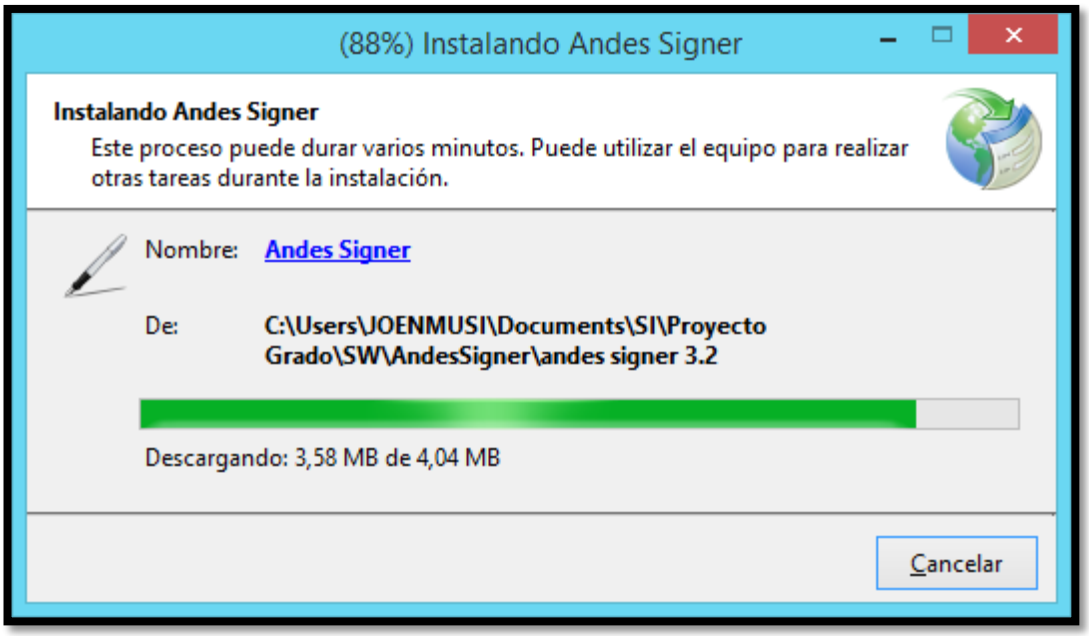
Figura 160. Asistente de instalación andes Signer



Fuente: Autores del proyecto

Inicia el proceso de instalación, esto puede tardar unos minutos. (Véase la figura 161).

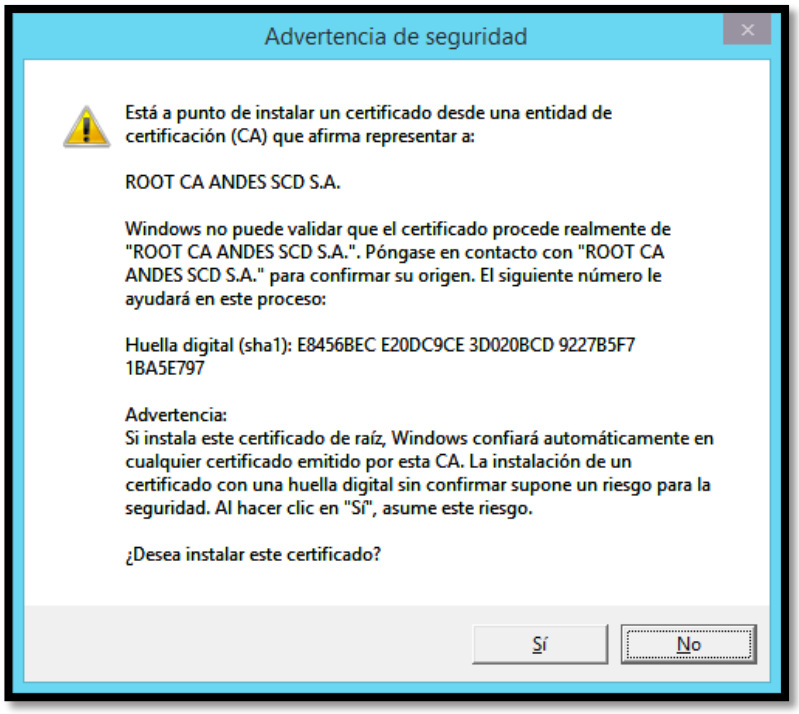
Figura 161. Asistente de instalación andes Signer, proceso de instalación



Fuente: Autores del proyecto

Si durante la instalación nos solicita autorización para realizar operaciones relacionadas con Andes Signer, hacemos clic en el botón "**SI**", para que la instalación se desarrolle sin inconvenientes. Una vez finalice la instalación, el asistente nos pedirá autorización para realizar la instalación de los certificados desde la entidad de certificación (CA), hacemos clic en el botón "**Si**". (Véase la figura 162).

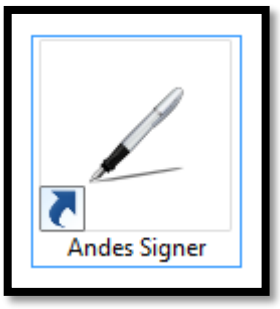
Figura 162. Autorización de instalación de certificados de la entidad de certificación de andes signer



Fuente: Autores del proyecto

Debemos encontrar en el "**Escritorio**" del equipo un acceso directo a la herramienta instalada por Andes Signer.

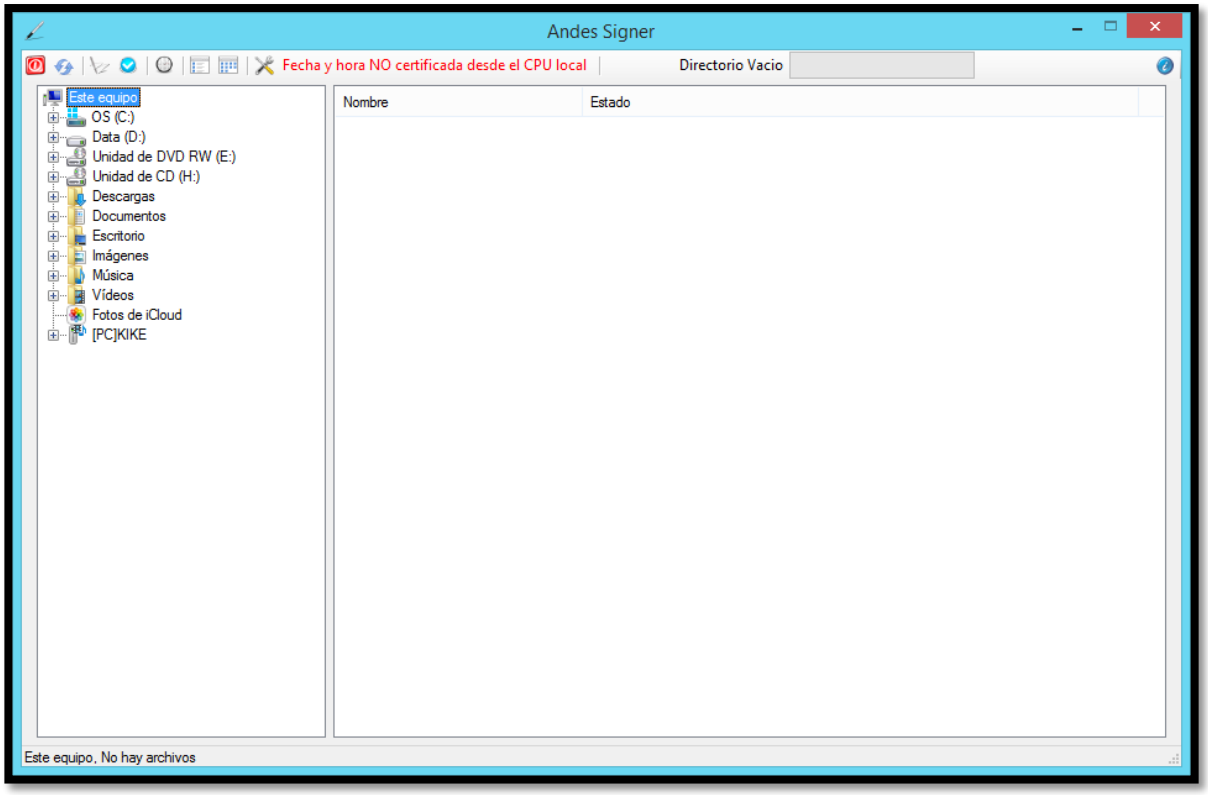
Figura 163. Acceso directo instalado por la herramienta andes Signer



Fuente: Autores del proyecto

Ejecutando “**Andes Signer**” podemos visualizar la interfaz para realizar la firma digital.

Figura 164. Interfaz de la herramienta certitool



Fuente: Autores del proyecto

11.3.3. Firma digital mediante Andes Signer. Para realizar la firma digital de los diferentes documentos electrónicos se deben haber completado previamente los procedimientos para “**Obtención de certificados de firma digital**”, “**Generación de certificados de firma digital**”, “**Instalación de certificado de firma digital**” e “**Instalación de certificado raíz**”, adicionalmente se debe tener instalada la herramienta “**Andes Signer**” y estar almacenado en el equipo de cómputo el certificado de firma digital en formato “**p12**”.

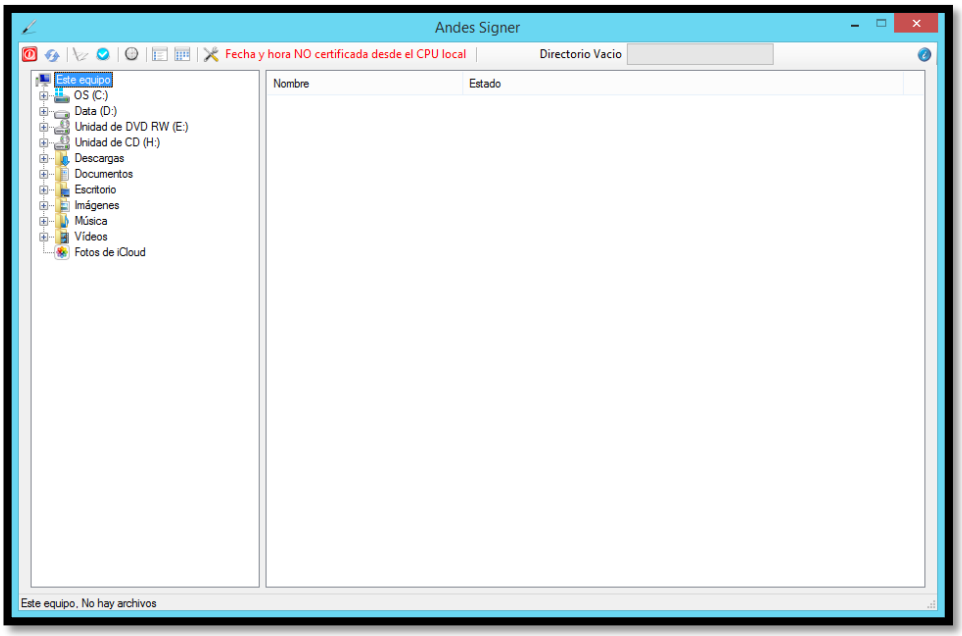
Para iniciar el proceso de firma digital buscamos en el escritorio el acceso directo a la aplicación "**Andes Signer**" y hacemos doble clic. (Véase la figura 165).

Figura 165. Acceso directo instalado por la herramienta andes Signer

Fuente: Autores del proyecto

Se abrirá la interfaz de la aplicación, esta está compuesta por una serie de botones de opción, la primera "**Salir**" que nos permitirá salir de la herramienta en cualquier, momento, la segunda "**Refrescar árbol de carpetas**" que nos permitirá actualizar el listado de directorios de la parte izquierda de la herramienta, la tercera opción es "**Firmar**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información y la cuarta opción "**Verificar la firma seleccionada**" que nos permitirá constatar la firma realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 166).

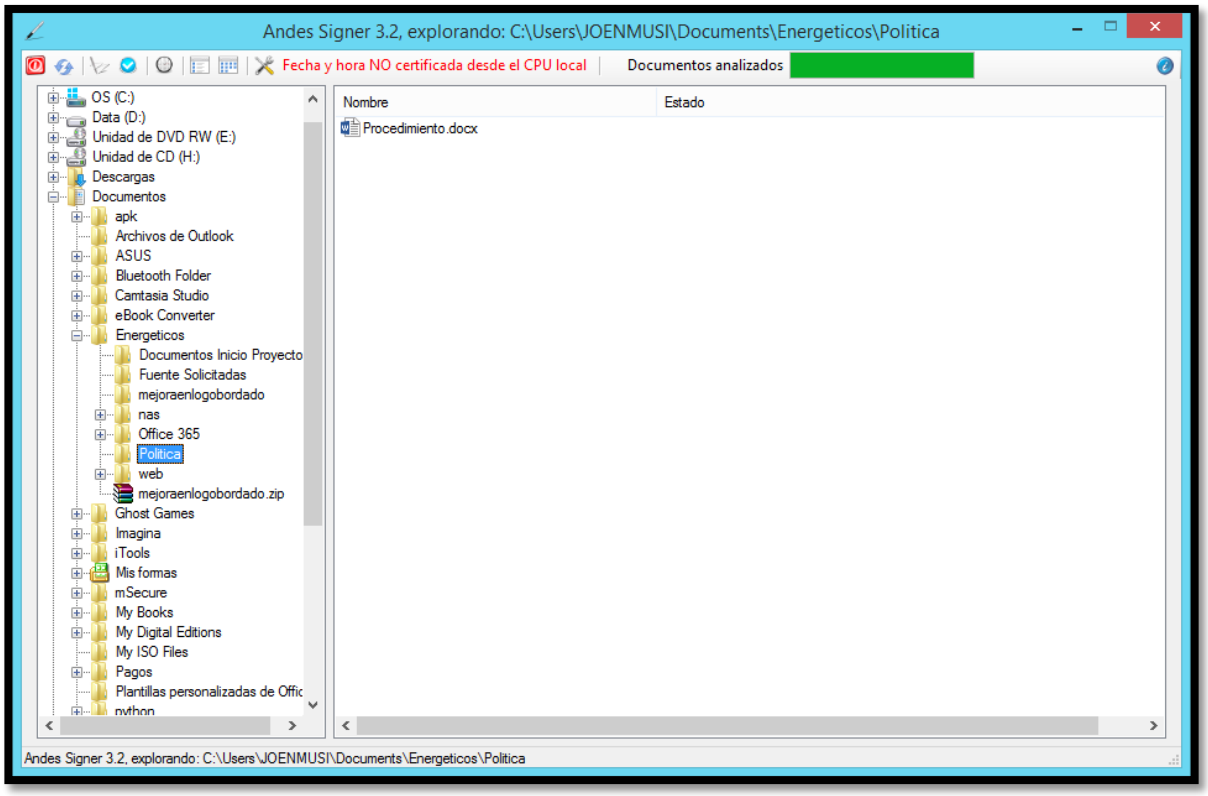
Figura 166. Interfaz de la herramienta andes Signer



Fuente: Autores del proyecto

Haciendo uso del árbol de carpetas o directorios de la parte izquierda de la herramienta, navegamos expandiendo (Haciendo clic en el símbolo +) carpetas hasta localizar el documento electrónico deseado y procedemos a hacer clic en la opción "**Firmar**". (Véase la figura 167).

Figura 167. Interfaz de la herramienta andes Signer, firmar digitalmente



Fuente**:** Autores del proyecto

Botón firmar. (Véase la figura 168).

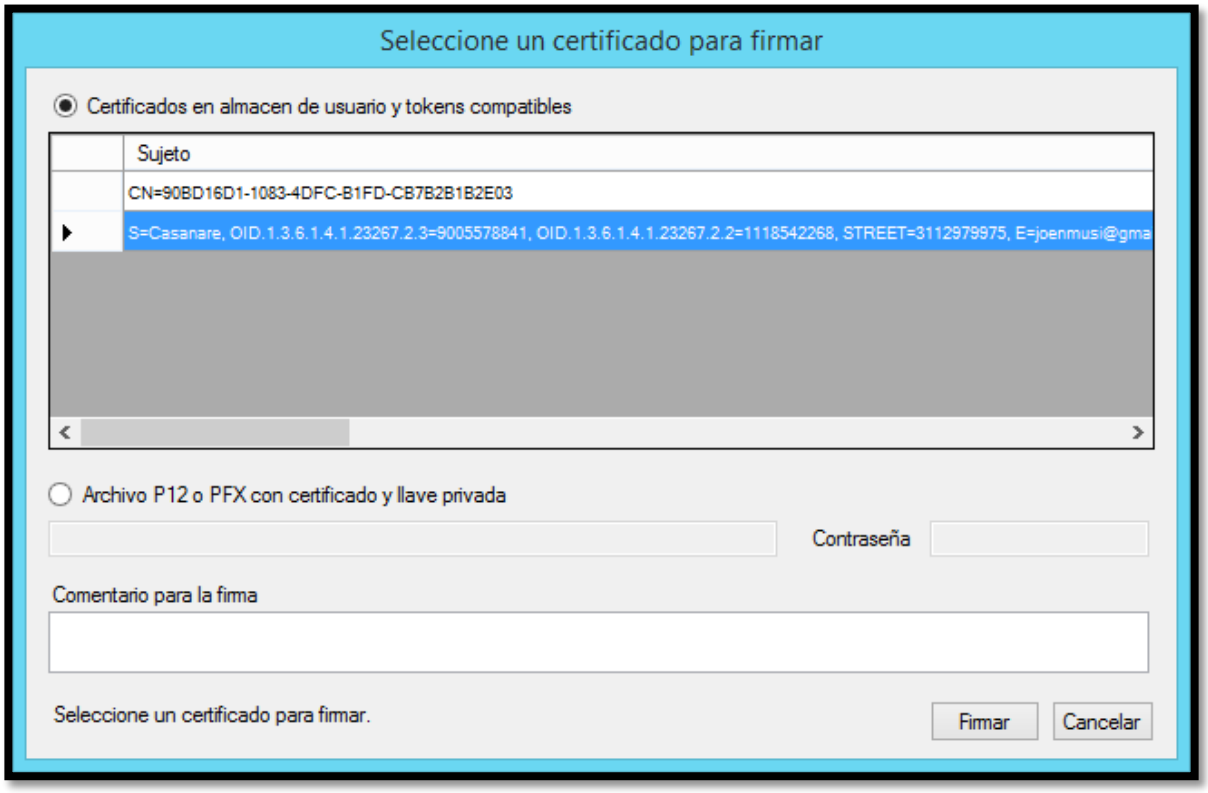
Figura 168. Botón firmar documento de la interfaz de andes Signer

Fuente**:** Autores del proyecto

La aplicación "**Andes Signer**" desplegará un cuadro de dialogo que nos mostrara dos opciones de uso del certificado de firma digital, la primera opción denominada "**Certificados en almacén de**

usuario y tokens compatibles" en el cual podremos utilizar el certificado de firma digital siempre y cuando se haya realizado el procedimiento "**Instalación de certificado de firma digital**", la segunda opción denominada "**Archivo P12 o PFX con certificado y llave privada**" en el cual podremos utilizar el certificado de firma digital siempre y cuando se haya realizado el procedimiento "**Generación de certificado de firma digital**". Podemos realizar el proceso de firma digital por cualquiera de las dos opciones, lo anterior no afecta el resultado y es decisión netamente del usuario. (Véase la figura 169)

Figura 169. Opciones de uso de certificado de firma digital de la herramienta andes Signer

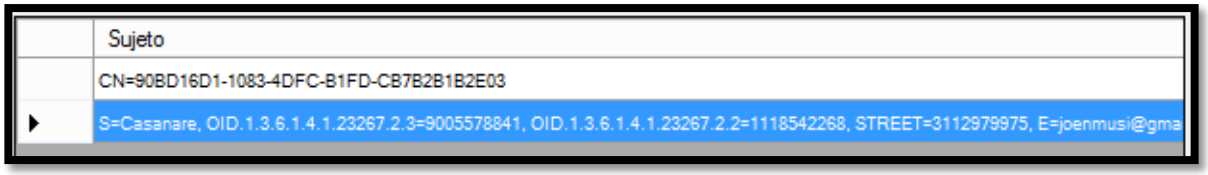


Fuente: Autores del proyecto

Procederemos a hacer el firmado con la opción "**Certificados en almacén de usuario y tokens compatibles**", para ello dentro de la cuadricula bajo esta opción seleccionamos el certificado de firma digital que posee nuestra información. Si desplazamos la barra horizontal de la parte inferior podemos

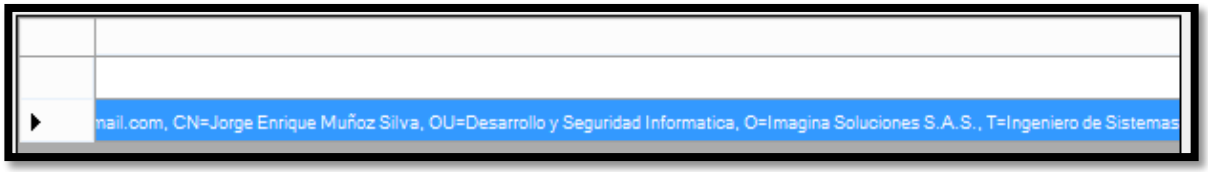
observar toda la información del certificado tanto del firmante como de la entidad de certificación. (Véase la figura 170).

Figura 170. Información de certificado de firma digital de la herramienta andes Signer A



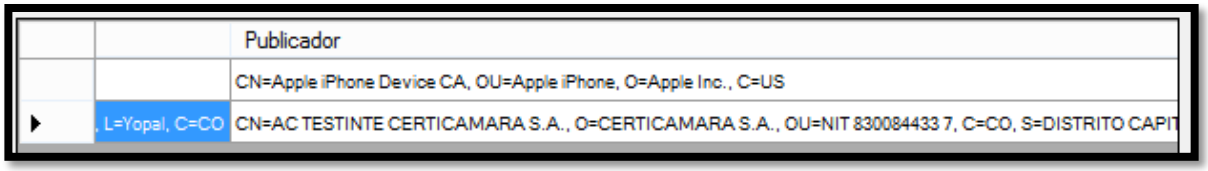
Fuente: Autores del proyecto

Figura 171. Información de certificado de firma digital de la herramienta andes Signer B



Fuente: Autores del proyecto

Figura 172. Información de certificado de firma digital de la herramienta andes Signer A



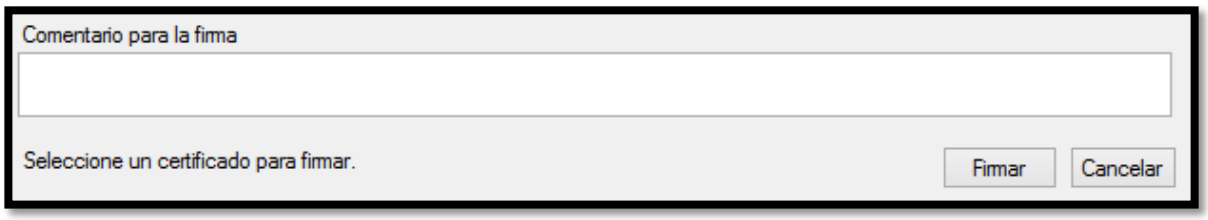
Fuente: Autores del proyecto

Figura 173. Información de certificado de firma digital de la herramienta andes Signer A

Fuente: Autores del proyecto

Una vez seleccionado el certificado de firma digital la herramienta en la parte inferior nos permite escribir algún comentario para la firma del documento electrónico, para finalizar el proceso hacemos clic en el botón "**Firmar**". (Véase la figura 174).

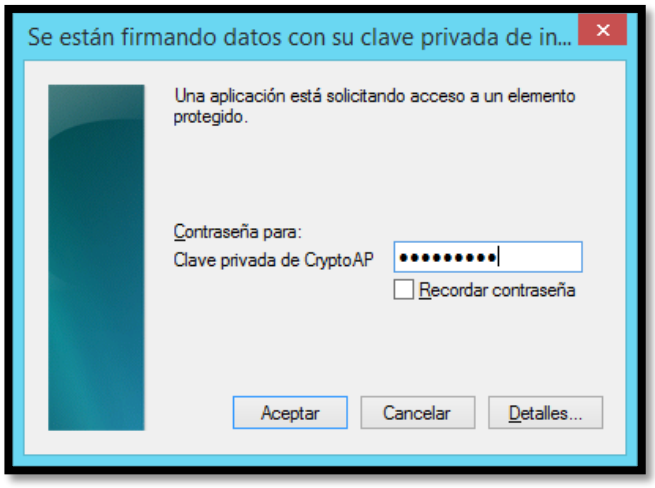
Figura 174. Cuadro de texto para adicionar comentarios de la firma digital en la herramienta andes Signer



Fuente: Autores del proyecto

La aplicación "**Andes signer**" desplegará un cuadro de dialogo en el cual debemos ingresar la contraseña de **USO** del certificado de firma digital asignada en el procedimiento "**Instalación de certificado de firma digital**" y hacemos clic en el botón "**Aceptar**". (Véase la figura 175).

Figura 175. Solicitud de contraseña de uso del certificado de firma digital en andes signer

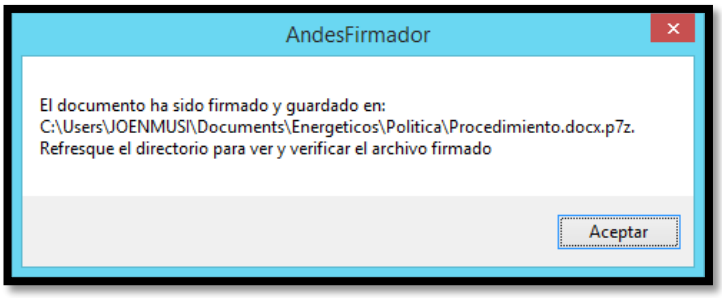


Fuente: Autores del proyecto

Advertencia: La contraseña de **USO** asignada en el procedimiento "**Instalación de certificado de firma digital**" puede ser distinta a la contraseña de **PROTECCIÓN** del certificado de firma digital asignada en el procedimiento "**Obtención de certificados de firma digital**". Por seguridad es recomendable que **NO** se active la casilla "**Recordar contraseña**" para evitar que el certificado de firma digital pueda ser utilizado sin su consentimiento, teniendo en cuenta que este cuenta con total validez jurídica.

La herramienta "**Andes Signer**" genera un cuadro de dialogo que informa que el documento ha sido firmado exitosamente y muestra la ruta de donde fue almacenado el documento electrónico firmado digitalmente. (Véase la figura 176).

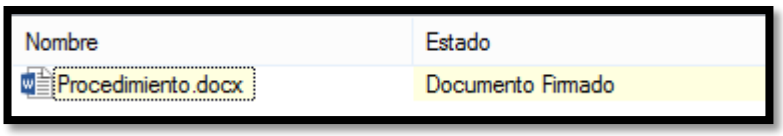
Figura 176. Mensaje de operación de firma digital exitoso de andes Signer



Fuente**:** Autores del proyecto

La grilla o cuadricula de la parte derecha de la herramienta "**Andes Signer**" muestra el documento firmado anteriormente en un color amarillo y su estado indica que es un "**Documento firmado**". (Véase la figura 177).

Figura 177. Listado de resultados del proceso de firma digital de andes Signer



Fuente: Autores del proyecto

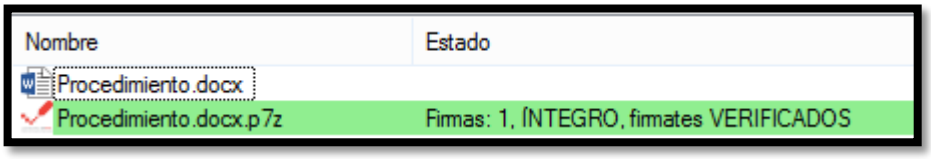
La herramienta requiere que se actualice el árbol de directorios, haga clic en el siguiente botón para refrescar. (Véase la figura 178).

Figura 178. Botón actualizar de la interfaz de andes Signer

Fuente: Autores del proyecto

El procedimiento anterior a su vez actualiza la grilla o cuadricula que muestra el nombre de los documentos electrónicos y el estado de los mismos. Note que el documento firmado anteriormente ha quedado de color blanco y se ha creado un archivo con extensión "**p7z**" resaltado en color verde y su estado indica que posee una (1) firma, que es un documento íntegro y que los firmantes han sido verificados (Véase la figura 179).

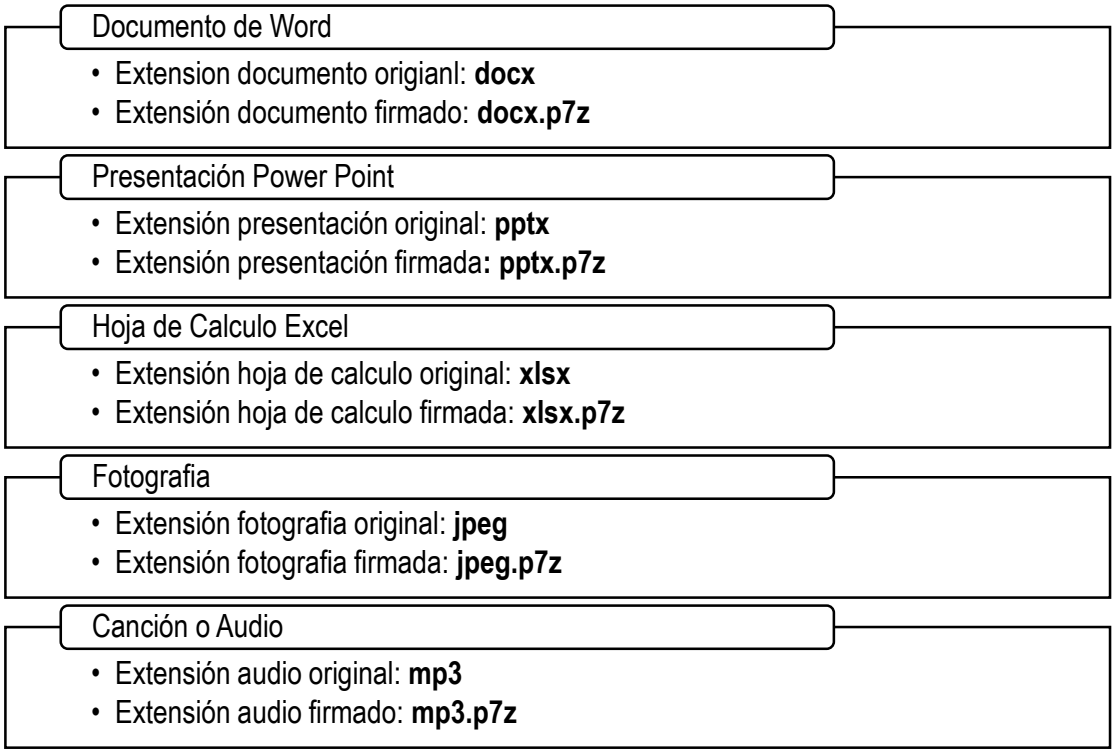
Figura 179. Archivos generados del proceso de firma digital mediante andes signer



Fuente: Autores del proyecto

Los archivos al ser firmados digitalmente por la herramienta "**Andes Signer**" se les agrega o adiciona una extensión de archivo anexo a la extensión del tipo de archivo que fue firmado, a continuación podemos ver algunos ejemplos de extensiones de documentos electrónicos comunes y sus respectivas extensiones una vez firmados:

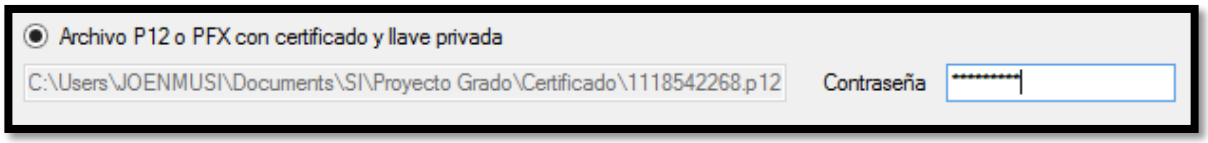
Figura 180. Ejemplos de extensiones de los archivos antes y después del proceso de firma digital mediante andes Signer



Fuente: Autores del proyecto

Procederemos a hacer el firmado con la opción "**Archivo P12 o PFX con certificado y llave privada**", para ello seleccionaos dicha opción, automáticamente la herramienta despliega un cuadro de dialogo para seleccionar el certificado de firma digital con extensión "**p12**" posteriormente ingresar la contraseña de **PROTECCIÓN** obtenida en el procedimiento "**Generación de certificado de firma digital**". (Véase la figura 181).

Figura 181. Selección de certificado e ingreso de contraseña de certificado digital en la herramienta andes Signer

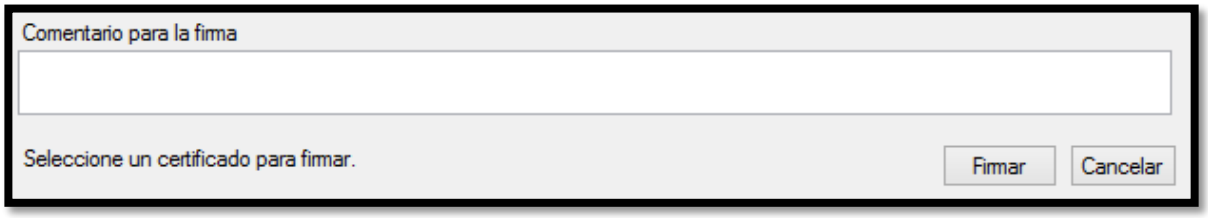


Fuente: Autores del proyecto

Advertencia: La contraseña de **USO** asignada en el procedimiento "**Instalación de certificado de firma digital**" puede ser distinta a la contraseña de **PROTECCIÓN** del certificado de firma digital asignada en el procedimiento "**Obtención de certificados de firma digital**".

Una vez seleccionado el certificado de firma digital la herramienta en la parte inferior nos permite escribir algún comentario para la firma del documento electrónico, para finalizar el proceso hacemos clic en el botón "**Firmar**". (Véase la figura 182).

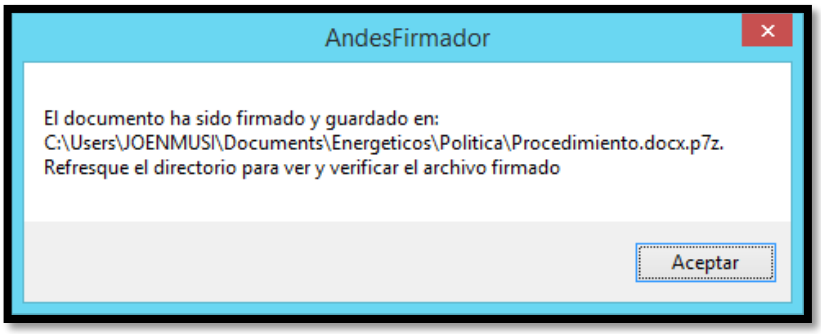
Figura 182. Cuadro de texto para adicionar comentarios de la firma digital en la herramienta andes Signer



Fuente**:** Autores del proyecto

La herramienta "**Andes Signer**" genera un cuadro de dialogo que informa que el documento ha sido firmado exitosamente y muestra la ruta de donde fue almacenado el documento electrónico firmado digitalmente. (Véase la figura 183).

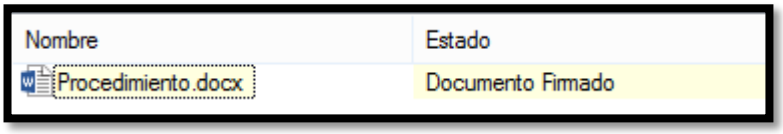
Figura 183. Mensaje de operación de firma digital exitoso de andes Signer



Fuente: Autores del proyecto

La grilla o cuadricula de la parte derecha de la herramienta "**Andes Signer**" muestra el documento firmado anteriormente en un color amarillo y su estado indica que es un "**Documento firmado**". (Véase la figura 184).

Figura 184. Listado de resultados del proceso de firma digital de andes Signer



Fuente: Autores del proyecto

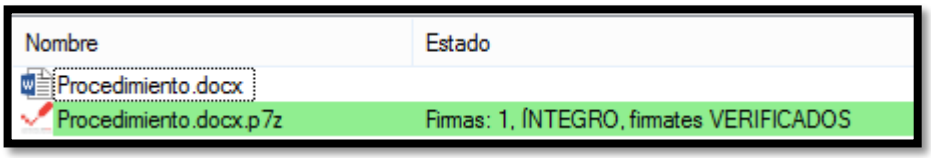
La herramienta requiere que se actualice el árbol de directorios, haga clic en el siguiente botón para refrescar. (Véase la figura 185).

Figura 185. Botón actualizar de la interfaz de andes Signer

Fuente: Autores del proyecto

El procedimiento anterior a su vez actualiza la grilla o cuadricula que muestra el nombre de los documentos electrónicos y el estado de los mismos. Note que el documento firmado anteriormente ha quedado de color blanco y se ha creado un archivo con extensión "**p7z**" resaltado en color verde y su estado indica que posee una (1) firma, que es un documento íntegro y que los firmantes han sido verificados (Véase la figura 186).

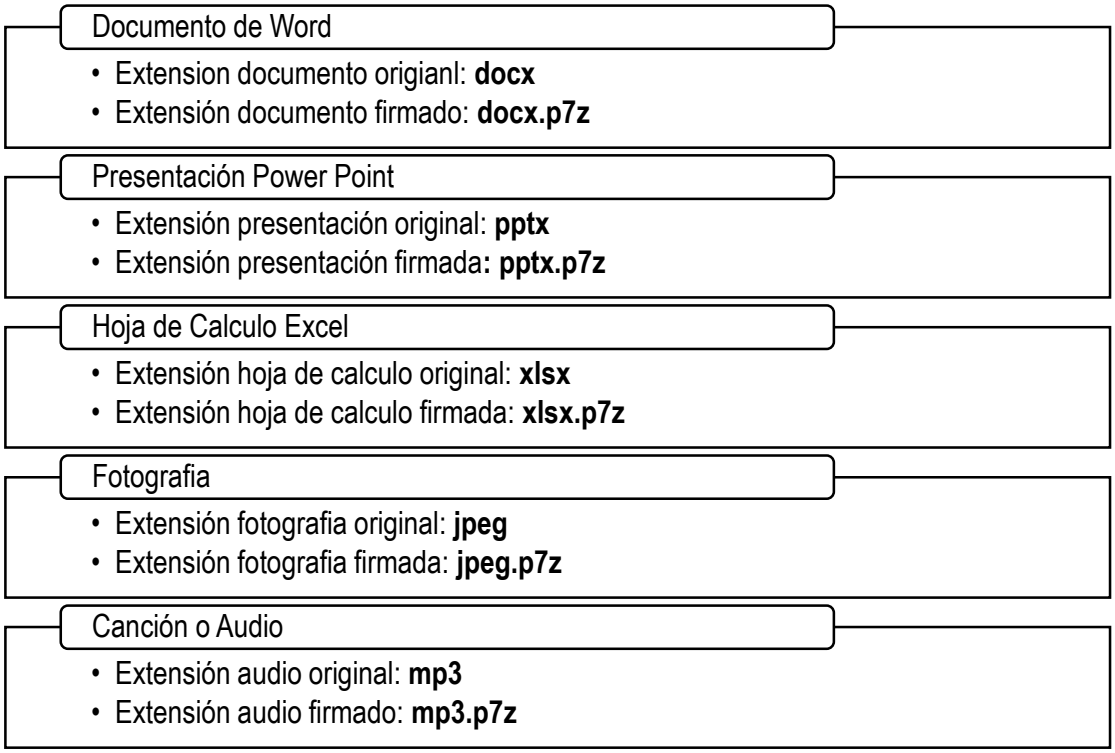
Figura 186. Archivos generados del proceso de firma digital mediante andes signer



Fuente: Autores del proyecto

Los archivos al ser firmados digitalmente por la herramienta "**Andes Signer**" se les agrega o adiciona una extensión de archivo anexo a la extensión del tipo de archivo que fue firmado, a continuación podemos ver algunos ejemplos de extensiones de documentos electrónicos comunes y sus respectivas extensiones una vez firmados:

Figura 187. Ejemplos de extensiones de los archivos antes y después del proceso de firma digital mediante andes Signer



Fuente: Autores del proyecto

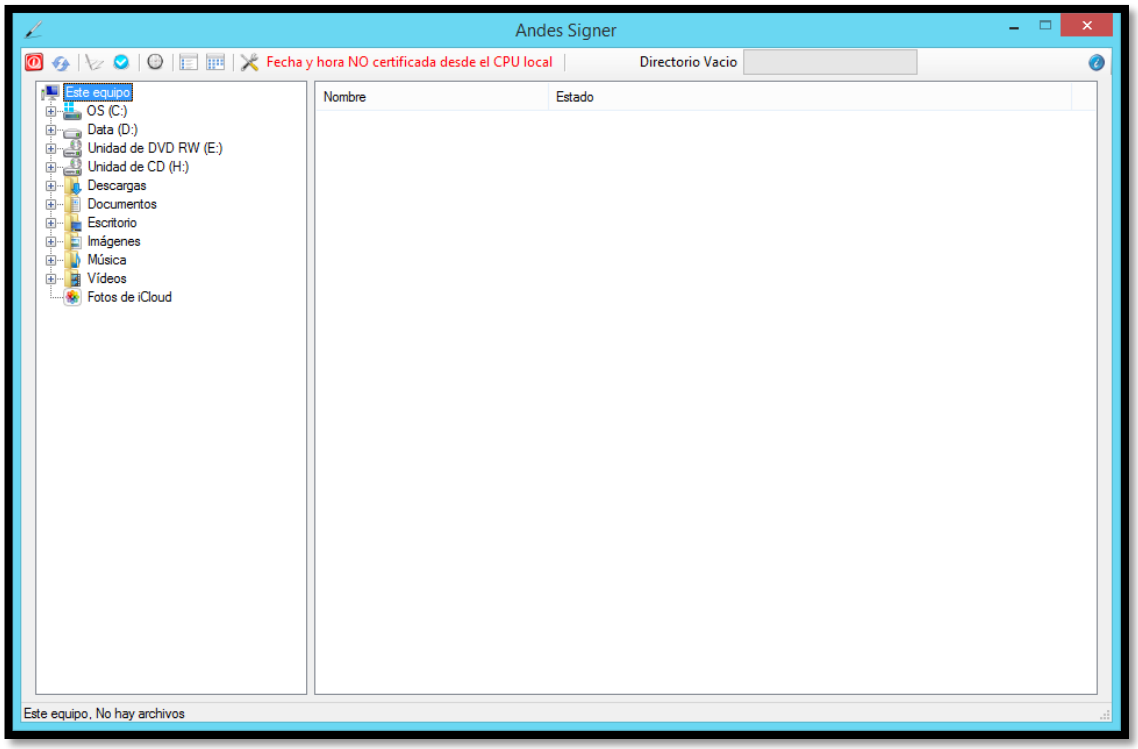
11.3.4. Verificar firma digital mediante Andes Signer. Para iniciar el proceso de verificación de validez de la firma digital buscamos en el escritorio el acceso directo a la aplicación "**Andes Signer**" y hacemos doble clic. (Véase la figura 188).

Figura 188. Acceso directo instalado por la herramienta andes Signer

Fuente: Autores del proyecto

Se abrirá la interfaz de la aplicación, esta está compuesta por una serie de botones de opción, la primera "**Salir**" que nos permitirá salir de la herramienta en cualquier, momento, la segunda "**Refrescar árbol de carpetas**" que nos permitirá actualizar el listado de directorios de la parte izquierda de la herramienta, la tercera opción es "**Firmar**" que nos permitirá firmar cualquier tipo de documento electrónico con nuestro certificado de firma digital con el objetivo de garantizar integridad de la información y la cuarta opción "**Verificar la firma seleccionada**" que nos permitirá constatar la firma realizada sobre cualquier tipo de documento electrónico y comprobar que esté sigue manteniendo su integridad y posee validez jurídica. (Véase la figura 189).

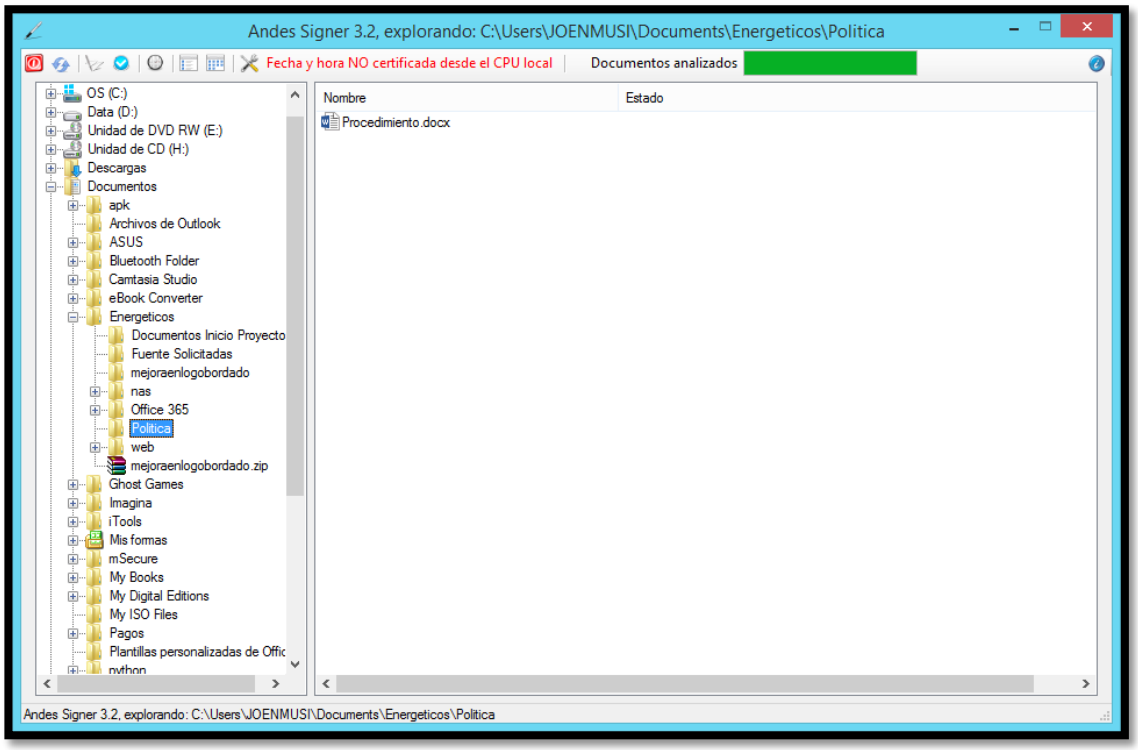
Figura 189. Interfaz de la herramienta andes Signer



Fuente: Autores del proyecto

Haciendo uso del árbol de carpetas o directorios de la parte izquierda de la herramienta, navegamos expandiendo (Haciendo clic en el símbolo +) carpetas hasta localizar el documento electrónico deseado y procedemos a hacer clic en la opción "**Verificar firma**". (Véase la figura 190).

Figura 190. Interfaz de la herramienta andes Signer, verificar firma



Fuente**:** Autores del proyecto

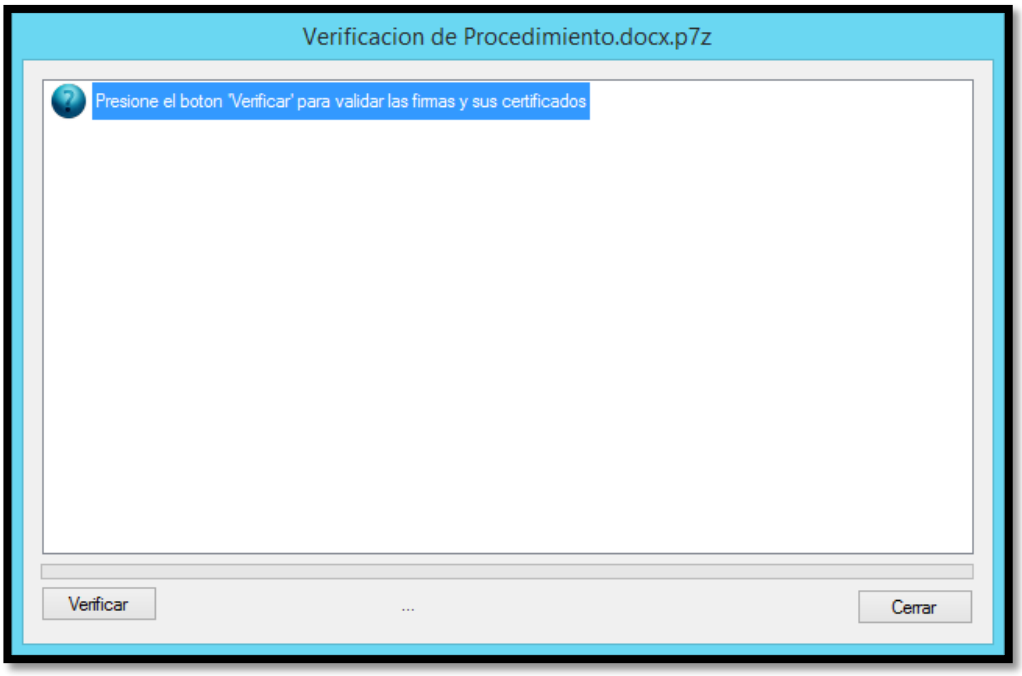
Botón firmar. (Véase la figura 191).

Figura 191. Botón verificar firma de la interfaz de andes Signer

Fuente: Autores del proyecto

La aplicación "**Andes Signer**" desplegará un cuadro de dialogo con la información de la verificación de la firma digital, para comprobar la validez hacemos clic en el botón "**Verificar**" de la parte inferior izquierda de la herramienta. (Véase la figura 192).

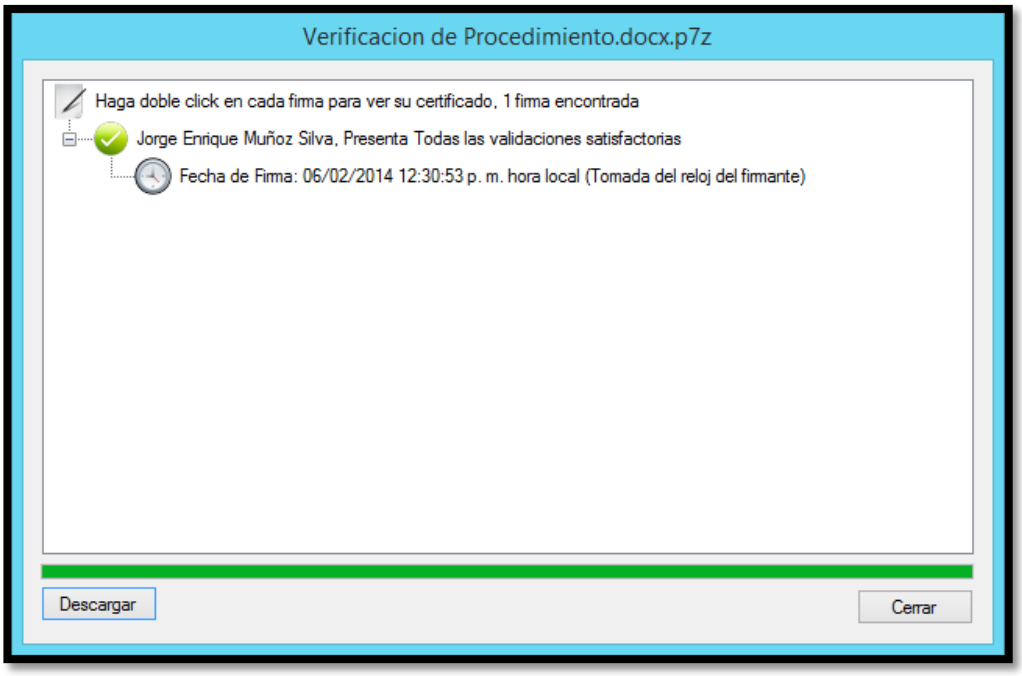
Figura 192. Inicio de proceso de verificación de la firma en la herramienta andes Signer



Fuente: Autores del proyecto

El asistente muestra la información del firmante, la fecha y hora de la firma digital. (Véase la figura 193).

Figura 193. Información general del firmante en la herramienta andes Signer



Fuente**:** Autores del proyecto

Haciendo uso del botón "**Descargar**" de la parte inferior izquierda de la herramienta podemos descargar el documento en formato original para hacer la revisión de su contenido si es necesario. Para cerrar la ventana de verificación presionamos en botón "**Cerrar**" de la parte inferior derecha. (Véase la figura 194).

Figura 194. Mensaje de operación de extraer el archivo original exitoso después de verificar firma digital mediante andes Signer

Fuente: Autores del proyecto

12. MARCO LEGAL

El marco legal proporciona las bases sobre las cuales las instituciones construyen y determinan el alcance y naturaleza de la participación política, a su vez faculta a la autoridad correspondiente para que lleve a cabo las labores de administración de conformidad a la estructura detallada dentro de sus mismas provisiones regulatorias y leyes interrelacionadas entre sí.

En Colombia los certificados y firmas digitales están enmarcadas sobre un conjunto de leyes que se detallan a continuación:

Ley 270 de 1996 o Ley Estatutaria de la administración de justicia, donde se establece la autorización general siempre vigente para propender por la incorporación de tecnología avanzada al servicio de la Administración de justicia, y regular los trámites judiciales y administrativos que se adelanten en los despachos judiciales, en los aspectos no previstos por el legislador.

Ley 527 de 1999 de 18 de agosto, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales(las cuales poseen plena presunción de autenticidad amparada bajo una entidad de certificación), y se establecen las entidades de certificación y se dictan otras disposiciones, logro puntualmente la consolidación del principio de equivalencia funcional con los medios tradicionales, otorgando total validez probatoria y jurídica de los mensajes de datos, actualmente esta ley posibilita iniciar una causa ante la justicia al contar con las garantías ofrecidas por la equivalencia funcional que elimino la necesidad de estatutos especiales para este tipo de actividades.

Ley 794 de 2003: Actos de comunicación procesal por medios electrónicos.

Ley 962 de 2005: Actuaciones administrativas por medios electrónicos.

Ley 1150 de 2007: Contratación del Estado por medios electrónicos.

Decreto 1747 de 2000: reglamenta parcialmente la Ley 527 de 1999 en aspectos relacionados con las entidades de certificación, los certificados y las firmas digitales.

Decreto 1929 de 2007: por el cual se reglamenta el artículo 616-1 del Estatuto Tributario.

Decreto 12 de 2002: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. Este decreto asigno las funciones que tenía la Superintendencia de Industria y Comercio (SIC) en materia de entidades de certificación de firmas digitales al Organismo Nacional de Acreditación de Colombia (ONAC).

Resolución 26930 de 2000 de la Superintendencia de Industria y Comercio: referencia los requisitos que deben cumplir las entidades de certificación abiertas o cerradas para solicitar su autorización y funcionamiento, clasificación que depende de los servicios que prestan y finalmente se desarrolla el tema de las firmas auditoras para las entidades de certificación y el contenido del informe de auditoría necesario para la autorización, el cual debe ser actualizado por lo menos anualmente.

12.1. ACTOS ADMINISTRATIVOS

Las entidades de certificación digital autorizadas por la SIC antes de la promulgación del decreto 12 de 2002 se encuentras establecidas mediante actos administrativos[31] los cuales fueron suministrados por la SIC a los autores de la presente guía mediante radicado "14-187143- -4- 1" (Ver Anexo A) donde se define:

- ✓ Sociedad Cameral de Certificación Digital Certicámara, S.A.
  Autorizada mediante resolución N°. 1007 del 24 de enero de 2002
  - ➢ Autorización de nuevos servicios – Ampliación de la autorización
    - ➢ **Resolución N°. 22456 (10/09/2004)**

[31]. En este sentido se identifica como acto administrativo a cualquier manifestación de voluntad para producir efectos jurídicos, que se dicte en ejercicio de la función administrativa, por cualquier órgano del Estado e incluso por los particulares (arts. 1 y 82).

- Resolución N°. 28012 (12/11/2004)
- Resolución N°. 9887 (12/04/2007)
- Resolución N°. 3816 (30/01/2009)

✓ Gestión de Seguridad Electrónica S.A. – GSE S.A.

Autorizada mediante resolución N°. 23344 del 2 de mayo de 2009

- Autorización de nuevos servicios – Ampliación de la autorización
  - Resolución N°. 1194 (21/01/2010)

✓ Andes Servicio de Certificación Digital S.A. – ANDES SCD

Autorizada mediante resolución 14349 del 23 de marzo de 2002

13. RESULTADOS OBTENIDOS

Para la ejecución de las pruebas piloto de la presente guía se realizaron dos (2) encuestas las cuales fueron aplicadas a cincuenta (50) MIPYMES de la ciudad de Yopal, departamento de Casanare. La primera con el objetivo de realizar un diagnóstico que permitiera determinar el estado inicial del contexto en el cual se desarrollaría la implementación de la guía y la segunda con el objetivo de realizar la medición del impacto de dicha implementación y el nivel de satisfacción de los empresarios de las MIPYMES frente al documento guía y aspectos tratados.

En la encuesta de medición se buscó inicialmente determinar el impacto del documento guía en las MIPYMES, el nivel de comprensión del documento guía en general y de los procedimientos de obtención, generación e instalación del certificado de firma digital, así mismo la facilidad de uso de las diferentes herramientas (Software) suministrado por las entidades de certificación, igualmente se buscó determinar el tiempo de ejecución del proceso de firma digital en las diferentes actividades de las empresas.

Basados en los sectores económicos en los que se distribuyen las cincuenta (50) MIPYMES, resultado obtenido mediante la aplicación de las encuestas de diagnóstico, se procedió a realizar la medición del impacto de la implementación del documento guía.

A continuación se da a conocer la información recopilada al desarrollar la primera encuesta.

13.1. DATOS DE LA ENCUESTA DIAGNÓSTICO

Cuadro 1 Resultados de los sectores económicos a los que pertenecen las mipymes encuestadas

	1) Seleccione el sector económico al que pertenece su empresa
Servicios	16
Industrial	5
Comercial	27
Salud	2
Otro, cual	0

Fuente: Autores del proyecto

Cuadro 2 Resultados obtenidos en las encuestas de diagnóstico aplicadas a las cincuenta (50) mipymes

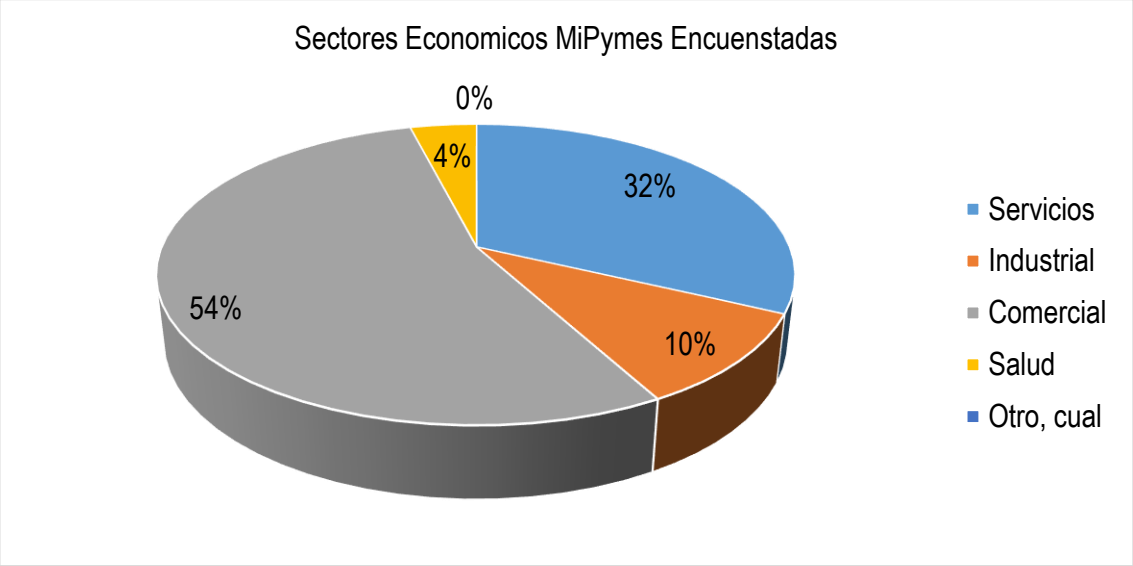
Pregunta	Si	No
2) ¿Dentro del desarrollo de los procesos de su empresa hace uso de equipos de cómputo para la generación, administración y/o almacenamiento de archivos en formato electrónico?	50	0
3) ¿El sistema operativo que se encuentra implementado en los equipos de cómputo de su empresa es Microsoft Windows?	50	0
4) ¿Conoce usted algún mecanismo para la protección de sus archivos en formato electrónico que son importantes para su empresa (Facturas, contratos, correos electrónicos, etc)?	20	30
5) ¿Está interesado en implementar herramientas que agreguen seguridad a la generación, administración y/o almacenamiento de archivos en formato electrónico?	40	10
6) ¿Conoce o está familiarizado con el concepto de Firma digital?	15	35
7) La firma digital es un mecanismo que permite identificar que su información no ha sido alterada después de ser firmada y comprobar que fue usted quien efectivamente generó el archivo electrónico, posee la misma validez de la firma manuscrita pero con numerosas ventajas técnicas. ¿Está interesado en implementar firmas digitales para asegurar sus archivos en formato electrónico?	40	10
8) ¿Le gustaría recibir una asesoría (Conceptos básicos, herramientas necesarias, documento guía) para la implementación de este mecanismo de seguridad?	50	0

Fuente: Autores del proyecto

13.2. ANALISIS DE LOS DATOS CAPTURADOS EN LA ENCUESTA DIAGNÓSTICO

En la encuesta de diagnóstico se buscó inicialmente determinar los sectores económicos a los cuales pertenecen las cincuenta (50) MIPYMES que fueron tomadas como muestra para la ejecución de las pruebas piloto.

Gráfico 1 Porcentajes de los sectores económicos a los que pertenecen las mipymes encuestadas

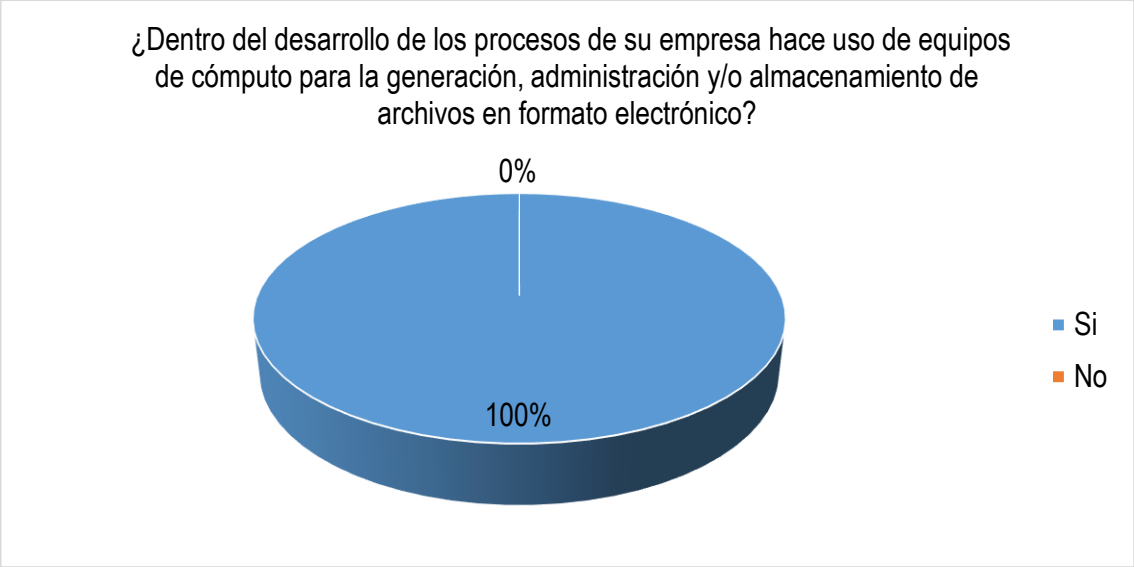


Fuente: Autores del proyecto

Dentro de los resultados de las cincuenta (50) MIPYMES encuestadas se evidencia la prevalencia de las empresas del sector comercial, seguidas por el sector servicios y finalmente industrial.

Conociendo las ventajas de la implementación de las TIC, se busca determinar si las MIPYMES hacían uso de equipos de cómputo en el desarrollo de sus procesos internos y externos para el cumplimiento de sus diferentes actividades.

Gráfico 2 Porcentaje de uso de equipos de cómputo en los procesos de las mipymes encuestadas

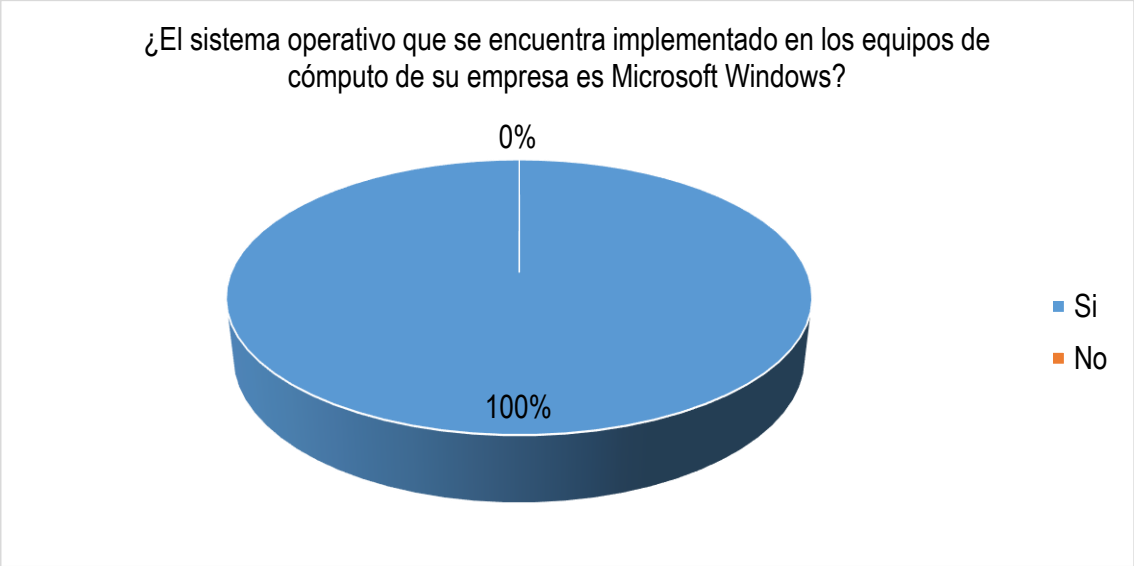


Fuente: Autores del proyecto

El uso de equipos de cómputo constituye el contexto apropiado para el desarrollo de la implementación de las firmas digitales y demás mecanismos de seguridad que permitan proteger los activos de información.

Teniendo como punto de partida el uso de equipos de cómputo en el desarrollo de las actividades de las MIPYMES, se buscó evaluar que en dichos equipos estuviera implementado el sistema operativo Microsoft Windows, debido a que las entidades de certificación ofrecen sus herramientas para realizar la firma digital para esta familia de sistemas operativos.

Gráfico 3 Porcentaje de las mipymes que poseen implementado el sistema operativo microsoft windows

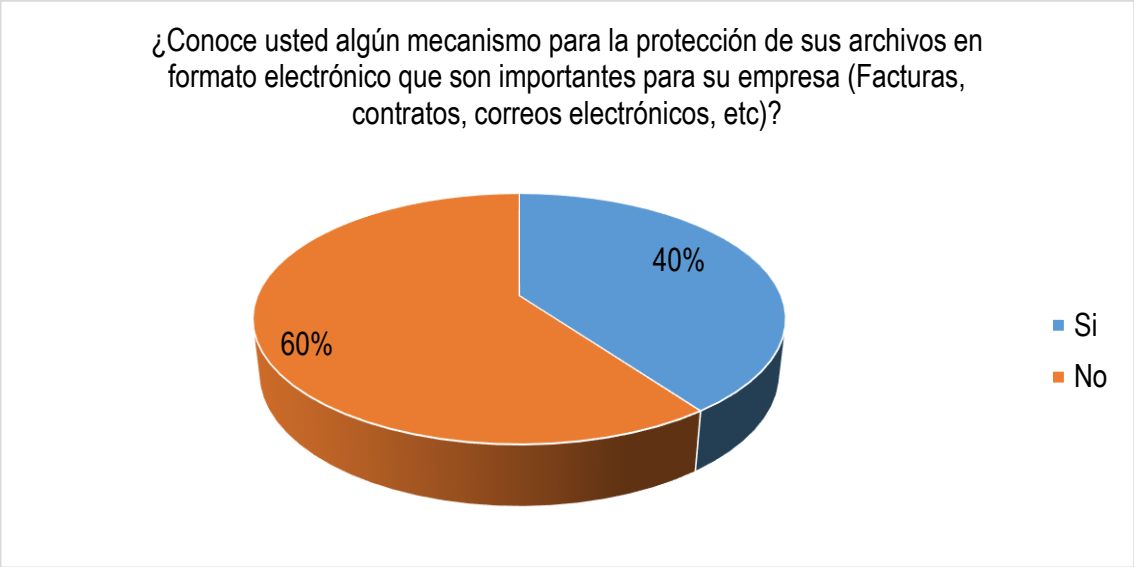


Fuente: Autores del proyecto

Se puede observar que la todas las MIPYMES encuestadas manejan el Sistema Operativo Microsoft Windows en sus equipos de cómputo, cumpliendo con los requerimientos técnicos mínimos para instalación de las diferentes herramientas de software proveídas por las entidades de certificación.

Basados en la importancia de conocer e implementar mecanismos de seguridad que permitan reducir el nivel de exposición al riesgo de los ecosistemas digitales, se busca determinar si los empresarios de las MIPYMES conocen algún mecanismo para la protección de los archivos en formato electrónico que sean importantes para sus empresas.

Gráfico 4 Porcentaje de conocimiento de mecanismos de protección de archivos en formato electrónico

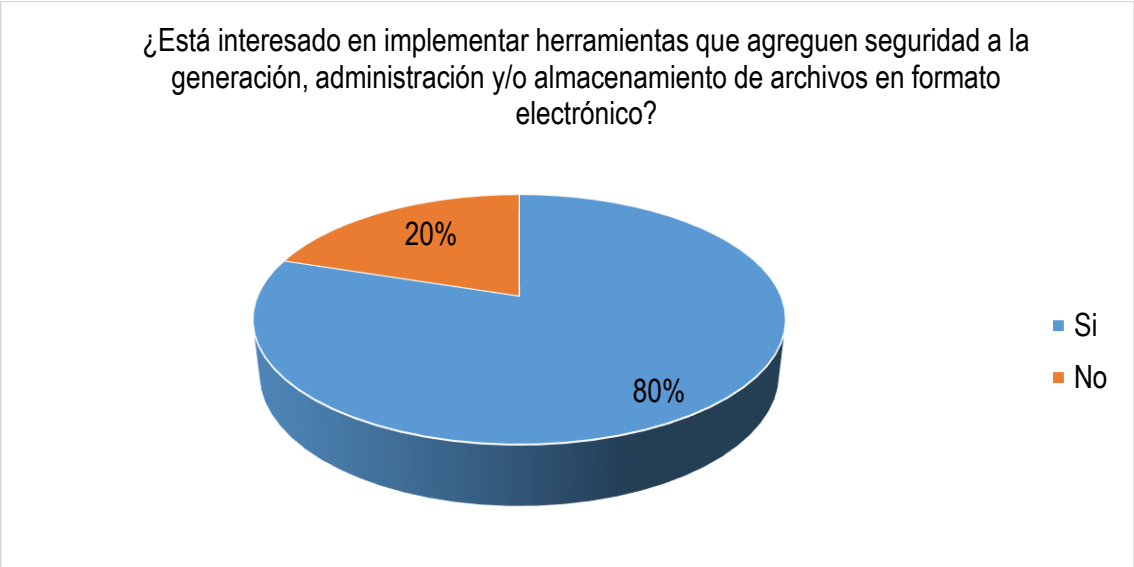


Fuente: Autores del proyecto

Se pudo observar que el 60 % de los empresarios respondieron que si conocen algún mecanismo de protección, al preguntarles sobre el mecanismo nos comunicaron, por ejemplo, el uso de antivirus, asignar contraseña a los archivos o realizar copias de seguridad de los mismos.

Se busca determinar si las MIPYMES estaban interesadas en implementar herramientas, específicamente mecanismos criptográficos, que agreguen seguridad a la generación, administración y/o almacenamiento de archivos en formato electrónico

Gráfico 5 Porcentaje de interés de las mipymes para la implementación de herramientas que agreguen seguridad a los archivos en formato electrónico

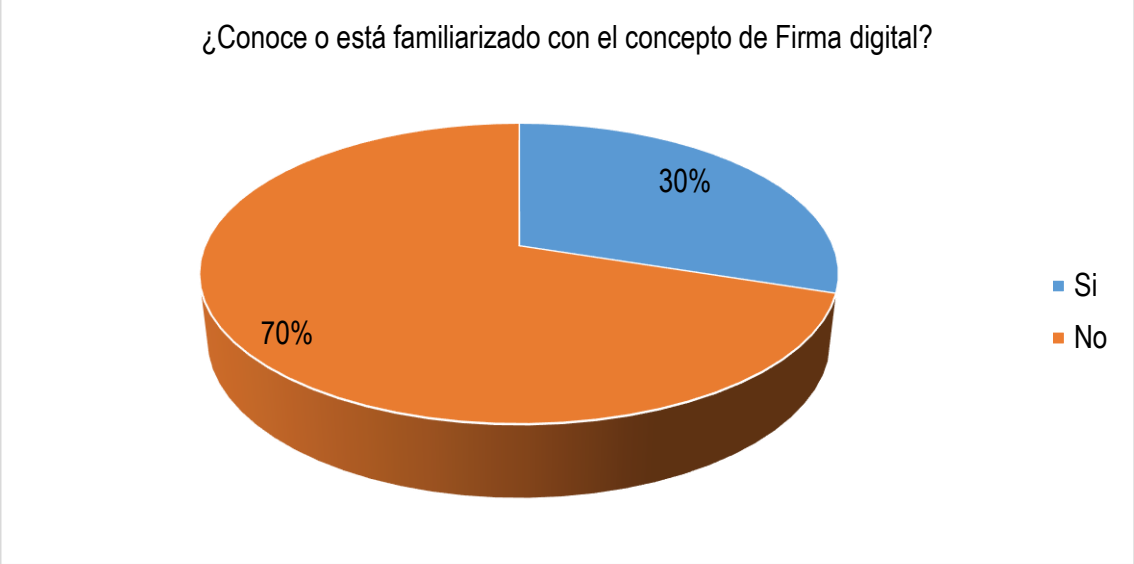


Fuente: Autores del proyecto

Las empresas encuestadas son conscientes de la necesidad de implementar mecanismos de seguridad en sus archivos en formato electrónico, lo anterior se evidencia en el 80 % de las empresas encuestadas las cuales muestran tener interés de realizar dicha implementación, se manifiesta que por de falta de conocimiento y pensando en los altos costos no se habían interesado.

Con el objetivo de ahondar más en el objetivo de la encuesta de diagnóstico, se busca determinar si los empresarios de las MIPYMES conocían o estaban familiarizados con el concepto de firma digital.

Gráfico 6 Porcentaje de conocimiento del concepto de firma digital por parte de los empresarios de las mipymes

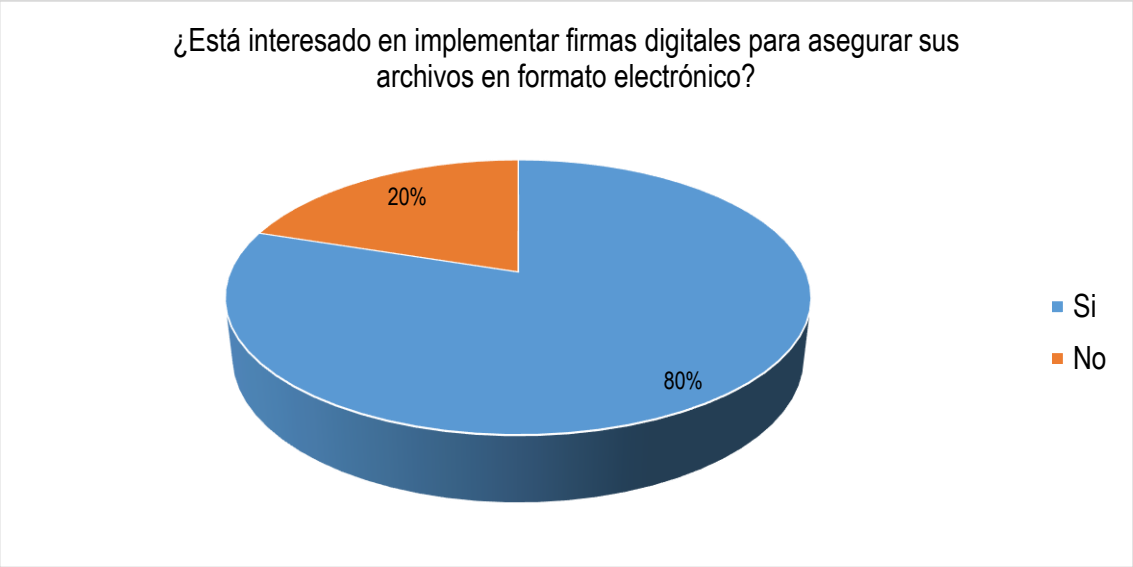


Fuente: Autores del proyecto

El 70 % de las empresas encuestadas respondieron no estar familiarizadas con el concepto de firma digital, el 30 % restante manifestó si están familiarizadas con el concepto de firma digital, por los procesos que realizan con la aplicación MUISCA de la DIAN, pero no tienen claro su funcionamiento y aplicabilidad a las actividades de su empresa.

Se procedió a suministrar un concepto básico y aplicaciones de la implementación del mecanismo de firma digital, con lo cual se busca determinar si los empresarios de las MIPYMES están interesados en explotar dichas aplicaciones mediante la implementación de firmas digitales para asegurar sus archivos en formato electrónico.

Gráfico 7 Porcentaje de interés de los empresarios de las mipymes de implementar firmas digitales



Fuente: Autores del proyecto

Al suministrar el concepto y aplicaciones de la firma digital el 80 % de las empresas encuestadas manifestaron estar interesadas en realizar la implementación de firmas digitales como mecanismo criptográfico para la protección de sus archivos en formato electrónico.

Finalmente se busca determinar si los empresarios de las MIPYMES estaban interesados en recibir una asesoría por parte de los autores del proyecto, donde se realizaría la explicación de los conceptos básicos de la firma digital, su validez funcional y probatoria, suministro de herramientas (Software) necesarias para realizar el proceso de firma digital y entrega del documento guía que contiene los procedimientos de solicitud, generación, instalación de los certificados de firma digital, procesos de firma, marco legal, actos administrativos que soportan dicho mecanismo de seguridad y establecen las entidades de certificación autorizadas para tal fin respectivamente.

Gráfico 8 Porcentaje de empresarios de las mipymes interesados en recibir una asesoría para la implementación del mecanismo de seguridad de la firma digital

Fuente: Autores del proyecto

Se observa el gran interés por usar la firma digital como mecanismo criptográfico por todas las empresas encuestadas al responder el 100 % que si estaban dispuestas a recibir una asesoría personalizada que permita la implementación en sus actividades diarias.

13.3. IMPLEMENTACIÓN EN EL SECTOR SERVICIOS

13.3.1. Datos de las encuestas del sector servicios

Cuadro 3 Resultados obtenidos en las encuestas de diagnóstico aplicadas a las mipymes del sector servicios

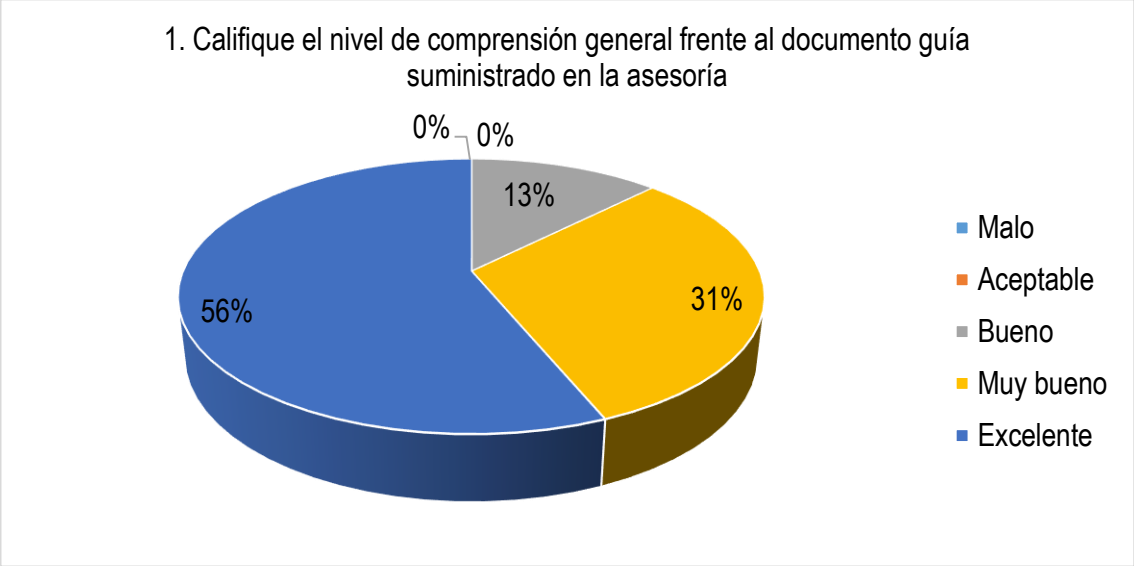
Pregunta	M*	A*	B*	MB*	E*
1) Califique el nivel de comprensión general frente al documento guía suministrado en la asesoría	0	0	2	5	9
2) Califique el tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación de certificado de firma digital	0	0	6	6	4
3) Califique el nivel de comprensión del proceso de instalación del certificado de firma digital	0	0	3	10	3
4) Califique la facilidad de uso de la herramienta "CertiFirma" para el proceso de firma digital	0	5	8	2	1
5) Califique la facilidad de uso de la herramienta "XolidoSign" para el proceso de firma digital	0	0	0	11	5
6) Califique la facilidad de uso de la herramienta "Andes Signer" para el proceso de firma digital	0	12	3	1	0
7) Califique en términos generales el tiempo que le tomo ejecutar el proceso de firma digital con archivos electrónicos necesarios en las diferentes actividades de su empresa	0	0	3	3	10
8) Califique el impacto de la implementación del mecanismo de firma digital a los archivos electrónicos en las diferentes actividades de su empresa	0	0	0	6	10

* M = Malo; A = Aceptable; B = Bueno; MB = Muy Bueno; E = Excelente

Fuente: Autores del proyecto

13.3.2. Análisis de los datos del sector servicios. Se busca que los empresarios de las MIPYMES del sector servicios califiquen en términos generales el nivel de comprensión frente al documento guía suministrado en la asesoría recibida posterior a la encuesta de diagnóstico.

Gráfico 9 Porcentaje del nivel de comprensión del documento guía en las empresas del sector servicios

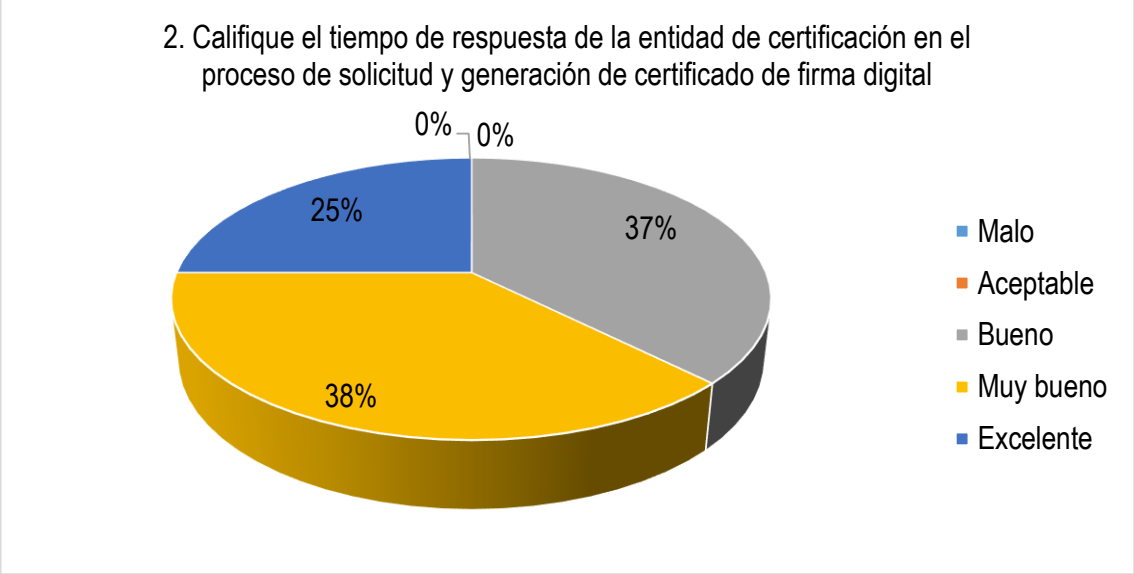


Fuente: Autores del proyecto

Se observa un alto grado de aceptación de la guía dada en la asesoría debido al evidenciar que el 87 % de las empresas encuestadas califica el nivel de comprensión de la guía como Excelente o Muy bueno debido a su contenido fácil de asimilar con el paso a paso de los procesos de obtención del certificado de firma digital y la forma de usar correctamente las aplicaciones de firmado como son Certifirma, XolidoSign, Andes Signer.

El elemento central para el desarrollo del documento guía por parte de los empresarios de las MIPYMES es el certificado de firma digital, debido a su importancia se busca que se califique el tiempo de respuesta de la entidad de certificación digital en el proceso de solicitud y generación.

Gráfico 10. Porcentaje de calificación del tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación del certificado de firma digital en las empresas del sector servicios

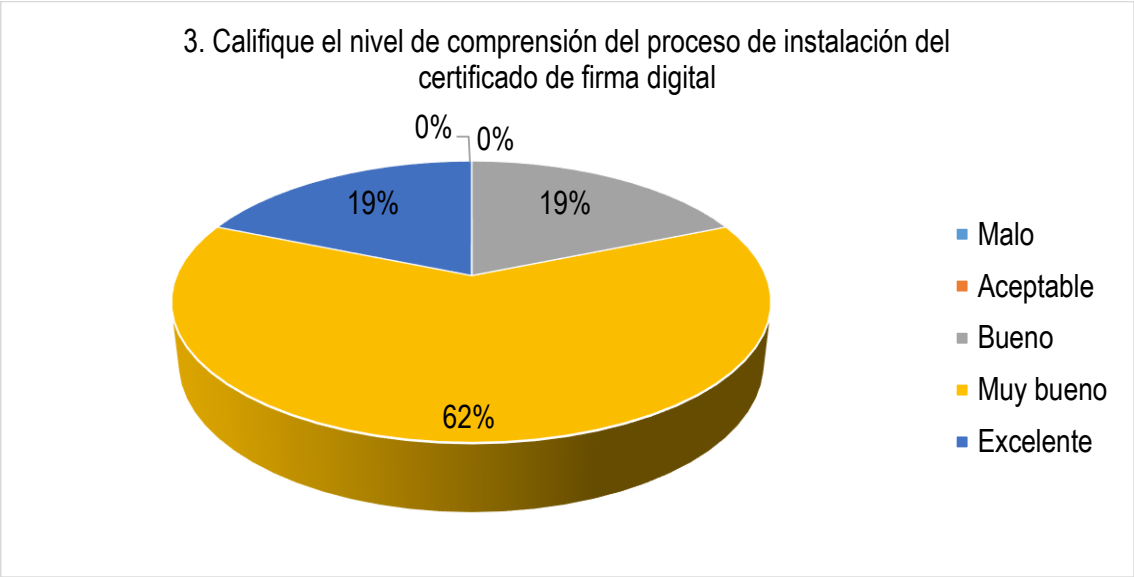


Fuente: Autores del proyecto

El tiempo estimado entre la obtención y la generación del certificado de firma digital por parte de la entidad de certificación está dentro del rango viable para el proceso según las empresas encuestadas, al responder el 63 % de las empresas que el tiempo de respuesta se encuentra entre excelente y muy bueno, otro 37 % califica el tiempo de respuesta como bueno, además que el proceso es fácil de realizar y se envían mensajes de correo electrónico con el estado del trámite e información de soporte.

Una vez determinada la percepción de los tiempos de respuesta de la entidad de certificación, se busca medir el nivel de comprensión por parte de los empresarios de las MIPYMES del proceso de instalación del certificado de firma digital tramitado ante la correspondiente entidad, lo anterior detallado en el documento guía suministrado en la asesoría.

Gráfico 11 Porcentaje del nivel de comprensión del proceso de instalación del certificado de firma digital en las empresas del sector servicios

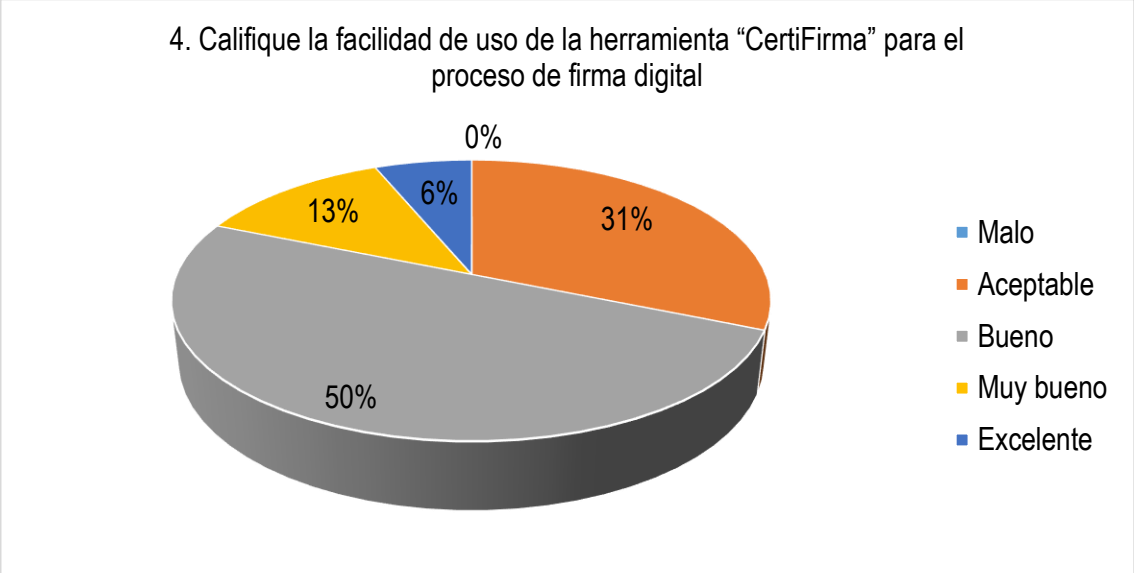


Fuente: Autores del proyecto

Se observa que el proceso detallado en la guía para la instalación del certificado está escrito de una forma muy clara, lo que permite con facilidad cumplir con el ejercicio y realizarlo de una forma rápida siguiendo el paso a paso descrito en el documento, lo anterior basado en la calificación dada por las empresas de las cuales el 81 % considera que el nivel de comprensión es excelente y muy bueno, otro 19 % manifiesta que el nivel de comprensión de la guía es bueno.

Complementario al certificado de firma digital, las herramientas (software) suministradas por las entidades de certificación digital forman parte fundamental del proceso y afectan el impacto y la satisfacción de la implementación de este mecanismo de seguridad, por lo anterior se buscó determinar la facilidad de uso de las herramientas propuestas en el documento guía (CertiFirma, XolidoSign, Andes Signer) por parte de los empresarios de las MIPYMES.

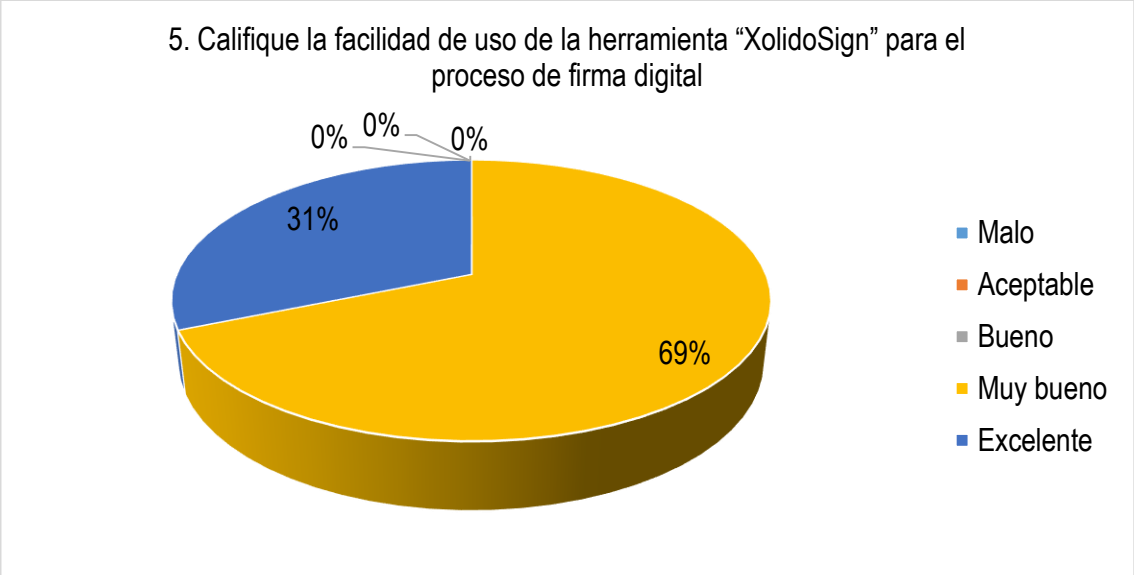
Gráfico 12 Porcentaje del nivel de facilidad de uso de la herramienta certifirma en las empresas del sector servicios



Fuente: Autores del proyecto

Se observa que por su funcionamiento la herramienta CertiFirma no generó gran interés a los empresarios encuestados, los cuales manifestaron que la herramienta empaqueta el archivo firmado con la firma, se requiere desempaquetar el contenido para poder visualizar el archivo firmado digitalmente lo que representa más tiempo para la ejecución de los diferentes procesos de la firma digital como el firmado y la validación.

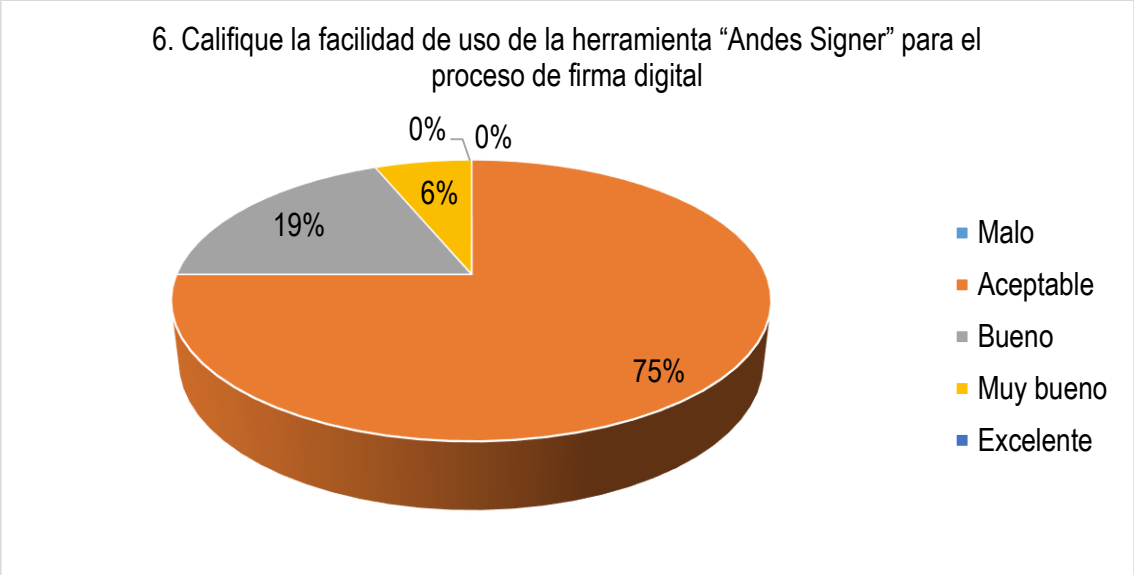
Gráfico 13 Porcentaje del nivel de facilidad de uso de la herramienta xolidosign en las empresas del sector servicios



Fuente: Autores del proyecto

Se observa que por su interfaz agradable y las opciones que ofrece la aplicación generó gran interés a las empresas encuestadas, se manifestó gran facilidad comparada con la herramienta CertiFirma debido a que XolidoSign genera un archivo complementario al archivo firmado digitalmente, por lo que no se lleva a cabo un proceso de empaquetado o desempaquetado, facilita las ejecución de los diferentes procesos de la firma digital como el firmado y la validación. Esta herramienta ofrece un servicio adicional de estampa de tiempo lo que atrajo la atención y preferencia de los empresarios.

Gráfico 14 Porcentaje del nivel de facilidad de uso de la herramienta andes signer en las empresas del sector servicios

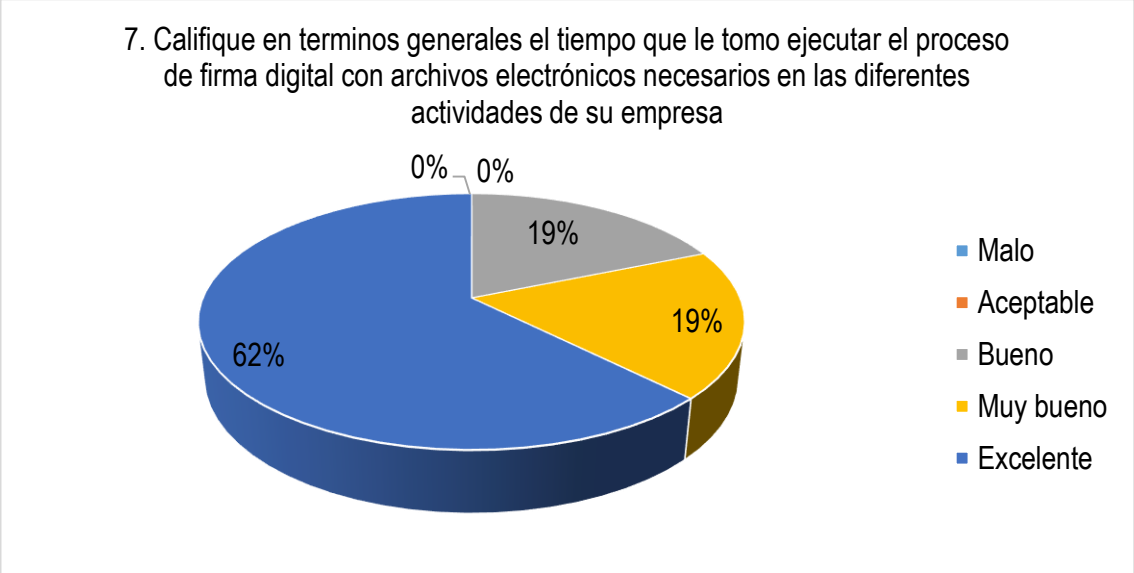


Fuente: Autores del proyecto

Se observa que por su interfaz demasiado simple la aplicación no generó gran interés a los empresarios encuestados, se manifestó que la ejecución de procesos de firma y validación eran confusos y no se sentían cómodos al intentar desarrollar sus actividades diarias.

Adicionalmente se buscó calificar en términos generales el tiempo que le tomo a los empresarios de las MIPYMES ejecutar el proceso de firma digital en las diferentes actividades de su empresa y finalmente calificar la percepción del impacto de la implementación del mecanismo de seguridad de firma digital en las actividades de su empresa.

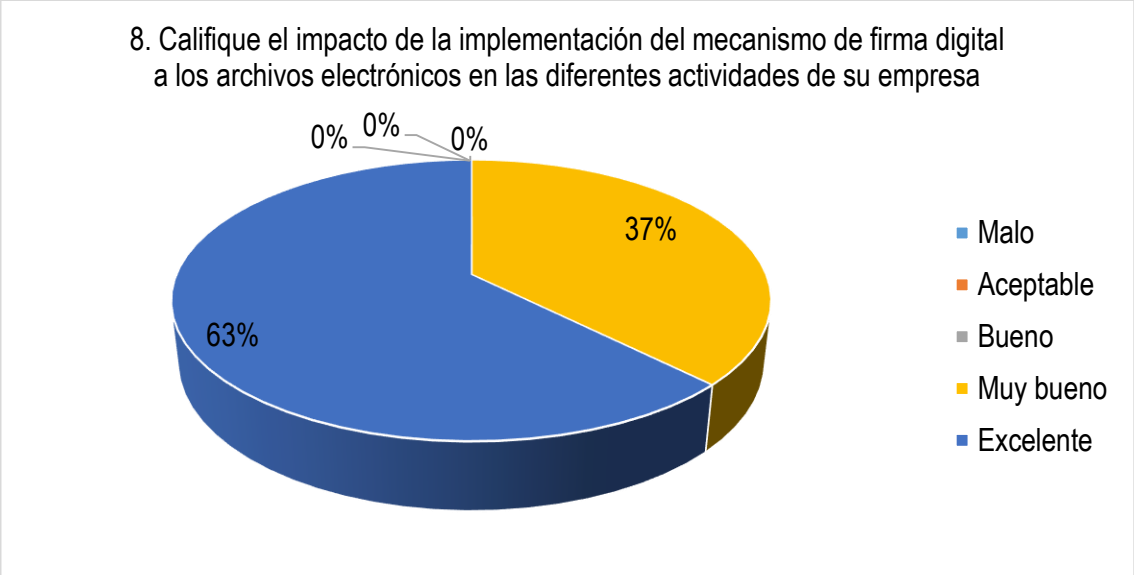
Gráfico 15 Porcentaje de calificación del tiempo de ejecución del proceso de firma digital en el desarrollo de las actividades de las empresas del sector servicios



Fuente: Autores del proyecto

Se observa gran satisfacción en el tiempo que se lleva realizar el proceso de firma digital con los archivos en formato electrónico, el 81 % de las empresas califico como excelente o muy bueno el tiempo que tomo ejecutar el procedimiento, otro 19 % lo califico como bueno.

Gráfico 16 Porcentaje de calificación del impacto de la implementación del mecanismo de firma digital en el desarrollo de las actividades de las empresas del sector servicios



Fuente: Autores del proyecto

Se observa un alto grado de aceptación y satisfacción por parte de las empresas encuestadas en la implementación del mecanismo de firma digital y la importancia de su uso en sus actividades diarias.

13.4. IMPLEMENTACIÓN EN EL SECTOR INDUSTRIAL

13.4.1. Datos de las encuestas del sector industrial

Cuadro 4 Resultados obtenidos en las encuestas de diagnóstico aplicadas a las mipymes del sector industrial

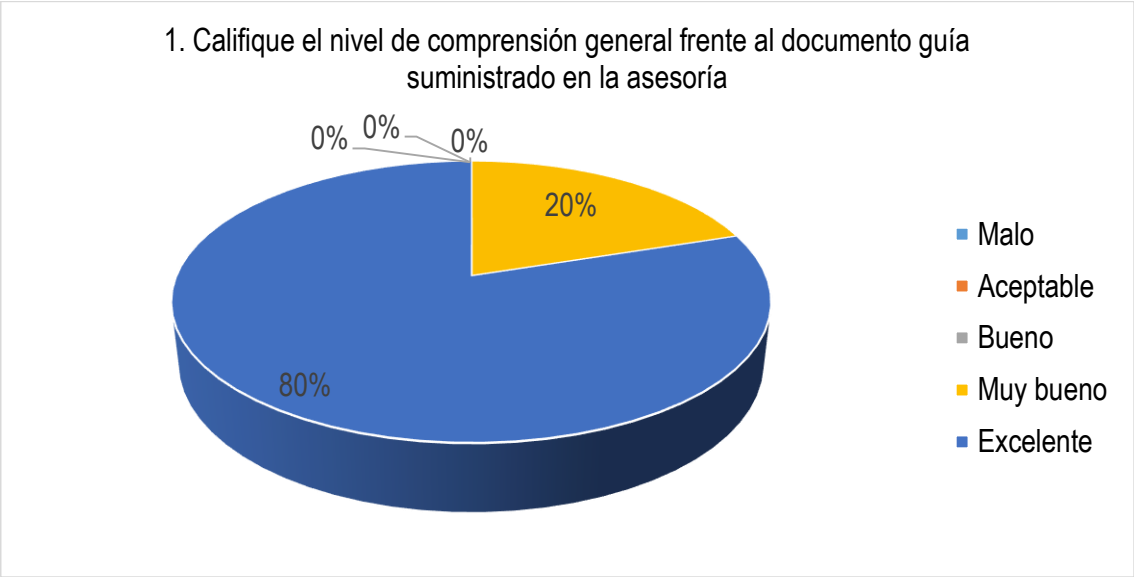
Pregunta	M*	A*	B*	MB*	E*
1) Califique el nivel de comprensión general frente al documento guía suministrado en la asesoría	0	0	0	1	4
2) Califique el tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación de certificado de firma digital	0	0	1	3	1
3) Califique el nivel de comprensión del proceso de instalación del certificado de firma digital	0	0	0	2	3
4) Califique la facilidad de uso de la herramienta “CertiFirma” para el proceso de firma digital	0	1	3	1	0
5) Califique la facilidad de uso de la herramienta “XolidoSign” para el proceso de firma digital	0	0	0	1	4
6) Califique la facilidad de uso de la herramienta “Andes Signer” para el proceso de firma digital	1	3	1	0	0
7) Califique en términos generales el tiempo que le tomo ejecutar el proceso de firma digital con archivos electrónicos necesarios en las diferentes actividades de su empresa	0	0	1	1	3
8) Califique el impacto de la implementación del mecanismo de firma digital a los archivos electrónicos en las diferentes actividades de su empresa	0	0	0	1	4

* M = Malo; A = Aceptable; B = Bueno; MB = Muy Bueno; E = Excelente

Fuente: Autores del proyecto

13.4.2. Análisis de los datos del sector industrial. Se busca que los empresarios de las MIPYMES del sector industrial califiquen en términos generales el nivel de comprensión frente al documento guía suministrado en la asesoría recibida posterior a la encuesta de diagnóstico.

Gráfico 17 Porcentaje del nivel de comprensión del documento guía en las empresas del sector industrial

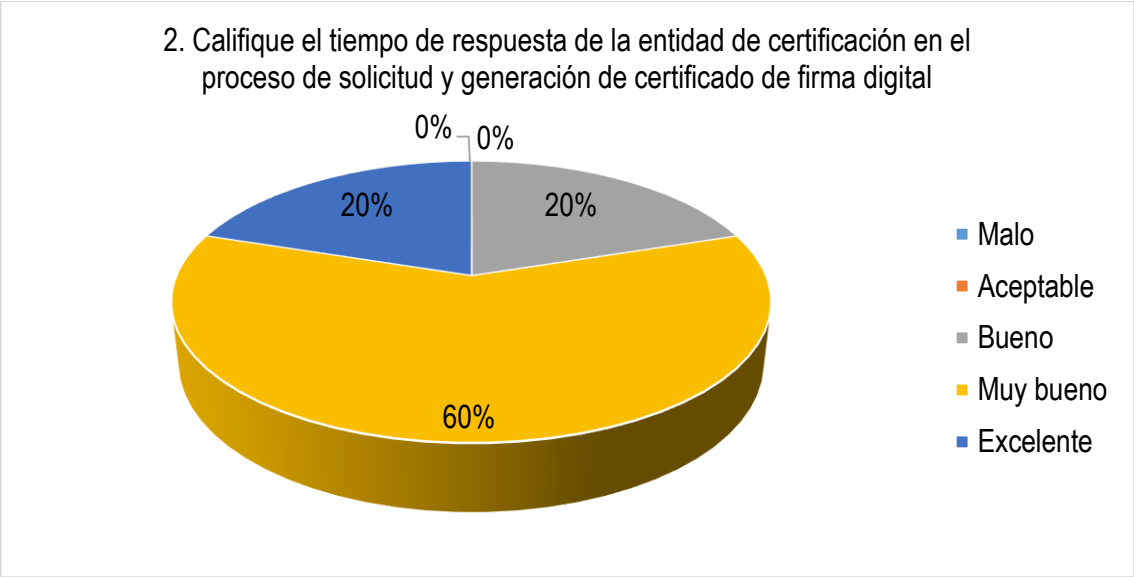


Fuente: Autores del proyecto

Se observa un alto grado de aceptación de la guía dada en la asesoría debido al evidenciar que el 80 % de las empresas encuestadas califica el nivel de comprensión de la guía como Excelente debido a su contenido fácil de asimilar con el paso a paso de los procesos de obtención del certificado de firma digital y la forma de usar correctamente las aplicaciones de firmado como son Certifirma, XolidoSign, Andes Signer.

El elemento central para el desarrollo del documento guía por parte de los empresarios de las MIPYMES es el certificado de firma digital, debido a su importancia se busca que se califique el tiempo de respuesta de la entidad de certificación digital en el proceso de solicitud y generación.

Gráfico 18 Porcentaje de calificación del tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación del certificado de firma digital en las empresas del sector industrial

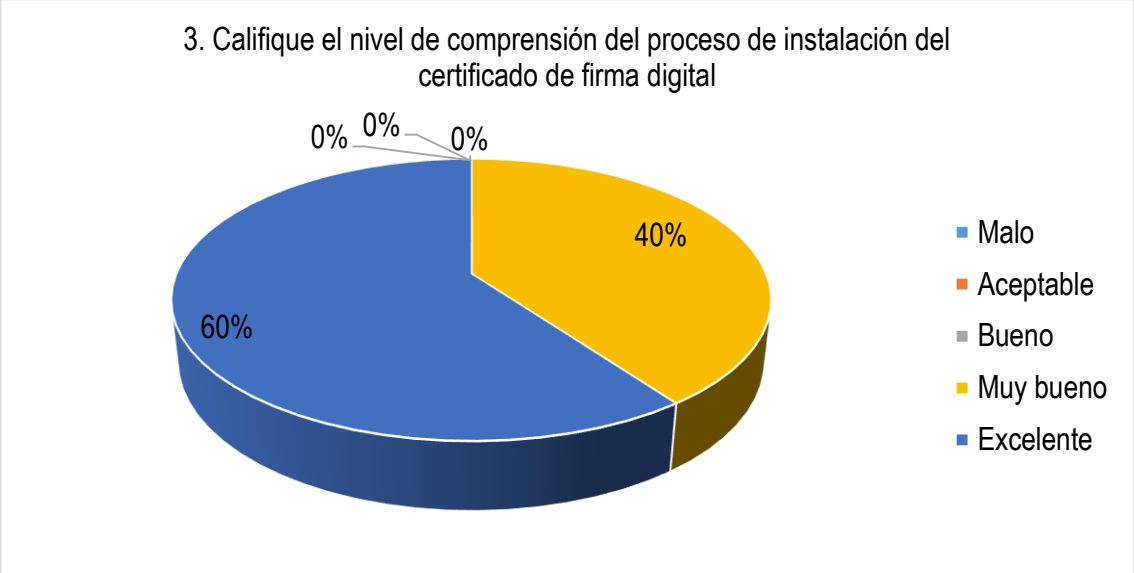


Fuente: Autores del proyecto

El tiempo estimado entre la obtención y la generación del certificado de firma digital por parte de la entidad de certificación está dentro del rango viable para el proceso según las empresas encuestadas, al responder el 80 % de las empresas que el tiempo de respuesta se encuentra entre excelente y muy bueno, otro 20 % califica el tiempo de respuesta como bueno, además que el proceso es fácil de realizar y se envían mensajes de correo electrónico con el estado del trámite e información de soporte.

Una vez determinada la percepción de los tiempos de respuesta de la entidad de certificación, se busca medir el nivel de comprensión por parte de los empresarios de las MIPYMES del proceso de instalación del certificado de firma digital tramitado ante la correspondiente entidad, lo anterior detallado en el documento guía suministrado en la asesoría.

Gráfico 19 Porcentaje del nivel de comprensión del proceso de instalación del certificado de firma digital en las empresas del sector industrial

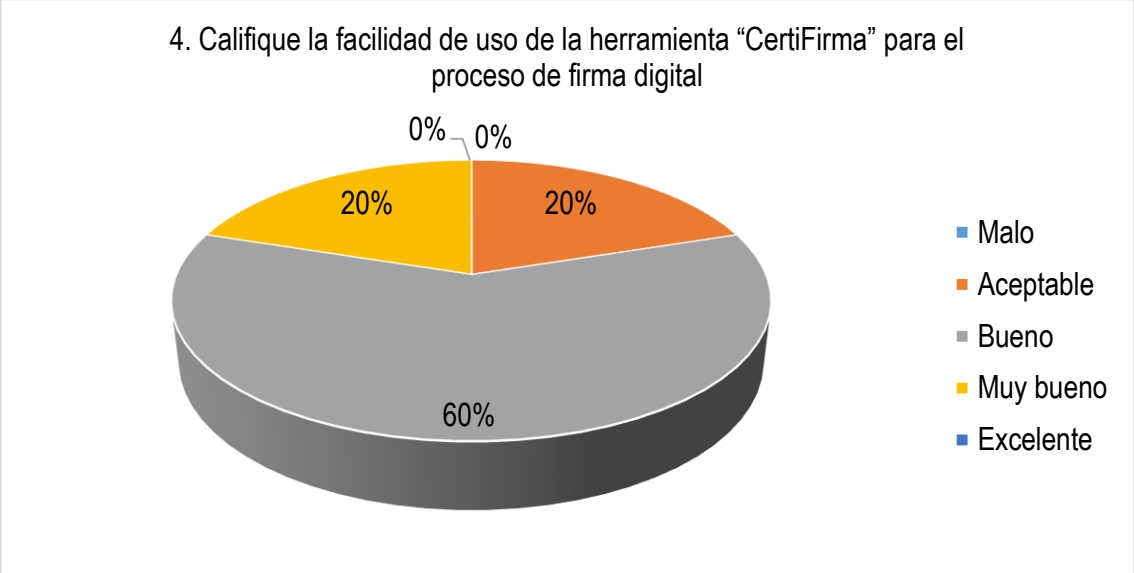


Fuente: Autores del proyecto

Se observa que el proceso detallado en la guía para la instalación del certificado está escrito de una forma muy clara, lo que permite con facilidad cumplir con el ejercicio y realizarlo de una forma rápida siguiendo el paso a paso descrito en el documento, lo anterior basado en la calificación dada por las empresas de las cuales el 60 % considera que el nivel de comprensión es excelente, otro 40 % manifiesta que el nivel de comprensión de la guía es muy bueno.

Complementario al certificado de firma digital, las herramientas (software) suministradas por las entidades de certificación digital forman parte fundamental del proceso y afectan el impacto y la satisfacción de la implementación de este mecanismo de seguridad, por lo anterior se buscó determinar la facilidad de uso de las herramientas propuestas en el documento guía (CertiFirma, XolidoSign, Andes Signer) por parte de los empresarios de las MIPYMES.

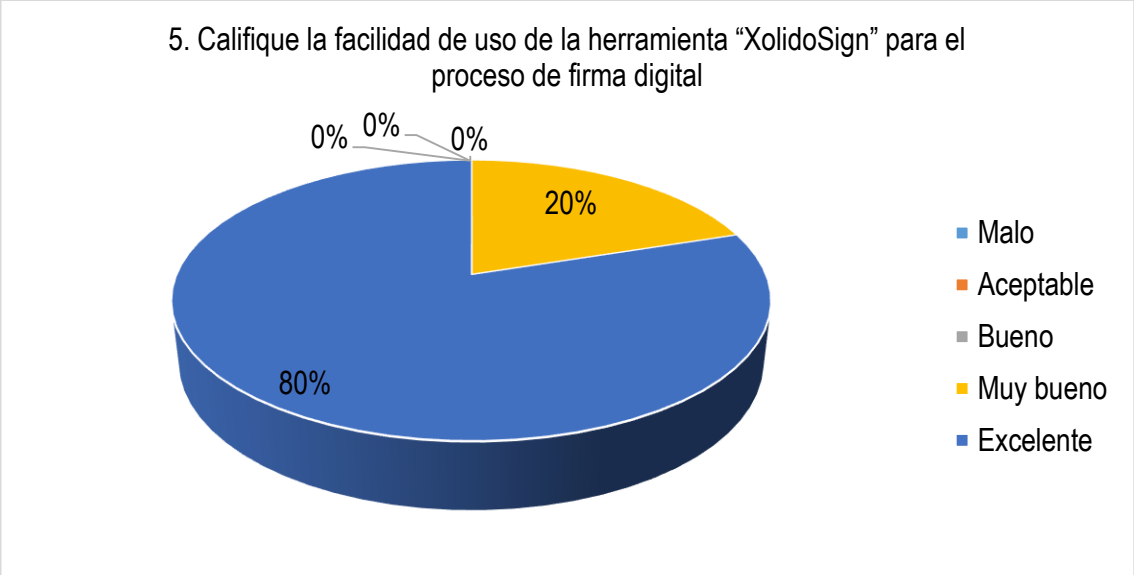
Gráfico 20 Porcentaje del nivel de facilidad de uso de la herramienta certifirma en las empresas del sector industrial



Fuente: Autores del proyecto

Se observa que por su funcionamiento la herramienta CertiFirma no generó gran interés a los empresarios encuestados, los cuales manifestaron que la herramienta empaqueta el archivo firmado con la firma, se requiere desempaquetar el contenido para poder visualizar el archivo firmado digitalmente lo que representa más tiempo para la ejecución de los diferentes procesos de la firma digital como el firmado y la validación.

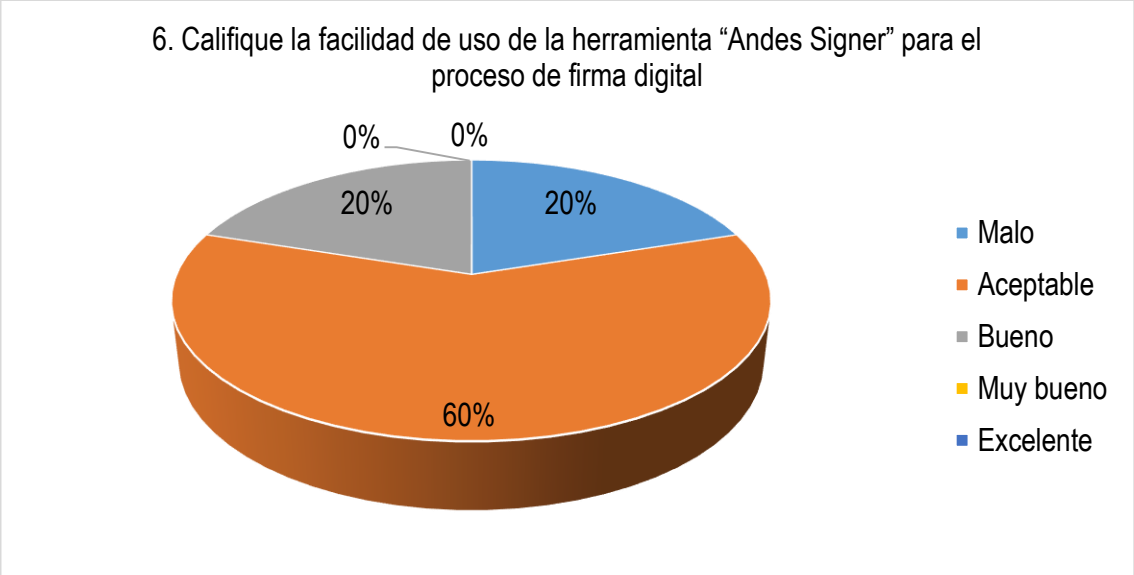
Gráfico 21 Porcentaje del nivel de facilidad de uso de la herramienta xolidosign en las empresas del sector industrial



Fuente: Autores del proyecto

Se observa que por su interfaz agradable y las opciones que ofrece la aplicación generó gran interés a las empresas encuestadas, se manifestó gran facilidad comparada con la herramienta CertiFirma debido a que XolidoSign genera un archivo complementario al archivo firmado digitalmente, por lo que no se lleva a cabo un proceso de empaquetado o desempaquetado, facilita las ejecución de los diferentes procesos de la firma digital como el firmado y la validación. Esta herramienta ofrece un servicio adicional de estampa de tiempo lo que atrajo la atención y preferencia de los empresarios

Gráfico 22 Porcentaje del nivel de facilidad de uso de la herramienta andes signer en las empresas del sector industrial

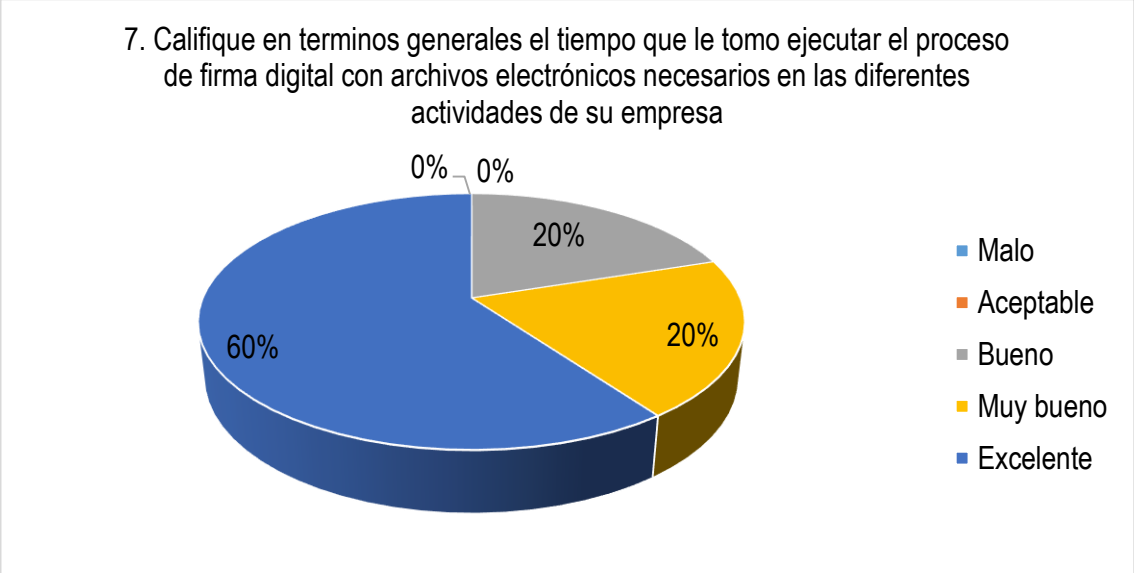


Fuente: Autores del proyecto

Se observa que por su interfaz demasiado simple la aplicación no generó gran interés a los empresarios encuestados, se manifestó que la ejecución de procesos de firma y validación eran confusos y no se sentían cómodos al intentar desarrollar sus actividades diarias.

Adicionalmente se buscó calificar en términos generales el tiempo que le tomo a los empresarios de las MIPYMES ejecutar el proceso de firma digital en las diferentes actividades de su empresa y finalmente calificar la percepción del impacto de la implementación del mecanismo de seguridad de firma digital en las actividades de su empresa.

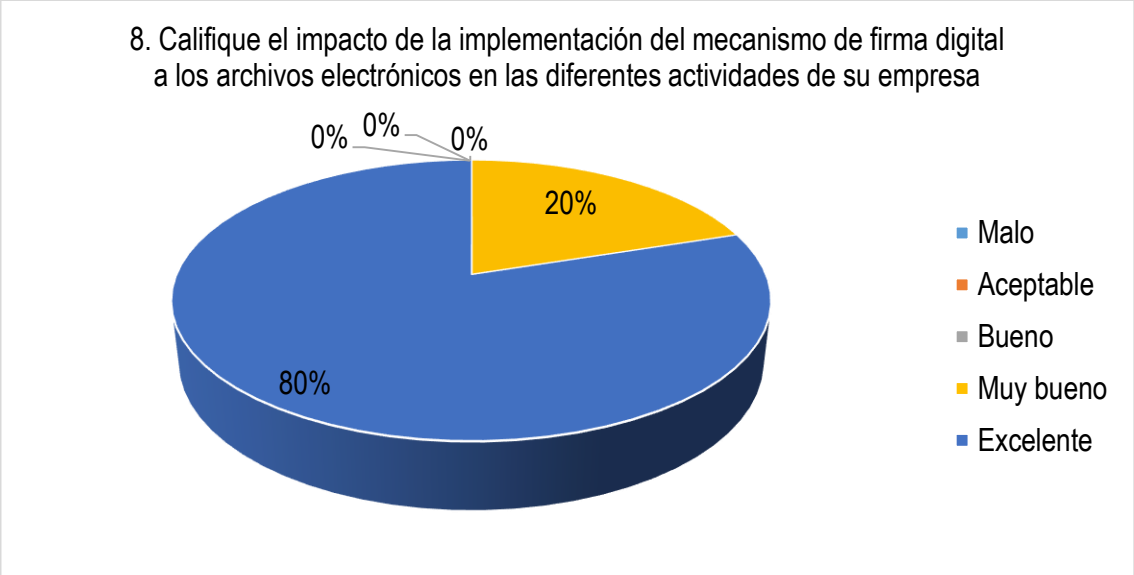
Gráfico 23 Porcentaje de calificación del tiempo de ejecución del proceso de firma digital en el desarrollo de las actividades de las empresas del sector industrial



Fuente: Autores del proyecto

Se observa gran satisfacción en el tiempo que se lleva realizar el proceso de firma digital con los archivos en formato electrónico, el 80 % de las empresas califico como excelente o muy bueno el tiempo que tomo ejecutar el procedimiento, otro 20 % lo califico como bueno.

Gráfico 24 Porcentaje de calificación del impacto de la implementación del mecanismo de firma digital en el desarrollo de las actividades de las empresas del sector industrial



Fuente: Autores del proyecto

Se observa un alto grado de aceptación y satisfacción por parte de las empresas encuestadas en la implementación del mecanismo de firma digital y la importancia de su uso en sus actividades diarias.

13.5. IMPLEMENTACIÓN EN EL SECTOR COMERCIAL

13.5.1. Datos de las encuestas del sector comercial

Cuadro 5 Resultados obtenidos en las encuestas de diagnóstico aplicadas a las mipymes del sector comercial

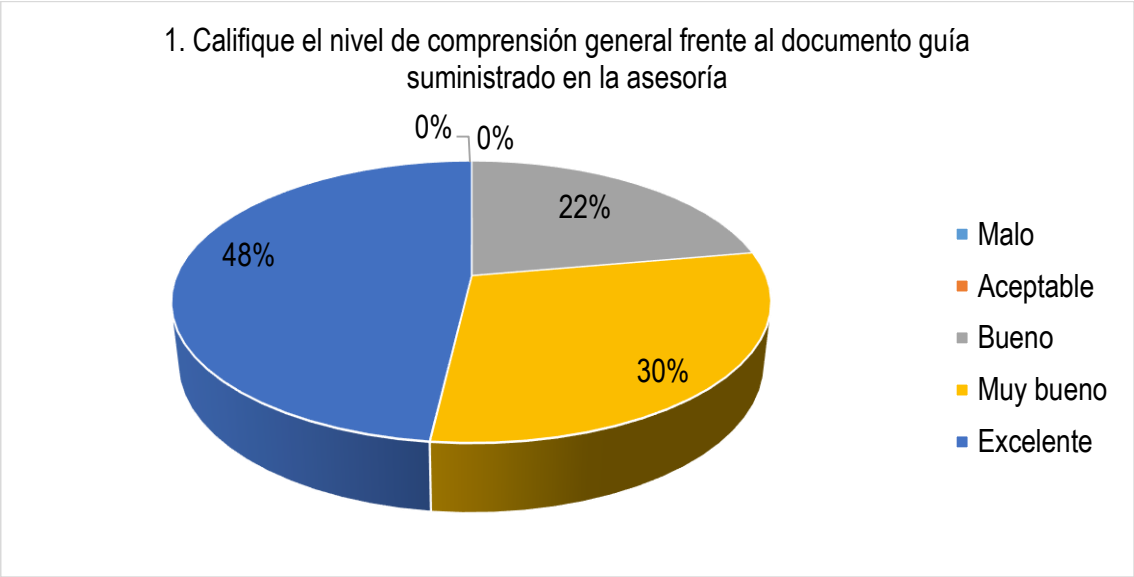
Pregunta	M*	A*	B*	MB*	E*
1) Califique el nivel de comprensión general frente al documento guía suministrado en la asesoría	0	0	6	8	13
2) Califique el tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación de certificado de firma digital	0	0	17	7	3
3) Califique el nivel de comprensión del proceso de instalación del certificado de firma digital	0	0	1	21	5
4) Califique la facilidad de uso de la herramienta “CertiFirma” para el proceso de firma digital	3	7	14	2	1
5) Califique la facilidad de uso de la herramienta “XolidoSign” para el proceso de firma digital	0	0	3	3	21
6) Califique la facilidad de uso de la herramienta “Andes Signer” para el proceso de firma digital	9	15	2	1	0
7) Califique en términos generales el tiempo que le tomo ejecutar el proceso de firma digital con archivos electrónicos necesarios en las diferentes actividades de su empresa	0	0	7	8	12
8) Califique el impacto de la implementación del mecanismo de firma digital a los archivos electrónicos en las diferentes actividades de su empresa	0	0	0	4	23

* M = Malo; A = Aceptable; B = Bueno; MB = Muy Bueno; E = Excelente

Fuente: Autores del proyecto

13.5.2. Análisis de los datos del sector comercial. Se busca que los empresarios de las MIPYMES del sector servicios califiquen en términos generales el nivel de comprensión frente al documento guía suministrado en la asesoría recibida posterior a la encuesta de diagnóstico.

Gráfico 25 Porcentaje del nivel de comprensión del documento guía en las empresas del sector comercial

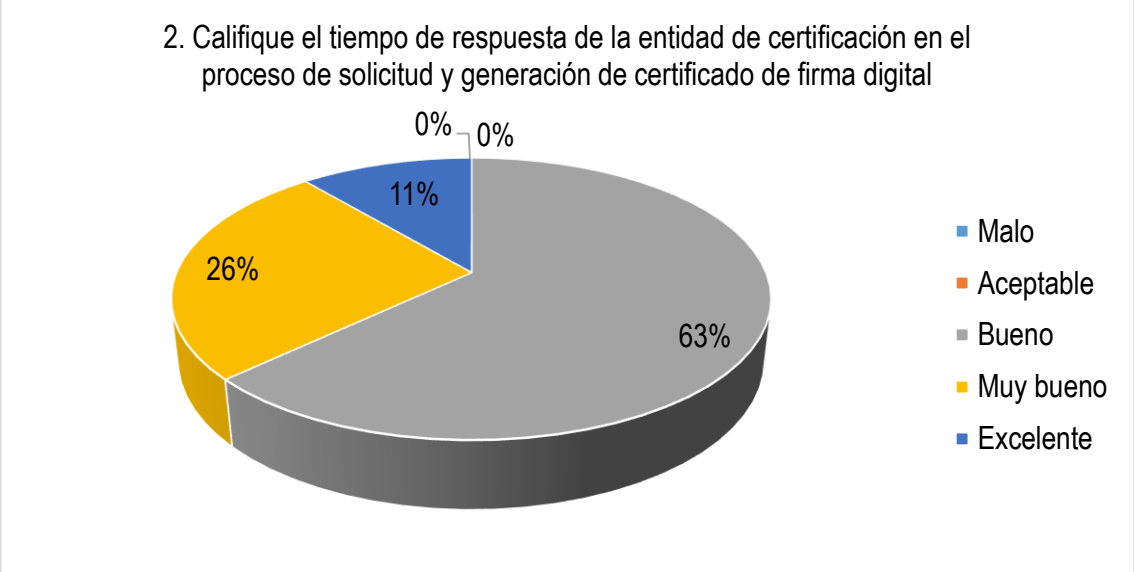


Fuente: Autores del proyecto

Se observa un alto grado de aceptación de la guía dada en la asesoría debido al evidenciar que el 78 % de las empresas encuestadas califica el nivel de comprensión de la guía como Excelente o Muy bueno debido a su contenido fácil de asimilar con el paso a paso de los procesos de obtención del certificado de firma digital y la forma de usar correctamente las aplicaciones de firmado como son Certifirma, XolidoSign, Andes Signer.

El elemento central para el desarrollo del documento guía por parte de los empresarios de las MIPYMES es el certificado de firma digital, debido a su importancia se busca que se califique el tiempo de respuesta de la entidad de certificación digital en el proceso de solicitud y generación.

Gráfico 26 Porcentaje de calificación del tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación del certificado de firma digital en las empresas del sector comercial

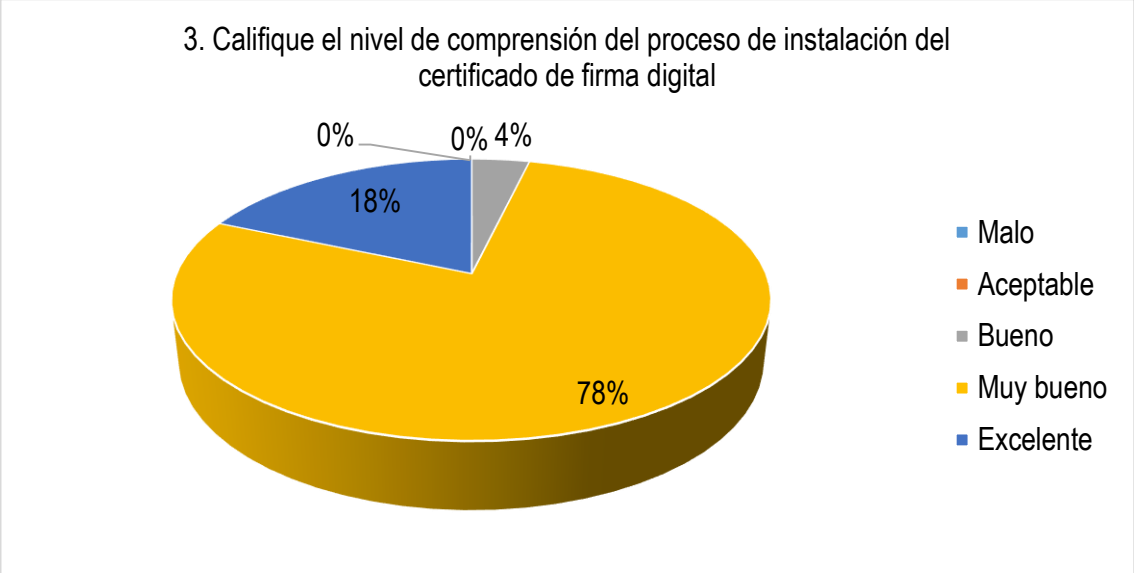


Fuente: Autores del proyecto

El tiempo estimado entre la obtención y la generación del certificado de firma digital por parte de la entidad de certificación está dentro del rango viable para el proceso según las empresas encuestadas, al responder el 37 % de las empresas que el tiempo de respuesta se encuentra entre excelente y muy bueno, otro 63 % califica el tiempo de respuesta como bueno, además que el proceso es fácil de realizar y se envían mensajes de correo electrónico con el estado del trámite e información de soporte.

Una vez determinada la percepción de los tiempos de respuesta de la entidad de certificación, se busca medir el nivel de comprensión por parte de los empresarios de las MIPYMES del proceso de instalación del certificado de firma digital tramitado ante la correspondiente entidad, lo anterior detallado en el documento guía suministrado en la asesoría.

Gráfico 27 Porcentaje del nivel de comprensión del proceso de instalación del certificado de firma digital en las empresas del sector comercial

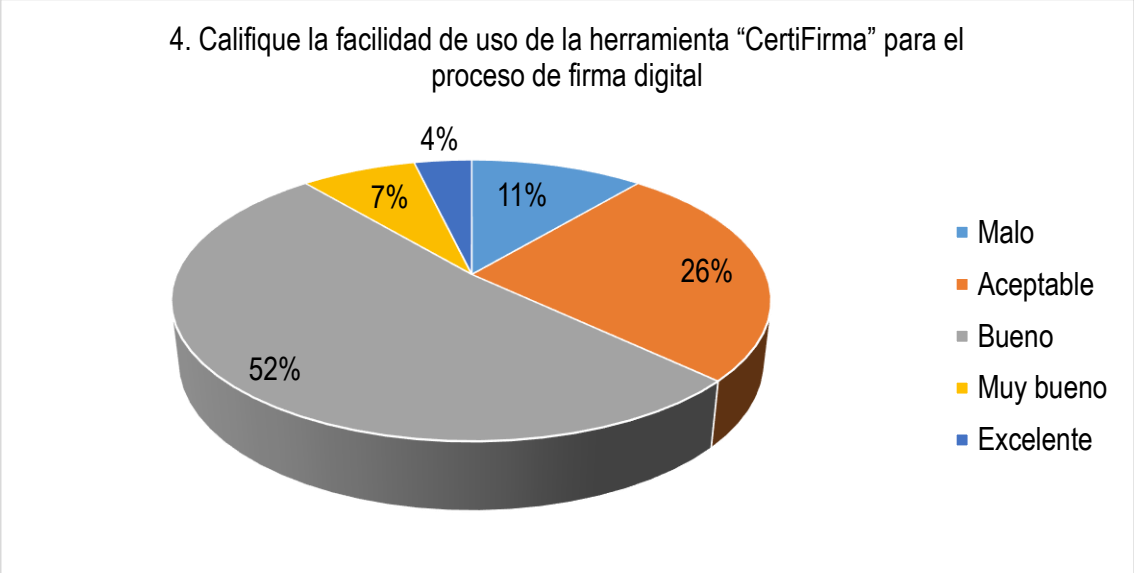


Fuente: Autores del proyecto

Se observa que el proceso detallado en la guía para la instalación del certificado está escrito de una forma muy clara, lo que permite con facilidad cumplir con el ejercicio y realizarlo de una forma rápida siguiendo el paso a paso descrito en el documento, lo anterior basado en la calificación dada por las empresas de las cuales el 96 % considera que el nivel de comprensión es excelente y muy bueno, otro 4 % manifiesta que el nivel de comprensión de la guía es bueno.

Complementario al certificado de firma digital, las herramientas (software) suministradas por las entidades de certificación digital forman parte fundamental del proceso y afectan el impacto y la satisfacción de la implementación de este mecanismo de seguridad, por lo anterior se buscó determinar la facilidad de uso de las herramientas propuestas en el documento guía (CertiFirma, XolidoSign, Andes Signer) por parte de los empresarios de las MIPYMES.

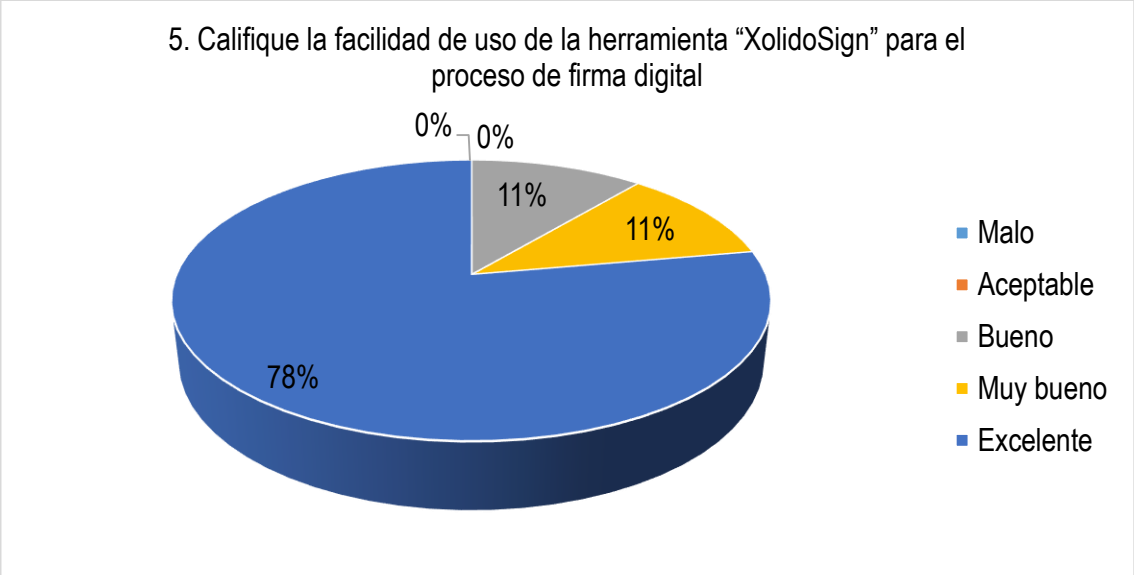
Gráfico 28 Porcentaje del nivel de facilidad de uso de la herramienta certifirma en las empresas del sector comercial



Fuente: Autores del proyecto

Se observa que por su funcionamiento la herramienta CertiFirma no generó gran interés a los empresarios encuestados, los cuales manifestaron que la herramienta empaqueta el archivo firmado con la firma, se requiere desempaquetar el contenido para poder visualizar el archivo firmado digitalmente lo que representa más tiempo para la ejecución de los diferentes procesos de la firma digital como el firmado y la validación.

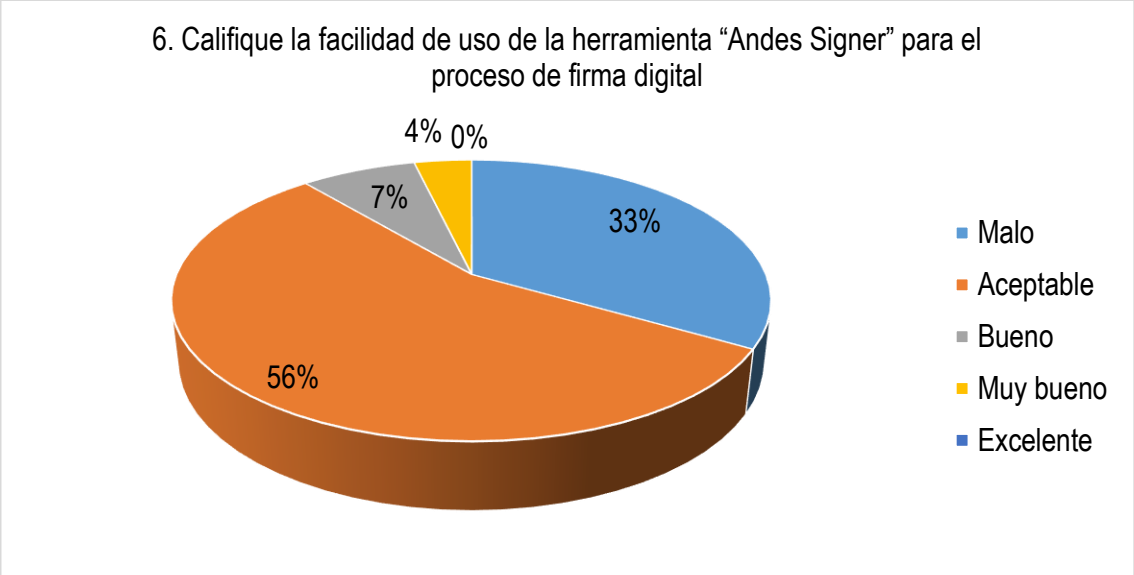
Gráfico 29 Porcentaje del nivel de facilidad de uso de la herramienta xolidosign en las empresas del sector comercial



Fuente: Autores del proyecto

Se observa que por su interfaz agradable y las opciones que ofrece la aplicación generó gran interés a las empresas encuestadas, se manifestó gran facilidad comparada con la herramienta CertiFirma debido a que XolidoSign genera un archivo complementario al archivo firmado digitalmente, por lo que no se lleva a cabo un proceso de empaquetado o desempaquetado, facilita las ejecución de los diferentes procesos de la firma digital como el firmado y la validación. Esta herramienta ofrece un servicio adicional de estampa de tiempo lo que atrajo la atención y preferencia de los empresarios.

Gráfico 30 Porcentaje del nivel de facilidad de uso de la herramienta andes Signer en las empresas del sector comercial

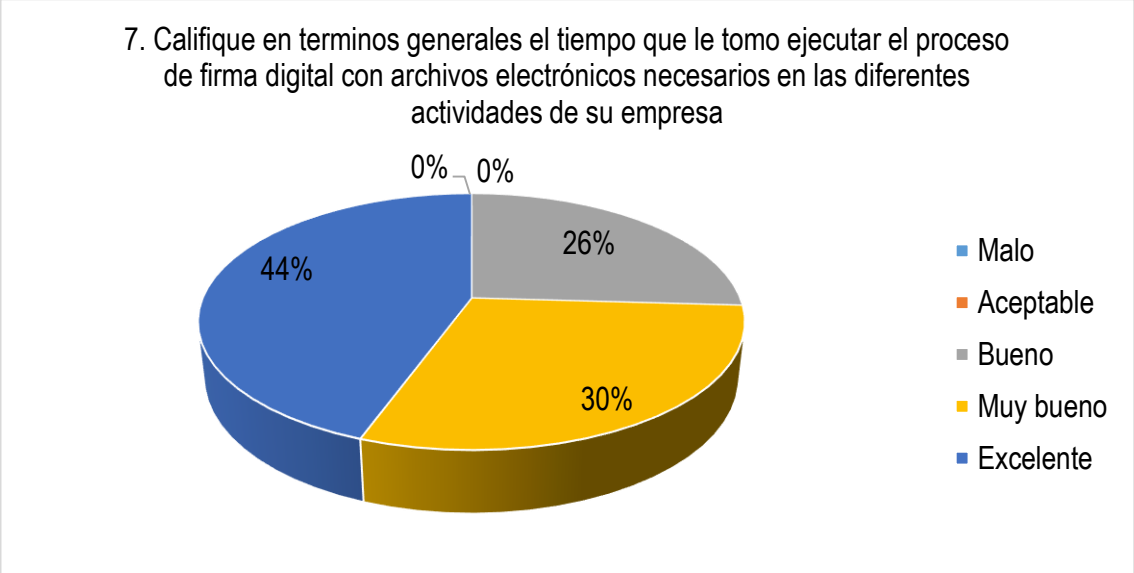


Fuente: Autores del proyecto

Se observa que por su interfaz demasiado simple la aplicación no generó gran interés a los empresarios encuestados, se manifestó que la ejecución de procesos de firma y validación eran confusos y no se sentían cómodos al intentar desarrollar sus actividades diarias.

Adicionalmente se buscó calificar en términos generales el tiempo que le tomo a los empresarios de las MIPYMES ejecutar el proceso de firma digital en las diferentes actividades de su empresa y finalmente calificar la percepción del impacto de la implementación del mecanismo de seguridad de firma digital en las actividades de su empresa.

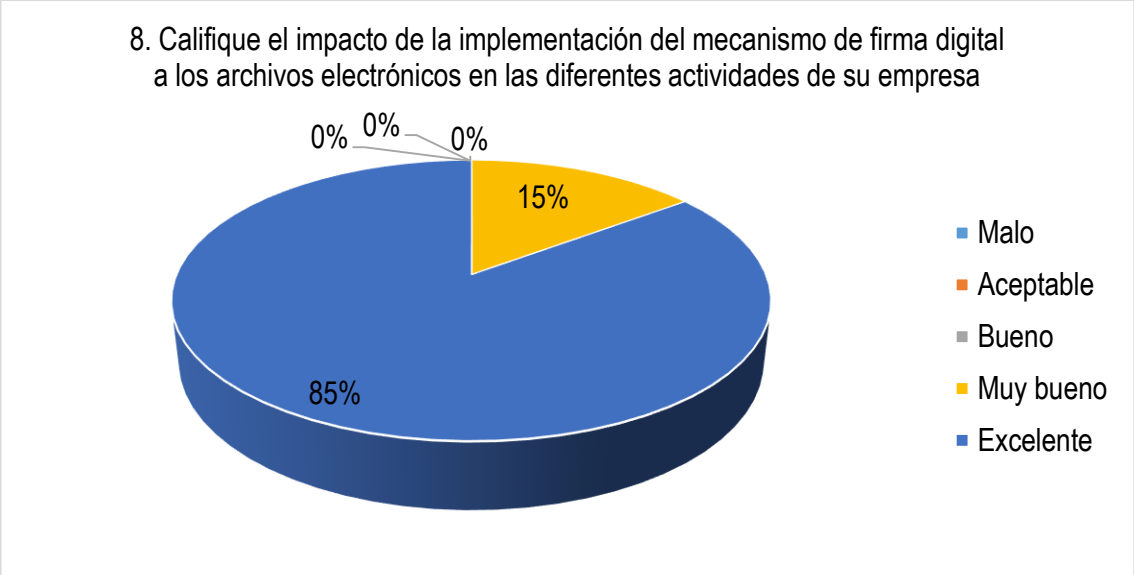
Gráfico 31 Porcentaje de calificación del tiempo de ejecución del proceso de firma digital en el desarrollo de las actividades de las empresas del sector comercial



Fuente: Autores del proyecto

Se observa gran satisfacción en el tiempo que se lleva realizar el proceso de firma digital con los archivos en formato electrónico, el 74 % de las empresas califico como excelente o muy bueno el tiempo que tomo ejecutar el procedimiento, otro 26 % lo califico como bueno.

Gráfico 32 Porcentaje de calificación del impacto de la implementación del mecanismo de firma digital en el desarrollo de las actividades de las empresas del sector comercial



Fuente: Autores del proyecto

Se observa un alto grado de aceptación y satisfacción por parte de las empresas encuestadas en la implementación del mecanismo de firma digital y la importancia de su uso en sus actividades diarias.

13.6. IMPLEMENTACIÓN EN EL SECTOR SALUD

13.6.1. Datos de las encuestas del sector salud

Cuadro 6 Resultados obtenidos en las encuestas de diagnóstico aplicadas a las mipymes del sector salud

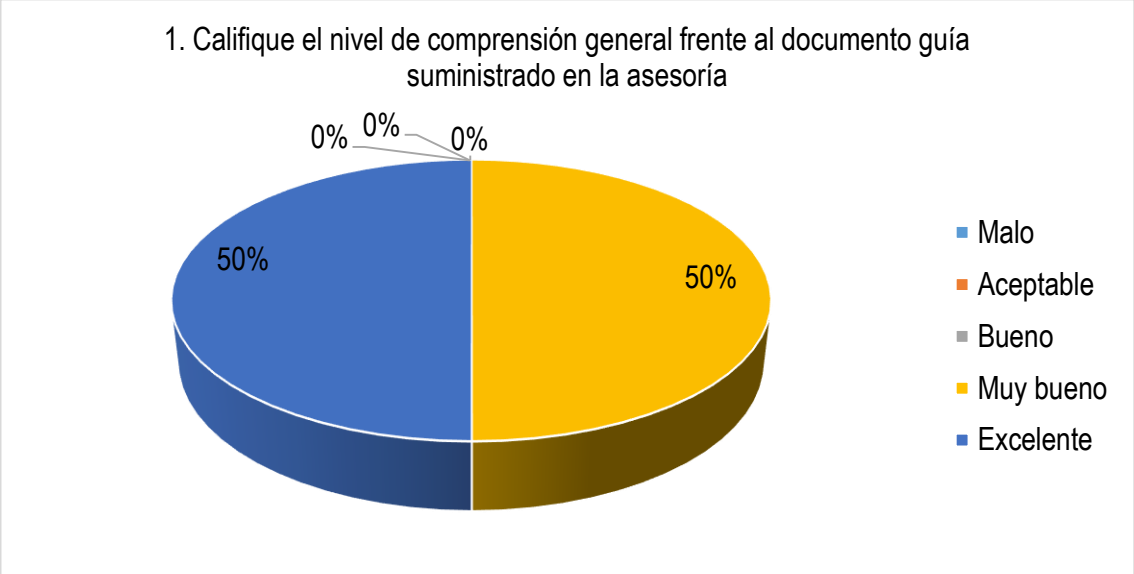
Pregunta	M*	A*	B*	MB*	E*
1) Califique el nivel de comprensión general frente al documento guía suministrado en la asesoría	0	0	0	1	1
2) Califique el tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación de certificado de firma digital	0	0	1	0	1
3) Califique el nivel de comprensión del proceso de instalación del certificado de firma digital	0	0	0	1	1
4) Califique la facilidad de uso de la herramienta "CertiFirma" para el proceso de firma digital	0	1	1	0	0
5) Califique la facilidad de uso de la herramienta "XolidoSign" para el proceso de firma digital	0	0	0	0	2
6) Califique la facilidad de uso de la herramienta "Andes Signer" para el proceso de firma digital	1	1	0	0	0
7) Califique en términos generales el tiempo que le tomo ejecutar el proceso de firma digital con archivos electrónicos necesarios en las diferentes actividades de su empresa	0	0	0	2	0
8) Califique el impacto de la implementación del mecanismo de firma digital a los archivos electrónicos en las diferentes actividades de su empresa	0	0	0	0	2

* M = Malo; A = Aceptable; B = Bueno; MB = Muy Bueno; E = Excelente

Fuente: Autores del proyecto

13.6.2. Análisis de los datos del sector salud. Se busca que los empresarios de las MIPYMES del sector salud califiquen en términos generales el nivel de comprensión frente al documento guía suministrado en la asesoría recibida posterior a la encuesta de diagnóstico.

Gráfico 33 Porcentaje del nivel de comprensión del documento guía en las empresas del sector salud

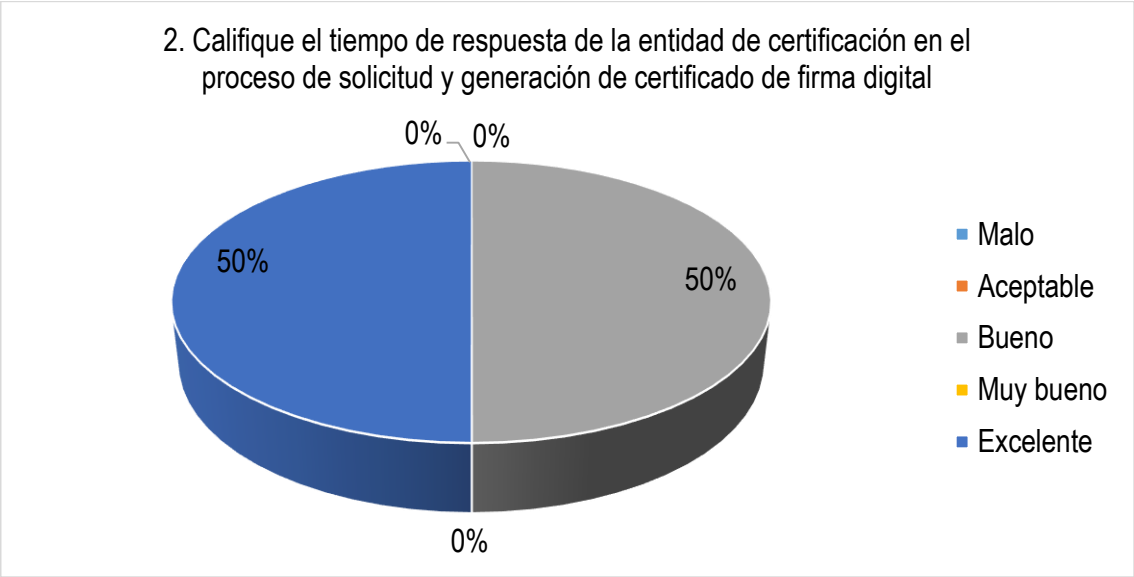


Fuente: Autores del proyecto

Se observa un alto grado de aceptación de la guía dada en la asesoría debido al evidenciar que el 50 % de las empresas encuestadas califica el nivel de comprensión de la guía como Excelente y otro 50 % lo califica como Muy bueno debido a su contenido fácil de asimilar con el paso a paso de los procesos de obtención del certificado de firma digital y la forma de usar correctamente las aplicaciones de firmado como son Certifirma, XolidoSign, Andes Signer.

El elemento central para el desarrollo del documento guía por parte de los empresarios de las MIPYMES es el certificado de firma digital, debido a su importancia se busca que se califique el tiempo de respuesta de la entidad de certificación digital en el proceso de solicitud y generación.

Gráfico 34 Porcentaje de calificación del tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación del certificado de firma digital en las empresas del sector salud

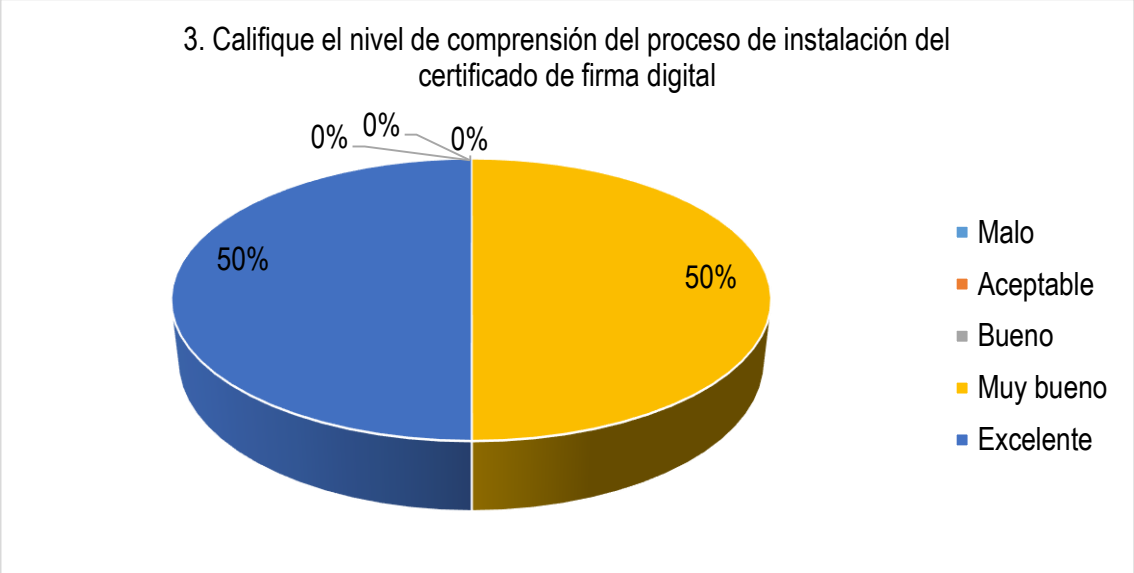


Fuente: Autores del proyecto

El tiempo estimado entre la obtención y la generación del certificado de firma digital por parte de la entidad de certificación está dentro del rango viable para el proceso según las empresas encuestadas, al responder el 50 % de las empresas que el tiempo de respuesta se encuentra entre excelente, otro 50 % califica el tiempo de respuesta como bueno, además que el proceso es fácil de realizar y se envían mensajes de correo electrónico con el estado del trámite e información de soporte.

Una vez determinada la percepción de los tiempos de respuesta de la entidad de certificación, se busca medir el nivel de comprensión por parte de los empresarios de las MIPYMES del proceso de instalación del certificado de firma digital tramitado ante la correspondiente entidad, lo anterior detallado en el documento guía suministrado en la asesoría.

Gráfico 35 Porcentaje del nivel de comprensión del proceso de instalación del certificado de firma digital en las empresas del sector salud

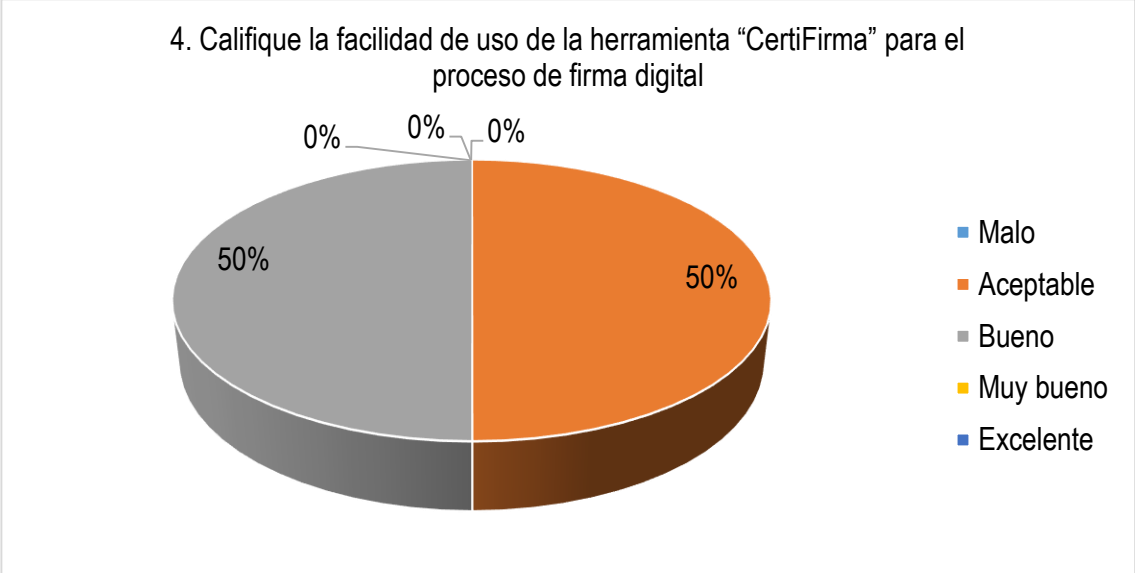


Fuente: Autores del proyecto

Se observa que el proceso detallado en la guía para la instalación del certificado está escrito de una forma muy clara, lo que permite con facilidad cumplir con el ejercicio y realizarlo de una forma rápida siguiendo el paso a paso descrito en el documento, lo anterior basado en la calificación dada por las empresas de las cuales el 50 % considera que el nivel de comprensión es excelente y otro 50 % considera que el nivel de comprensión es muy bueno.

Complementario al certificado de firma digital, las herramientas (software) suministradas por las entidades de certificación digital forman parte fundamental del proceso y afectan el impacto y la satisfacción de la implementación de este mecanismo de seguridad, por lo anterior se buscó determinar la facilidad de uso de las herramientas propuestas en el documento guía (CertiFirma, XolidoSign, Andes Signer) por parte de los empresarios de las MIPYMES.

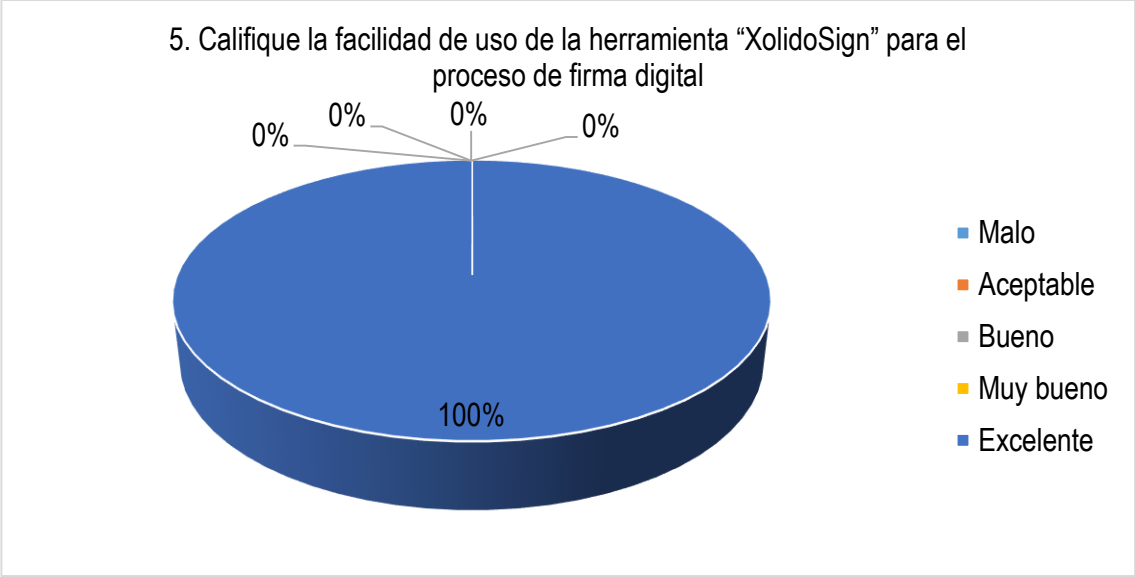
Gráfico 36 Porcentaje del nivel de facilidad de uso de la herramienta certifirma en las empresas del sector salud



Fuente: Autores del proyecto

Se observa que por su funcionamiento la herramienta CertiFirma no generó gran interés a los empresarios encuestados, los cuales manifestaron que la herramienta empaqueta el archivo firmado con la firma, se requiere desempaquetar el contenido para poder visualizar el archivo firmado digitalmente lo que representa más tiempo para la ejecución de los diferentes procesos de la firma digital como el firmado y la validación.

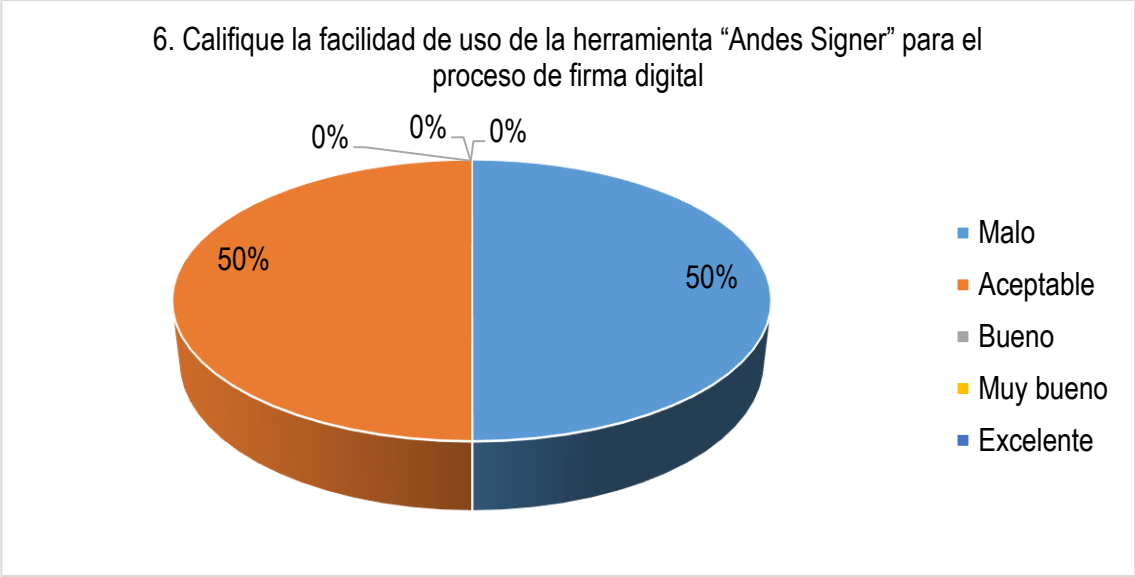
Gráfico 37 Porcentaje del nivel de facilidad de uso de la herramienta xolidosign en las empresas del sector salud



Fuente: Autores del proyecto

Se observa que por su interfaz agradable y las opciones que ofrece la aplicación generó gran interés a las empresas encuestadas, se manifestó gran facilidad comparada con la herramienta CertiFirma debido a que XolidoSign genera un archivo complementario al archivo firmado digitalmente, por lo que no se lleva a cabo un proceso de empaquetado o desempaquetado, facilita las ejecución de los diferentes procesos de la firma digital como el firmado y la validación. Esta herramienta ofrece un servicio adicional de estampa de tiempo lo que atrajo la atención y preferencia de los empresarios.

Gráfico 38 Porcentaje del nivel de facilidad de uso de la herramienta andes Signer en las empresas del sector salud

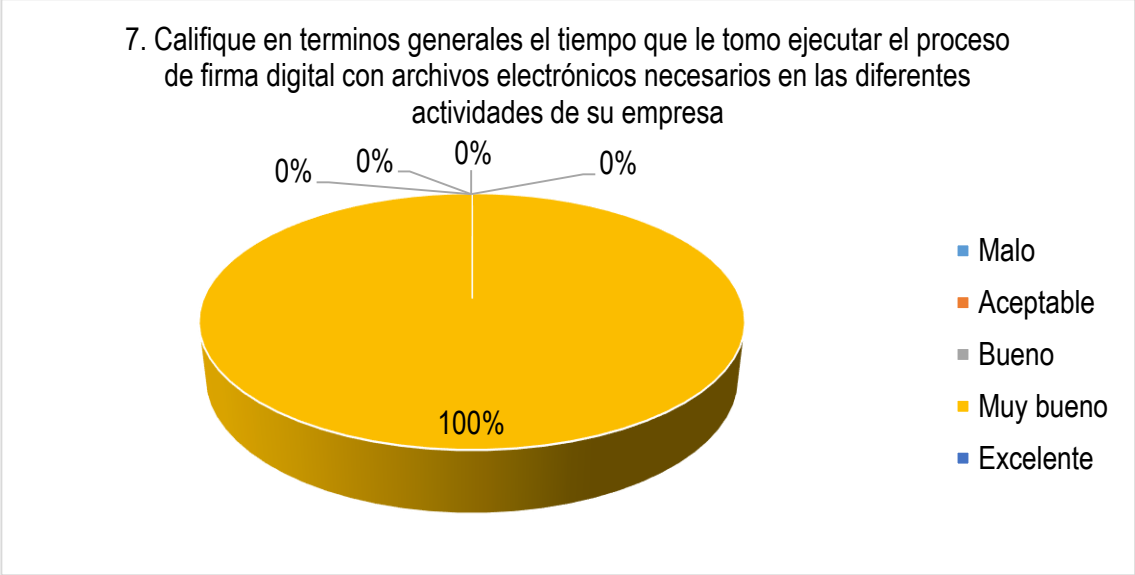


Fuente: Autores del proyecto

Se observa que por su interfaz demasiado simple la aplicación no generó gran interés a los empresarios encuestados, se manifestó que la ejecución de procesos de firma y validación eran confusos y no se sentían cómodos al intentar desarrollar sus actividades diarias.

Adicionalmente se buscó calificar en términos generales el tiempo que le tomo a los empresarios de las MIPYMES ejecutar el proceso de firma digital en las diferentes actividades de su empresa y finalmente calificar la percepción del impacto de la implementación del mecanismo de seguridad de firma digital en las actividades de su empresa.

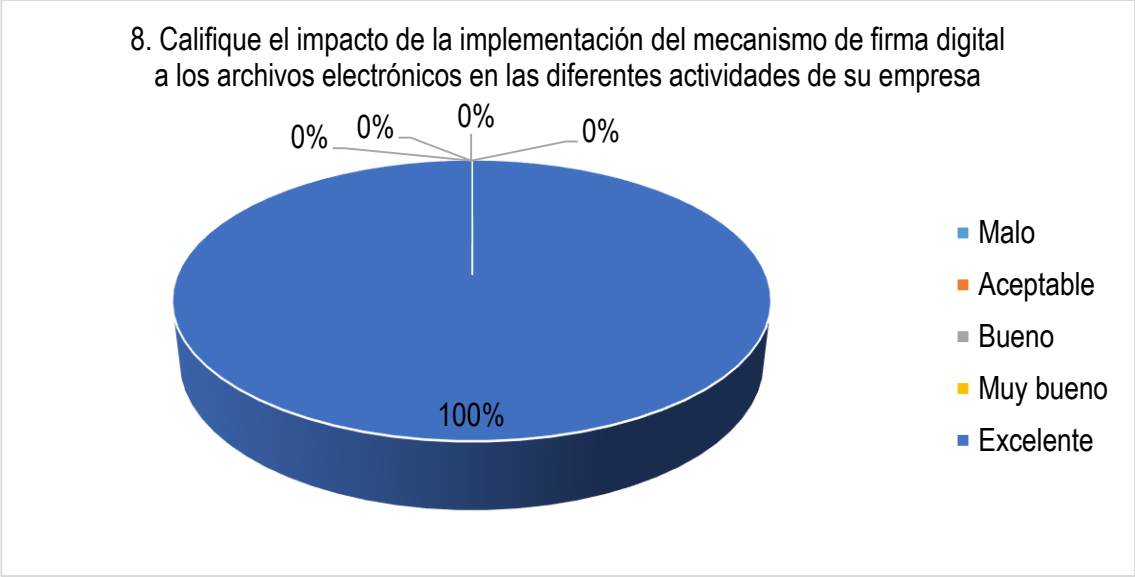
Gráfico 39 Porcentaje de calificación del tiempo de ejecución del proceso de firma digital en el desarrollo de las actividades de las empresas del sector salud



Fuente: Autores del proyecto

Se observa gran satisfacción en el tiempo que se lleva realizar el proceso de firma digital con los archivos en formato electrónico, el 100 % de las empresas califico como excelente el tiempo que tomo ejecutar el procedimiento.

Gráfico 40 Porcentaje de calificación del impacto de la implementación del mecanismo de firma digital en el desarrollo de las actividades de las empresas del sector salud



Fuente: Autores del proyecto

Se observa un alto grado de aceptación y satisfacción por parte de las empresas encuestadas en la implementación del mecanismo de firma digital y la importancia de su uso en sus actividades diarias.

14. CONCLUSIONES

La captura de los requerimientos técnicos permitió a los autores del proyecto establecer el ecosistema Microsoft Windows como el entorno computacional para implementación de firmas digitales, basado en las herramientas de firma digital suministradas por las entidades de certificación que solo están disponibles para esta plataforma, la de mayor uso a nivel mundial y la que adquieren la mayor cantidad de empresarios por su facilidad y simplicidad en su uso.

El establecimiento del contexto jurídico para la implementación de firmas digitales en Colombia permitió a los autores del proyecto determinar las organizaciones establecidas para la autorización de las entidades de certificación digital, adicionalmente establecer la validez probatoria y el alcance legal dado por las leyes del país a estos mecanismos criptográficos.

La ejecución de una estrategia de capacitaciones permitió a los autores del proyecto trasmitir a los empresarios la facilidad de uso y las ventajas tecnologías y legales que ofrece la implementación de certificados y firmas digitales en el desarrollo de los diferentes procesos de sus MIPYMES tanto en sus actividades digitales propias, como en el desarrollo del comercio electrónico que se realizará de la mano del proyecto marco ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE.

La creación y ejecución de pruebas piloto permitió a los autores del proyecto evaluar el producto final de este proyecto, la guía de implementación de certificados y firmas digitales que evidencio que los empresarios con conocimientos básicos y las herramientas de tecnológicas adecuadas pueden incorporar estos mecanismos criptográficos en los procesos internos y externos que desarrolle la empresa con archivos electrónicos los cuales poseen total validez legal y características matemáticas que garanticen su integridad, autenticidad y no repudio.

BIBLIOGRAFÍA

FUSTER SABATER, Amparo. HERNÁNDEZ ENCINAS, Luis. MARTIN MUÑOZ, Agustín. MONTOYA VITINI, Fausto. MUÑOZ MASQUE. Jaime. Criptografía protección de datos y aplicaciones: Guía para estudiantes y profesionales. México: Alfaomega grupo editor, 2013.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Acuerdo de licencia. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Acuerdo_de_licencia>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Algoritmo de cifrado. [en línea]. < http://www.inteco.es/glossary/Formacion/Glosario/Algoritmo_de_cifrado>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Autenticación. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/AuTenticacion>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptografía. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptografia_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptografía Asimétrica. [en línea].

<http://www.inteco.es/glossary/Formacion/Glosario/Criptografia_Asimetrica_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptografía Simétrica. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptografia_Simetrica_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Criptograma. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Criptograma_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Ejecutable. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Ejecutable>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Evidencia Electrónica. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Evidencia_Electronica_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - HSM. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/HSM_Glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - HTTPS. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/HTTPS>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Log. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Log_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Protocolo. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Protocolo>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Servidor. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Servidor_Glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Sistema Operativo. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Sistema_Operativo1>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Software. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Software1>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Suplantación de identidad. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/suplantacion_de_identidad_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Timestamping. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Timestamping_glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Token criptográfico. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/token_criptografico>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - URL. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/URL>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Usuario. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Usuario_Glosario>. [citado en 24 de marzo de 2014].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos - Vulnerabilidad. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/Vulnerabilidad_Glosario>. [citado en 24 de marzo de 2014].

SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL. Manuales de soporte técnico. [en línea]. <https://web.certicamara.com/soporte-tecnico/manuales-de-soporte-t%C3%A9cnico/>. [citado en 10 de febrero de 2014].

SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL. Marco legal. [en línea]. <https://web.certicamara.com/marco-legal/>. [citado en 25 de enero de 2014].

SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL. Centro de descargas. [en línea]. <https://web.certicamara.com/centro-de-descargas/>. [citado en 10 de febrero de 2014].

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Chat gobierno en línea. [en línea]. <http://chat.gobiernoenlinea.gov.co/webchat/sic/>. [citado en 29 de enero de 2014].

ALCALDÍA DE BOGOTÁ. Ley 527 de 2009. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276>. [citado en 9 de noviembre de 2013].

ALCALDÍA DE BOGOTÁ. Ley 794 DE 2003. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6922>. [citado en 9 de noviembre de 2013].

ALCALDÍA DE BOGOTÁ. Ley 962 DE 2005. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17004>. [citado en 9 de noviembre de 2013].

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Decreto 1747 de 2000. [en línea]. <http://www.sic.gov.co/documents/10157/397811/Decreto_1747_2000.pdf/1bbcb205-a35c-435b-a5ba-413c641f4f86>. [citado en 9 de noviembre de 2013].

ALCALDÍA DE BOGOTÁ. Decreto 1929 de 2007. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=25311>. [citado en 9 de noviembre de 2013].

ALCALDÍA DE BOGOTÁ. Decreto 2474 de 2008. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31185>. [citado en 9 de noviembre de 2013].

ALCALDÍA DE BOGOTÁ. Decreto 2150 de 1995. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1208>. [citado en 9 de noviembre de 2013].

ALCALDÍA DE BOGOTÁ. Ley 270 de 1996. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6548>. [citado en 9 de noviembre de 2013].

Anexo A Formato de encuesta de diagnóstico aplicado a empresarios de las MIPYMES

GUÍA DE IMPLEMENTACIÓN DE CERTIFICADOS Y FIRMAS DIGITALES

Encuesta # 1 – Diagnostico

Nombre: NIT:

Empresa:

1) Seleccione el sector económico al que pertenece su empresa.
   a) Servicios
   b) Industrial
   c) Comercial
   d) Salud
   e) Otro, cual_____
2) ¿Dentro del desarrollo de los procesos de su empresa hace uso de equipos de cómputo para la generación, administración y/o almacenamiento de archivos en formato electrónico?
   a) Si
   b) No
3) ¿El sistema operativo que se encuentra implementado en los equipos de cómputo de su empresa es Microsoft Windows?
   a) Si
   b) No
4) ¿Conoce usted algún mecanismo para la protección de sus archivos en formato electrónico que son importantes para su empresa (Facturas, contratos, correos electrónicos, etc)?
   a) Si
   b) No
5) ¿Está interesado en implementar herramientas que agreguen seguridad a la generación, administración y/o almacenamiento de archivos en formato electrónico?
   a) Si
   b) No
6) ¿Conoce o está familiarizado con el concepto de Firma digital?
   a) Si
   b) No
7) La firma digital es un mecanismo que permite identificar que su información no ha sido alterada después de ser firmada y comprobar que fue usted quien efectivamente generó el archivo electrónico, posee la misma validez de la firma manuscrita pero con numerosas ventajas técnicas. ¿Está interesado en implementar firmas digitales para asegurar sus archivos en formato electrónico?
   a) Si
   b) No
8) ¿Le gustaría recibir una asesoría (Conceptos básicos, herramientas necesarias, documento guía) para la implementación de este mecanismo de seguridad?
   a) Si
   b) No

Fuente: Autores del proyecto

Anexo B Formato encuesta de medición de impacto de implementación página 1 de 2

GUÍA DE IMPLEMENTACIÓN DE CERTIFICADOS Y FIRMAS DIGITALES

Encuesta # 2 – Medición

Nombre: NIT:

Empresa:

1) Califique el nivel de comprensión general frente al documento guía suministrado en la asesoría:
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente
2) Califique el tiempo de respuesta de la entidad de certificación en el proceso de solicitud y generación de certificado de firma digital:
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente
3) Califique el nivel de comprensión del proceso de instalación del certificado de firma digital
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente
4) Califique la facilidad de uso de la herramienta "CertiFirma" para el proceso de firma digital
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente
5) Califique la facilidad de uso de la herramienta "XolidoSign" para el proceso de firma digital
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente
6) Califique la facilidad de uso de la herramienta "Andes Signer" para el proceso de firma digital
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno

Fuente: Autores del proyecto

Formato encuesta de medición de impacto de implementación página 2 de 2

e) Excelente

7) Califique en términos generales el tiempo que le tomo ejecutar el proceso de firma digital con archivos electrónicos necesarios en las diferentes actividades de su empresa:
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente
8) Califique el impacto de la implementación del mecanismo de firma digital a los archivos electrónicos en las diferentes actividades de su empresa:
   a) Malo
   b) Aceptable
   c) Bueno
   d) Muy bueno
   e) Excelente

Fuente: Autores del proyecto

Anexo C Radicado número 14-187143- -4- 1 en respuesta de Superintendencia de Industria y Comercio a los autores del proyecto sobre los actos administrativos para la autorización de entidades de certificación digital

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RAD: 14-18713- -4-1 **FECHA:** 2014-02-18 17:25:23
DEP: 6000 DESPACHO DEL SUPERINTENDENTE DELEGAD **EVE:** SIN EVENTO
TRA: 362 DP-SOLICITUD COPIAS **FOLIOS:** 19
ACT: 440 RESPUESTA

Bogotá D.C.

6000

Señor
JORGE ENRIQUE MUÑOZ SILVA
Ingeniero de Sistemas
Candidato a Esp. Seguridad Informática - UniPilóto
joenmusi@gmail.com

Asunto: Radicación: 14-18713- -4-1
Trámite: 362
Evento:
Actuación: 440
Folios: 19

Estimado Señor:

En respuesta a solicitud le informo que el decreto 19 de 2012 asignó las funciones que tenía la Superintendencia de Industria y Comercio en materia de entidades de certificación de firmas digitales al Organismo Nacional de Acreditación de Colombia – ONAC, por lo que nos limitaremos a otorgar información con anterioridad a la expedición de dicho decreto. Adjunto remito los actos administrativos por los cuales esta Superintendencia autorizó a las siguientes empresas como entidades de Certificación Digital:

SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL CERTICÁMARA, S.A.
Autorizada mediante resolución No. 1007 del 24 de enero de 2002

Autorización de nuevos servicios – Ampliación de la Autorización:
Resolución No. 22456 (10/09/2004)
Resolución No. 28012 (12/11/2004)
Resolución No. 9887 (13/04/2007)
Resolución No. 3816 (30/01/2009)

GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A. - GSE S.A.
Autorizada mediante resolución No. 23344 del 12 de mayo de 2009

Autorización de nuevos servicios – Ampliación de la Autorización:
Resolución No. 1194 (21/01/2010)

ANDES SERVICIO DE CERTIFICACIÓN DIGITAL S.A. ANDES SCD
Autorizada mediante Resolución 14349 del 23 de marzo de 2012

Atentamente,

ALEJANDRO GIRALDO LOPEZ
Superintendente Delegado para el Control y Verificación de Reglamentos Técnicos y Metrología Legal

Elaboró:Amparo Navarro
Revisó: Alejandro Giraldo
Aprobó: Alejandro Giraldo

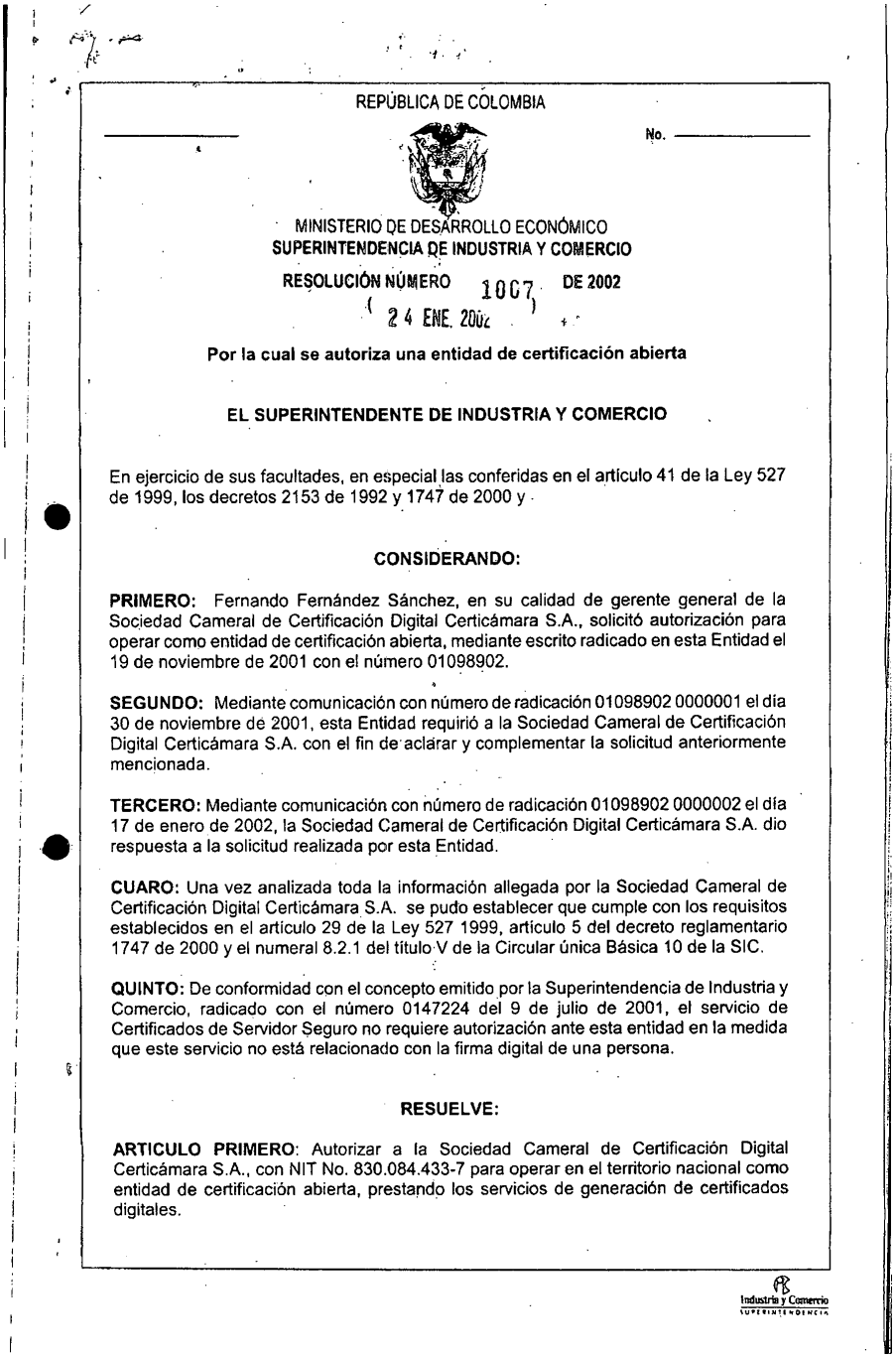
Sede Centro: Carrera 13 No. 27-00 pisos 1, 3, 5, 7 y 10 PBX: (571) 5870000
Call Center (571) 592 04 00. Linea gratuita Nacional 01800-910165
Web: www.sic.gov.co e-mail: contactenos@sic.gov.co
Bogotá D.C. Colombia

Al contestar favor indique el número de radicación que se indica a continuación:
Radicación: 14-18713- -4-1 2014-02-18 17:25:23

MinCIT PROSPERIDAD PARA TODOS

Fuente: Superintendencia de Industria y Comercio

Anexo D Resolución N°. 1007 del 24 de enero de 2002 superintendencia de industria y comercio pagina 1 de 2



REPÚBLICA DE COLOMBIA

No. _____

MINISTERIO DE DESARROLLO ECONÓMICO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 1007 **DE 2002**
(24 ENE. 2002)

Por la cual se autoriza una entidad de certificación abierta

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

En ejercicio de sus facultades, en especial las conferidas en el artículo 41 de la Ley 527 de 1999, los decretos 2153 de 1992 y 1747 de 2000 y

CONSIDERANDO:

PRIMERO: Fernando Fernández Sánchez, en su calidad de gerente general de la Sociedad Cameral de Certificación Digital Certicámara S.A., solicitó autorización para operar como entidad de certificación abierta, mediante escrito radicado en esta Entidad el 19 de noviembre de 2001 con el número 01098902.

SEGUNDO: Mediante comunicación con número de radicación 01098902 0000001 el día 30 de noviembre de 2001, esta Entidad requirió a la Sociedad Cameral de Certificación Digital Certicámara S.A. con el fin de aclarar y complementar la solicitud anteriormente mencionada.

TERCERO: Mediante comunicación con número de radicación 01098902 0000002 el día 17 de enero de 2002, la Sociedad Cameral de Certificación Digital Certicámara S.A. dio respuesta a la solicitud realizada por esta Entidad.

CUARO: Una vez analizada toda la información allegada por la Sociedad Cameral de Certificación Digital Certicámara S.A. se pudo establecer que cumple con los requisitos establecidos en el artículo 29 de la Ley 527 1999, artículo 5 del decreto reglamentario 1747 de 2000 y el numeral 8.2.1 del título V de la Circular única Básica 10 de la SIC.

QUINTO: De conformidad con el concepto emitido por la Superintendencia de Industria y Comercio, radicado con el número 0147224 del 9 de julio de 2001, el servicio de Certificados de Servidor Seguro no requiere autorización ante esta entidad en la medida que este servicio no está relacionado con la firma digital de una persona.

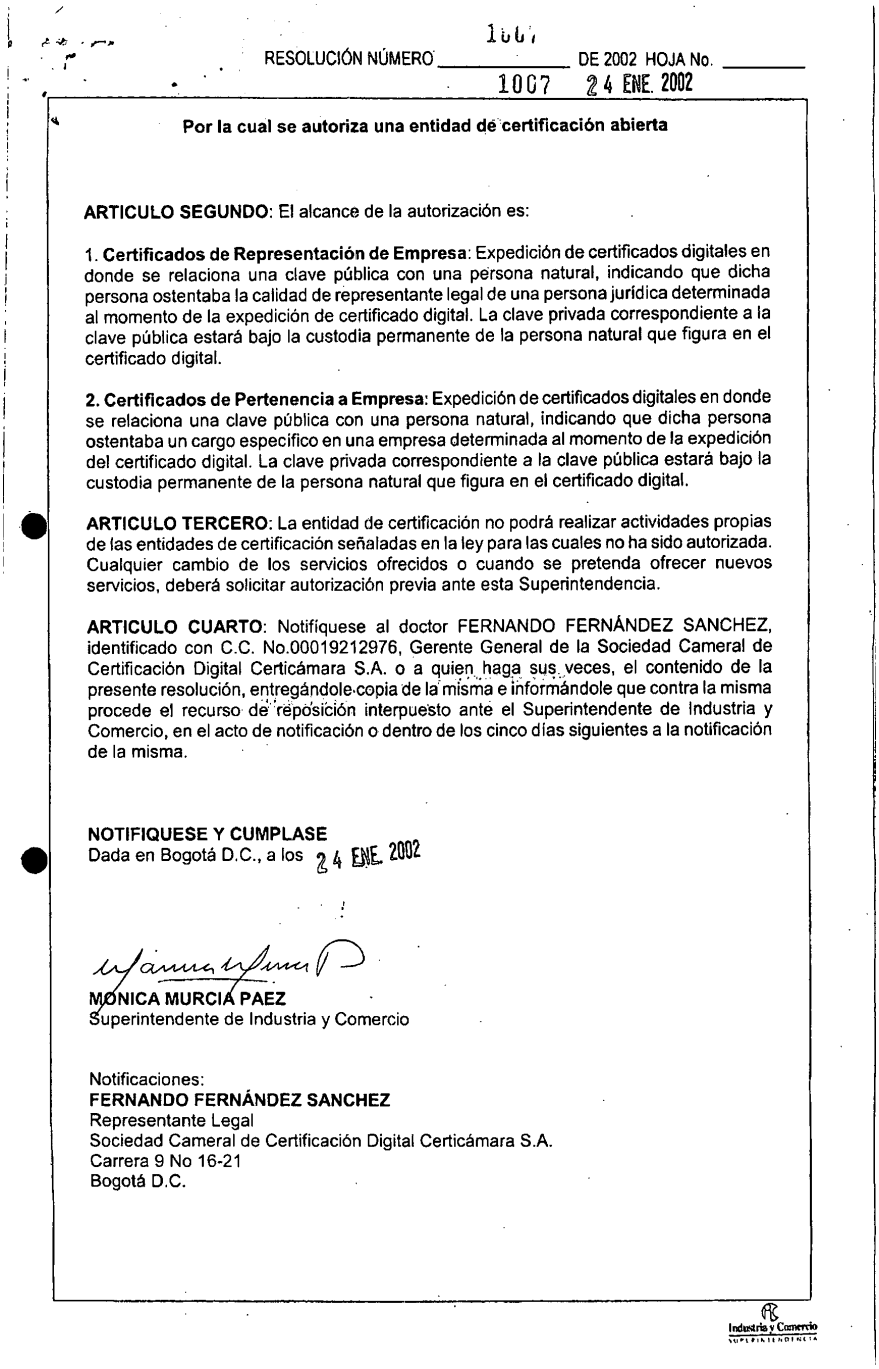
RESUELVE:

ARTICULO PRIMERO: Autorizar a la Sociedad Cameral de Certificación Digital Certicámara S.A., con NIT No. 830.084.433-7 para operar en el territorio nacional como entidad de certificación abierta, prestando los servicios de generación de certificados digitales.

Industria y Comercio
SUPERINTENDENCIA

Fuente: Superintendencia de Industria y Comercio

Resolución N°. 1007 del 24 de enero de 2002 superintendencia de industria y comercio pagina 2 de 2



RESOLUCIÓN NÚMERO 1007 DE 2002 HOJA No. _____

1007 24 ENE. 2002

Por la cual se autoriza una entidad de certificación abierta

ARTICULO SEGUNDO: El alcance de la autorización es:

1. **Certificados de Representación de Empresa**: Expedición de certificados digitales en donde se relaciona una clave pública con una persona natural, indicando que dicha persona ostentaba la calidad de representante legal de una persona jurídica determinada al momento de la expedición de certificado digital. La clave privada correspondiente a la clave pública estará bajo la custodia permanente de la persona natural que figura en el certificado digital.

2. Certificados de Pertenencia a Empresa: Expedición de certificados digitales en donde se relaciona una clave pública con una persona natural, indicando que dicha persona ostentaba un cargo específico en una empresa determinada al momento de la expedición del certificado digital. La clave privada correspondiente a la clave pública estará bajo la custodia permanente de la persona natural que figura en el certificado digital.

ARTICULO TERCERO: La entidad de certificación no podrá realizar actividades propias de las entidades de certificación señaladas en la ley para las cuales no ha sido autorizada. Cualquier cambio de los servicios ofrecidos o cuando se pretenda ofrecer nuevos servicios, deberá solicitar autorización previa ante esta Superintendencia.

ARTICULO CUARTO: Notifíquese al doctor FERNANDO FERNÁNDEZ SANCHEZ, identificado con C.C. No.00019212976, Gerente General de la Sociedad Cameral de Certificación Digital Certicámara S.A. o a quien haga sus veces, el contenido de la presente resolución, entregándole copia de la misma e informándole que contra la misma procede el recurso de reposición interpuesto ante el Superintendente de Industria y Comercio, en el acto de notificación o dentro de los cinco días siguientes a la notificación de la misma.

NOTIFIQUESE Y CUMPLASE
Dada en Bogotá D.C., a los 24 ENE. 2002

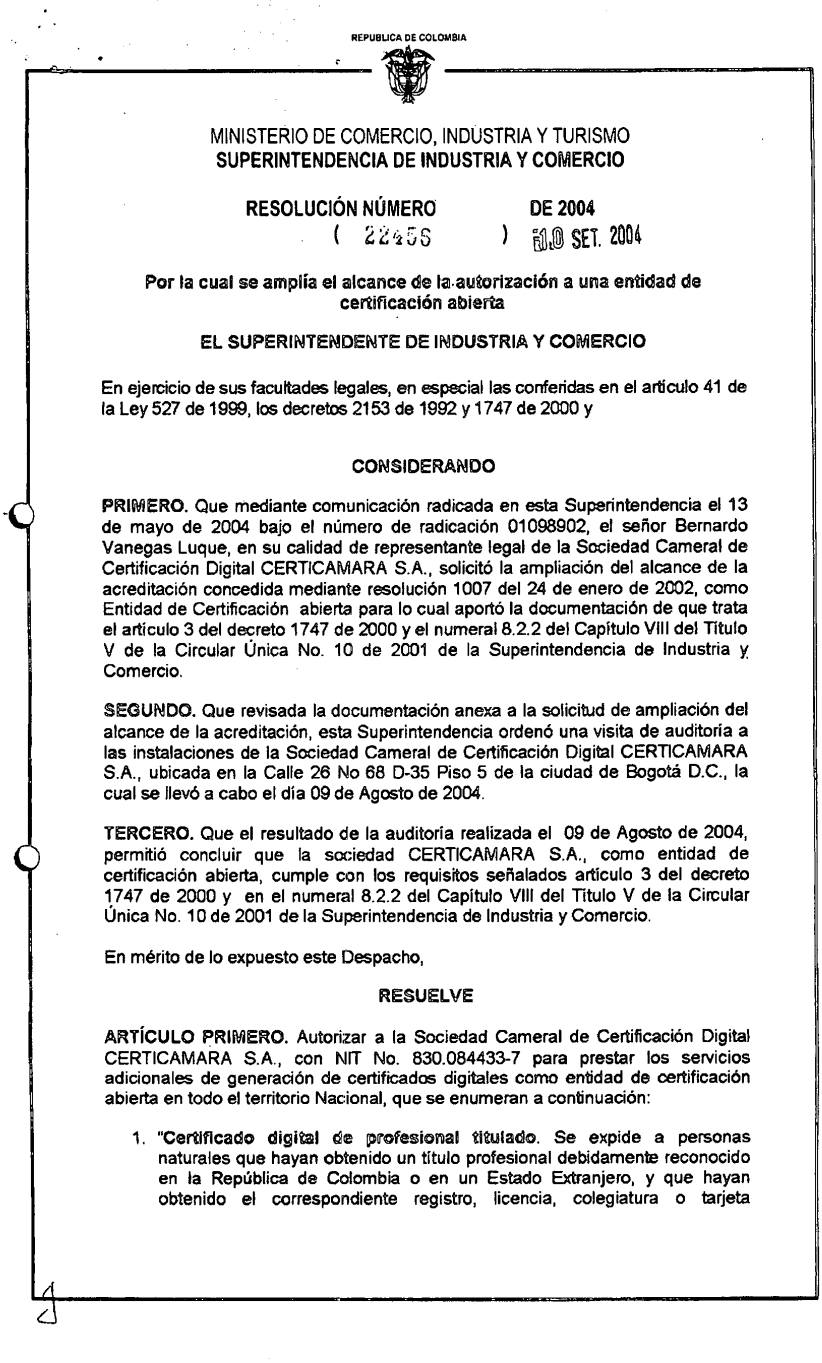
MÓNICA MURCIA PAEZ
Superintendente de Industria y Comercio

Notificaciones:
FERNANDO FERNÁNDEZ SANCHEZ
Representante Legal
Sociedad Cameral de Certificación Digital Certicámara S.A.
Carrera 9 No 16-21
Bogotá D.C.

Industria y Comercio
SUPERINTENDENCIA

Fuente: Superintendencia de Industria y Comercio

Anexo E Resolución N°. 22456 (10/09/2004) superintendencia de industria y comercio pagina 1 de 2



REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO **DE 2004**
(22456) 10 SET. 2004

Por la cual se amplía el alcance de la autorización a una entidad de certificación abierta

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

En ejercicio de sus facultades legales, en especial las conferidas en el artículo 41 de la Ley 527 de 1999, los decretos 2153 de 1992 y 1747 de 2000 y

CONSIDERANDO

PRIMERO. Que mediante comunicación radicada en esta Superintendencia el 13 de mayo de 2004 bajo el número de radicación 01098902, el señor Bernardo Vanegas Luque, en su calidad de representante legal de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., solicitó la ampliación del alcance de la acreditación concedida mediante resolución 1007 del 24 de enero de 2002, como Entidad de Certificación abierta para lo cual aportó la documentación de que trata el artículo 3 del decreto 1747 de 2000 y el numeral 8.2.2 del Capítulo VIII del Título V de la Circular Única No. 10 de 2001 de la Superintendencia de Industria y Comercio.

SEGUNDO. Que revisada la documentación anexa a la solicitud de ampliación del alcance de la acreditación, esta Superintendencia ordenó una visita de auditoría a las instalaciones de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., ubicada en la Calle 26 No 68 D-35 Piso 5 de la ciudad de Bogotá D.C., la cual se llevó a cabo el día 09 de Agosto de 2004.

TERCERO. Que el resultado de la auditoría realizada el 09 de Agosto de 2004, permitió concluir que la sociedad CERTICAMARA S.A., como entidad de certificación abierta, cumple con los requisitos señalados artículo 3 del decreto 1747 de 2000 y en el numeral 8.2.2 del Capítulo VIII del Título V de la Circular Única No. 10 de 2001 de la Superintendencia de Industria y Comercio.

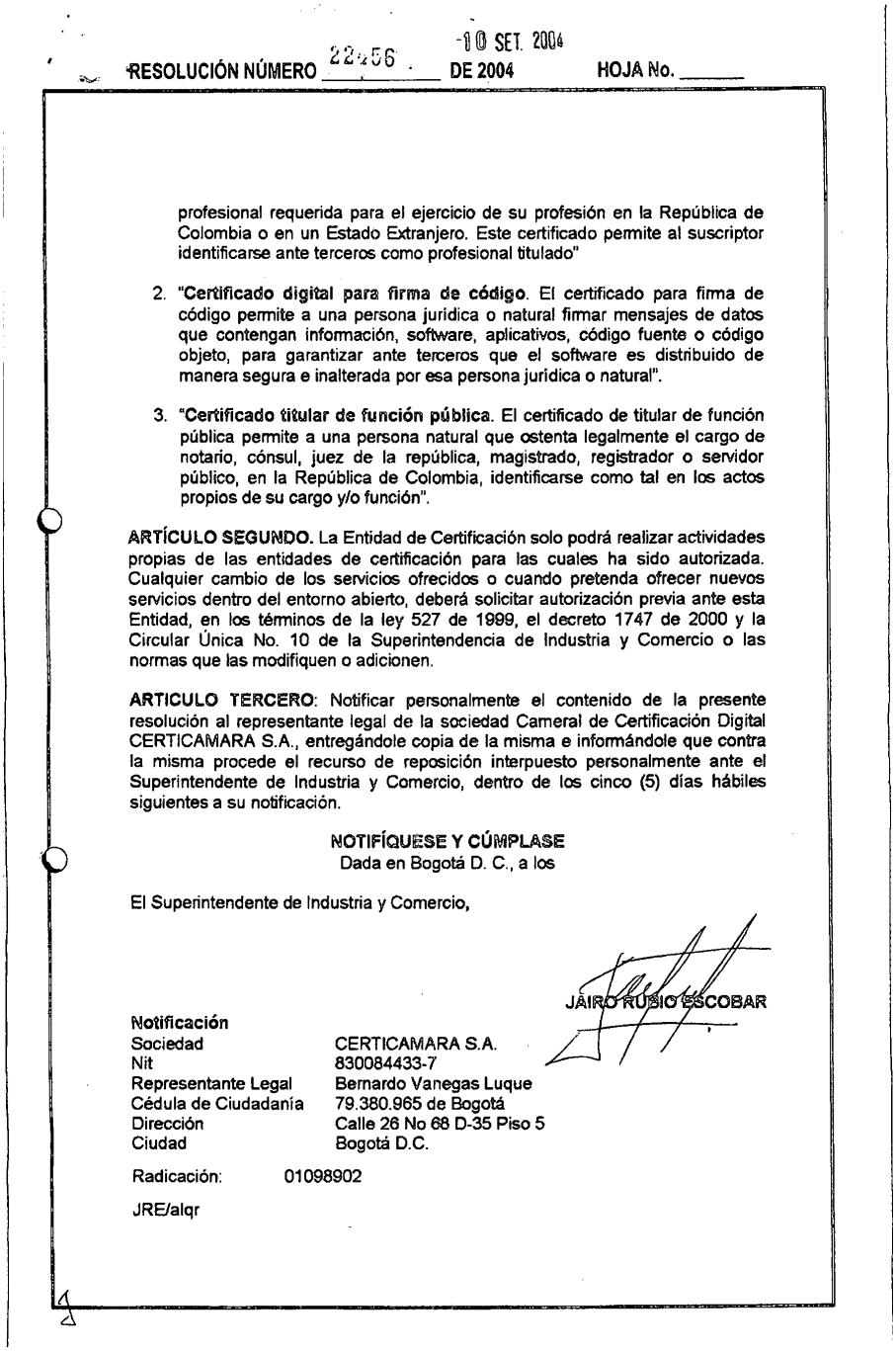
En mérito de lo expuesto este Despacho,

RESUELVE

ARTÍCULO PRIMERO. Autorizar a la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., con NIT No. 830.084433-7 para prestar los servicios adicionales de generación de certificados digitales como entidad de certificación abierta en todo el territorio Nacional, que se enumeran a continuación:

1. "**Certificado digital de profesional titulado.** Se expide a personas naturales que hayan obtenido un título profesional debidamente reconocido en la República de Colombia o en un Estado Extranjero, y que hayan obtenido el correspondiente registro, licencia, colegiatura o tarjeta

Fuente: Superintendencia de Industria y Comercio



-10 SET. 2004

RESOLUCIÓN NÚMERO 22456 DE 2004 HOJA No. _____

profesional requerida para el ejercicio de su profesión en la República de Colombia o en un Estado Extranjero. Este certificado permite al suscriptor identificarse ante terceros como profesional titulado"

2. "**Certificado digital para firma de código**. El certificado para firma de código permite a una persona jurídica o natural firmar mensajes de datos que contengan información, software, aplicativos, código fuente o código objeto, para garantizar ante terceros que el software es distribuido de manera segura e inalterada por esa persona jurídica o natural".

3. "**Certificado titular de función pública**. El certificado de titular de función pública permite a una persona natural que ostenta legalmente el cargo de notario, cónsul, juez de la república, magistrado, registrador o servidor público, en la República de Colombia, identificarse como tal en los actos propios de su cargo y/o función".

ARTÍCULO SEGUNDO. La Entidad de Certificación solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Cualquier cambio de los servicios ofrecidos o cuando pretenda ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta Entidad, en los términos de la ley 527 de 1999, el decreto 1747 de 2000 y la Circular Única No. 10 de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTICULO TERCERO: Notificar personalmente el contenido de la presente resolución al representante legal de la sociedad Cameral de Certificación Digital CERTICAMARA S.A., entregándole copia de la misma e informándole que contra la misma procede el recurso de reposición interpuesto personalmente ante el Superintendente de Industria y Comercio, dentro de los cinco (5) días hábiles siguientes a su notificación.

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá D. C., a los

El Superintendente de Industria y Comercio,

JAIRO RUBIO ESCOBAR

Notificación

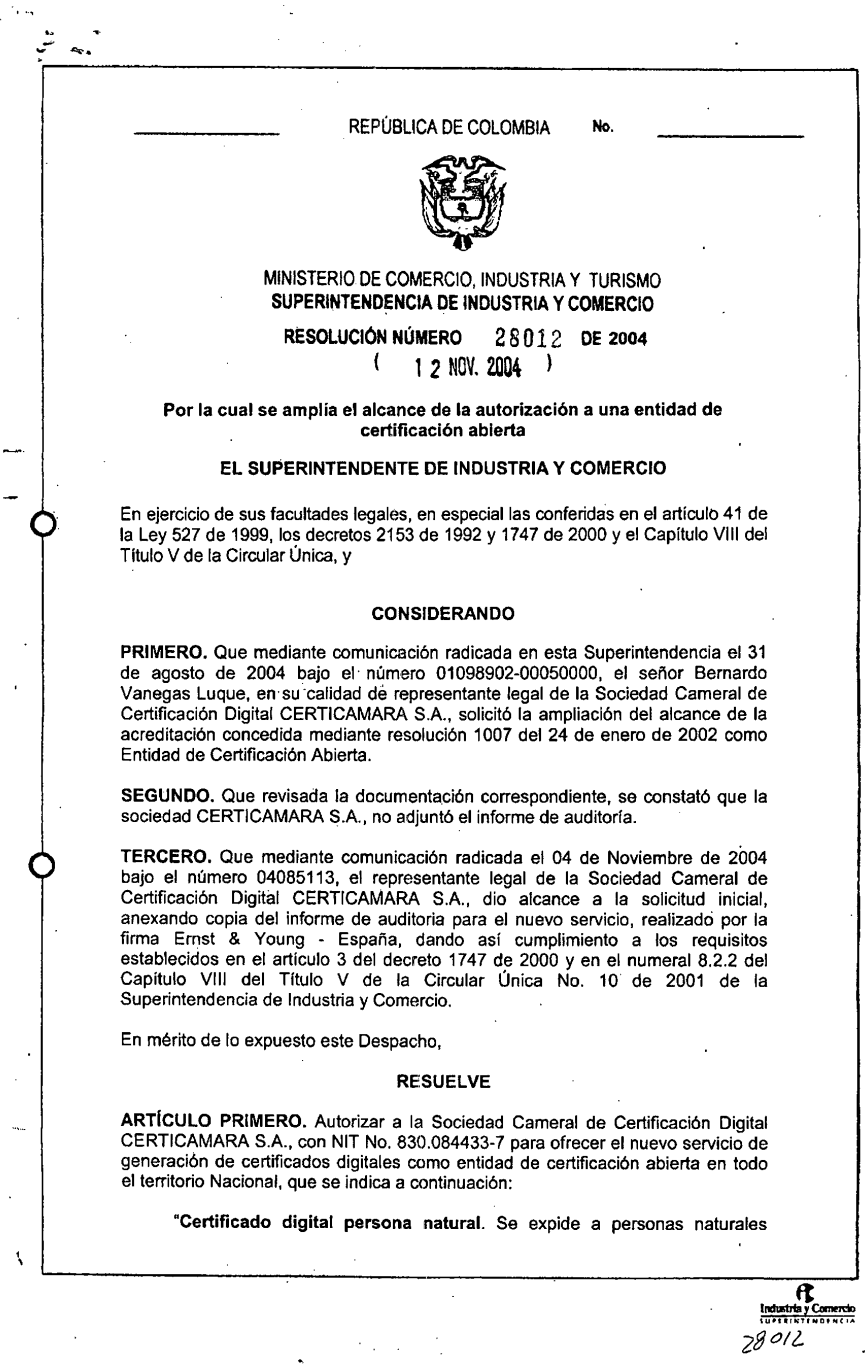
Sociedad	CERTICAMARA S.A.
Nit	830084433-7
Representante Legal	Bernardo Vanegas Luque
Cédula de Ciudadanía	79.380.965 de Bogotá
Dirección	Calle 26 No 68 D-35 Piso 5
Ciudad	Bogotá D.C.

Radicación: 01098902

JRE/alqr

Fuente: Superintendencia de Industria y Comercio

Anexo F Resolución N°. 28012 (12/11/2004) superintendencia de industria y comercio pagina 1 de 2



REPÚBLICA DE COLOMBIA No.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 28012 **DE 2004**
(12 NOV. 2004)

Por la cual se amplía el alcance de la autorización a una entidad de certificación abierta

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

En ejercicio de sus facultades legales, en especial las conferidas en el artículo 41 de la Ley 527 de 1999, los decretos 2153 de 1992 y 1747 de 2000 y el Capítulo VIII del Título V de la Circular Única, y

CONSIDERANDO

PRIMERO. Que mediante comunicación radicada en esta Superintendencia el 31 de agosto de 2004 bajo el número 01098902-00050000, el señor Bernardo Vanegas Luque, en su calidad de representante legal de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., solicitó la ampliación del alcance de la acreditación concedida mediante resolución 1007 del 24 de enero de 2002 como Entidad de Certificación Abierta.

SEGUNDO. Que revisada la documentación correspondiente, se constató que la sociedad CERTICAMARA S.A., no adjuntó el informe de auditoría.

TERCERO. Que mediante comunicación radicada el 04 de Noviembre de 2004 bajo el número 04085113, el representante legal de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., dio alcance a la solicitud inicial, anexando copia del informe de auditoria para el nuevo servicio, realizado por la firma Ernst & Young - España, dando así cumplimiento a los requisitos establecidos en el artículo 3 del decreto 1747 de 2000 y en el numeral 8.2.2 del Capítulo VIII del Título V de la Circular Única No. 10 de 2001 de la Superintendencia de Industria y Comercio.

En mérito de lo expuesto este Despacho,

RESUELVE

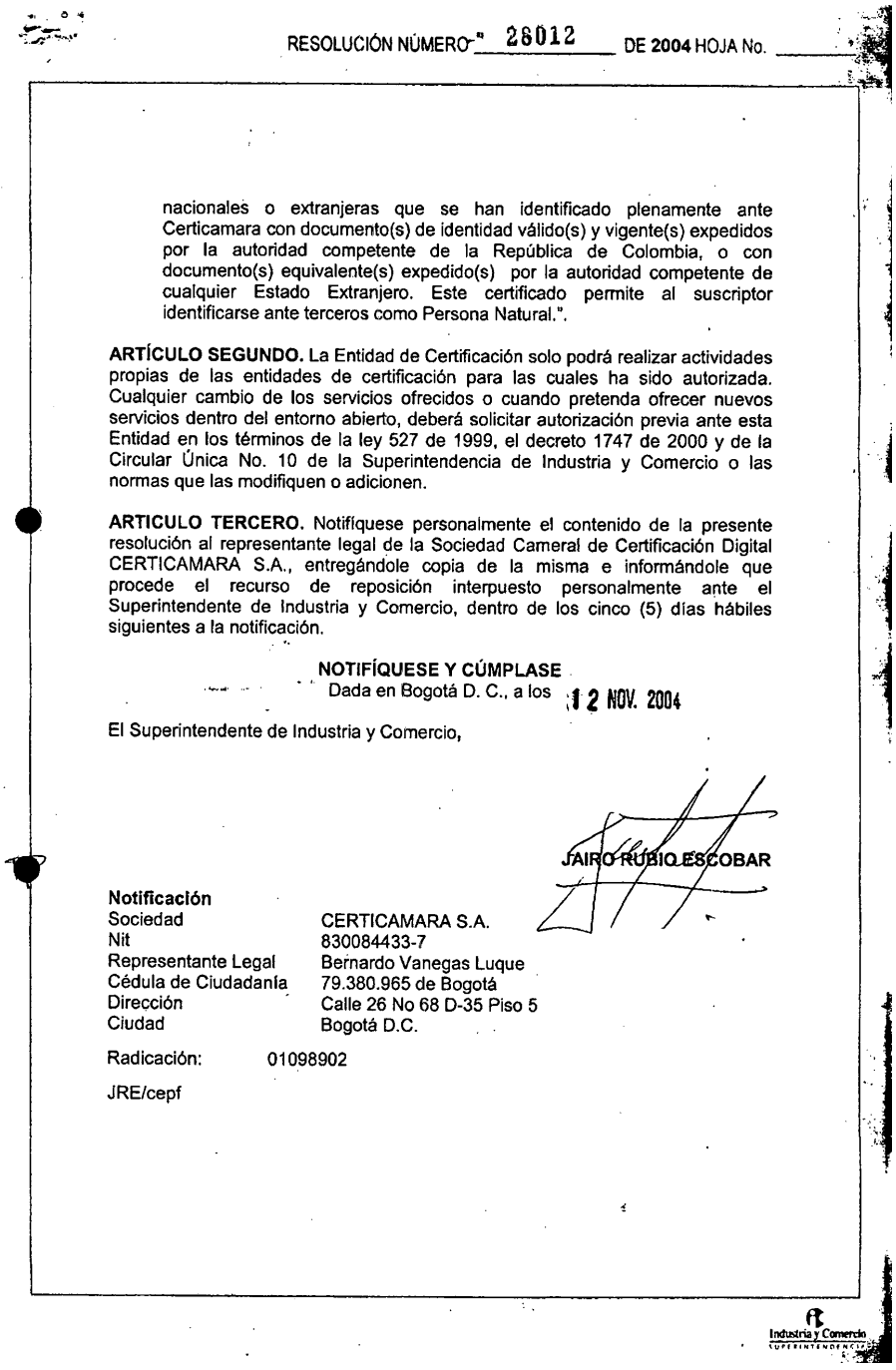
ARTÍCULO PRIMERO. Autorizar a la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., con NIT No. 830.084433-7 para ofrecer el nuevo servicio de generación de certificados digitales como entidad de certificación abierta en todo el territorio Nacional, que se indica a continuación:

"**Certificado digital persona natural**. Se expide a personas naturales

Industria y Comercio
SUPERINTENDENCIA
28012

Fuente: Superintendencia de Industria y Comercio

Resolución N°. 28012 (12/11/2004) superintendencia de industria y comercio pagina 2 de 2



RESOLUCIÓN NÚMERO 28012 DE 2004 HOJA No. _____

nacionales o extranjeras que se han identificado plenamente ante Certicamara con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero. Este certificado permite al suscriptor identificarse ante terceros como Persona Natural.".

ARTÍCULO SEGUNDO. La Entidad de Certificación solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Cualquier cambio de los servicios ofrecidos o cuando pretenda ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta Entidad en los términos de la ley 527 de 1999, el decreto 1747 de 2000 y de la Circular Única No. 10 de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTICULO TERCERO. Notifíquese personalmente el contenido de la presente resolución al representante legal de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., entregándole copia de la misma e informándole que procede el recurso de reposición interpuesto personalmente ante el Superintendente de Industria y Comercio, dentro de los cinco (5) días hábiles siguientes a la notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., a los 12 NOV. 2004

El Superintendente de Industria y Comercio,

JAIRO RUBIO ESCOBAR

Notificación

Sociedad	CERTICAMARA S.A.
Nit	830084433-7
Representante Legal	Bernardo Vanegas Luque
Cédula de Ciudadanía	79.380.965 de Bogotá
Dirección	Calle 26 No 68 D-35 Piso 5
Ciudad	Bogotá D.C.

Radicación: 01098902

JRE/cepf

Industria y Comercio
SUPERINTENDENCIA

Fuente: Superintendencia de Industria y Comercio

Anexo G Resolución N°. 9887 (12/04/2007) superintendencia de industria y comercio pagina 1 de 2

REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 9887
(13 ABR. 2007)

Por la cual se amplia el alcance de la autorización a una entidad de certificación abierta

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO (E)

En ejercicio de sus facultades legales, en especial las que se le confirieron en la ley 527 de 1999, los decretos 2153 de 1992, 1747 de 2000, y

CONSIDERANDO

PRIMERO. Que mediante comunicación radicada en esta Superintendencia el 30 de octubre del año 2006 bajo el número 01098902, el doctor Bernardo Vanegas Luque, en su calidad de representante legal de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., solicitó la ampliación del alcance de la acreditación concedida mediante resolución 1007 del 24 de enero de 2002 y 28012 del 12 de noviembre de 2004 como entidad de Certificación abierta.

SEGUNDO. Que una vez revisada la documentación anexa a la solicitud de ampliación del alcance de la autorización, esta Superintendencia ordenó una visita de evaluación en las instalaciones de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A, ubicadas en la Avenida Calle 26 No 68D-35 de la ciudad de Bogotá, la cual se llevó a cabo el 11 de diciembre del año 2006.

TERCERO. Que el resultado del informe rendido por los evaluadores comisionados, de fecha 22 de diciembre del año 2006, permitió concluir que la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., cumple con los requisitos señalados en la ley 527 de 1999, el decreto 1747 de 2000 y el capitulo VIII del titulo V de la Circular Única No. 10 de 2001 de la Superintendencia de Industria y Comercio.

En merito de lo expuesto este Despacho,

RESUELVE:

ARTÍCULO PRIMERO. Autorizar a la Sociedad Cameral de Certificación Digital CERTICAMARA S.A, con Nit No 830.084433-7, para ofrecer el nuevo servicio de estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

ARTÍCULO SEGUNDO. La Entidad de certificación solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Cualquier cambio de los servicios ofrecidos o cuando pretenda ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta entidad en los terminos de la ley 527

Fuente: Superintendencia de Industria y Comercio

Resolución N°. 9887 (12/04/2007) superintendencia de industria y comercio pagina 2 de 2

RESOLUCION NUMERO 9887 **Hoja N°. 2**

Por la cual se amplia el alcance de la autorización a una entidad de certificación abierta

de 1999, el decreto 1747 de 2000 y de la Circular Única No. 10 de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTÍCULO TERCERO. Notifíquese personalmente el contenido de la presente resolución al representante legal del la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., entregándole copia de la misma e informándole que procede el recurso de reposición interpuesto personalmente ante el Superintendente de Industria y Comercio, en el acto de notificación o dentro de los cinco (5) días hábiles siguientes a la notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 13 ABR. 2007

El Superintendente de Industria y Comercio (e),

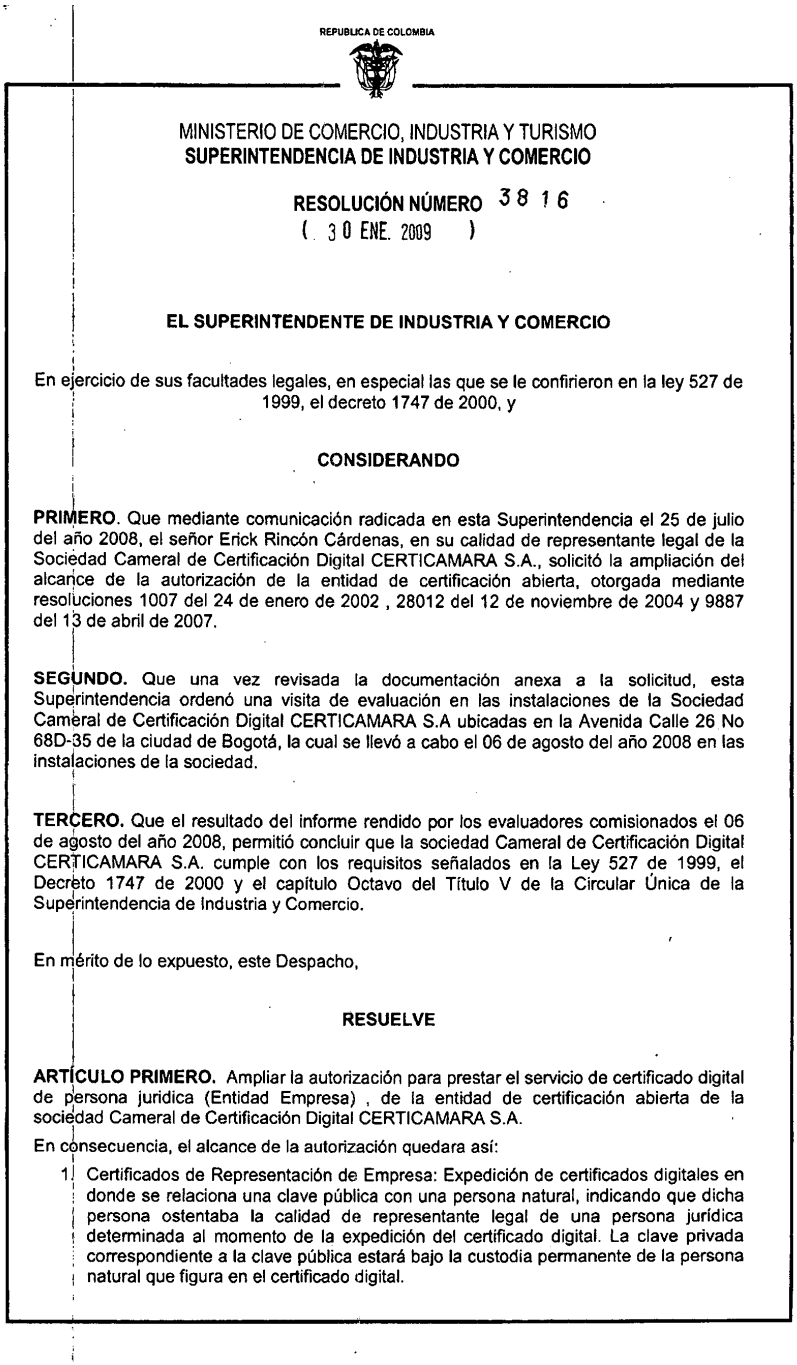
GIANCARLO MARCENARO JIMENEZ

Notificación

Entidad:	Sociedad Cameral de Certificación Digital CERTICAMARA S.A
Nit.:	830084433-7
Representante Legal:	Bernardo Vanegas Luque
Cédula:	79'380.965 de Bogotá
Dirección:	Avenida Calle 26 No 68D-35
Ciudad:	Bogotá, D.C.
Radicación	01098902

Fuente: Superintendencia de industria y comercio

Anexo H Resolución N°. 3816 (30/01/2009) superintendencia de industria y comercio pagina 1 de 2



REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 3816
(30 ENE. 2009)

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

En ejercicio de sus facultades legales, en especial las que se le confirieron en la ley 527 de 1999, el decreto 1747 de 2000, y

CONSIDERANDO

PRIMERO. Que mediante comunicación radicada en esta Superintendencia el 25 de julio del año 2008, el señor Erick Rincón Cárdenas, en su calidad de representante legal de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A., solicitó la ampliación del alcance de la autorización de la entidad de certificación abierta, otorgada mediante resoluciones 1007 del 24 de enero de 2002 , 28012 del 12 de noviembre de 2004 y 9887 del 13 de abril de 2007.

SEGUNDO. Que una vez revisada la documentación anexa a la solicitud, esta Superintendencia ordenó una visita de evaluación en las instalaciones de la Sociedad Cameral de Certificación Digital CERTICAMARA S.A ubicadas en la Avenida Calle 26 No 68D-35 de la ciudad de Bogotá, la cual se llevó a cabo el 06 de agosto del año 2008 en las instalaciones de la sociedad.

TERCERO. Que el resultado del informe rendido por los evaluadores comisionados el 06 de agosto del año 2008, permitió concluir que la sociedad Cameral de Certificación Digital CERTICAMARA S.A. cumple con los requisitos señalados en la Ley 527 de 1999, el Decreto 1747 de 2000 y el capítulo Octavo del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

En mérito de lo expuesto, este Despacho,

RESUELVE

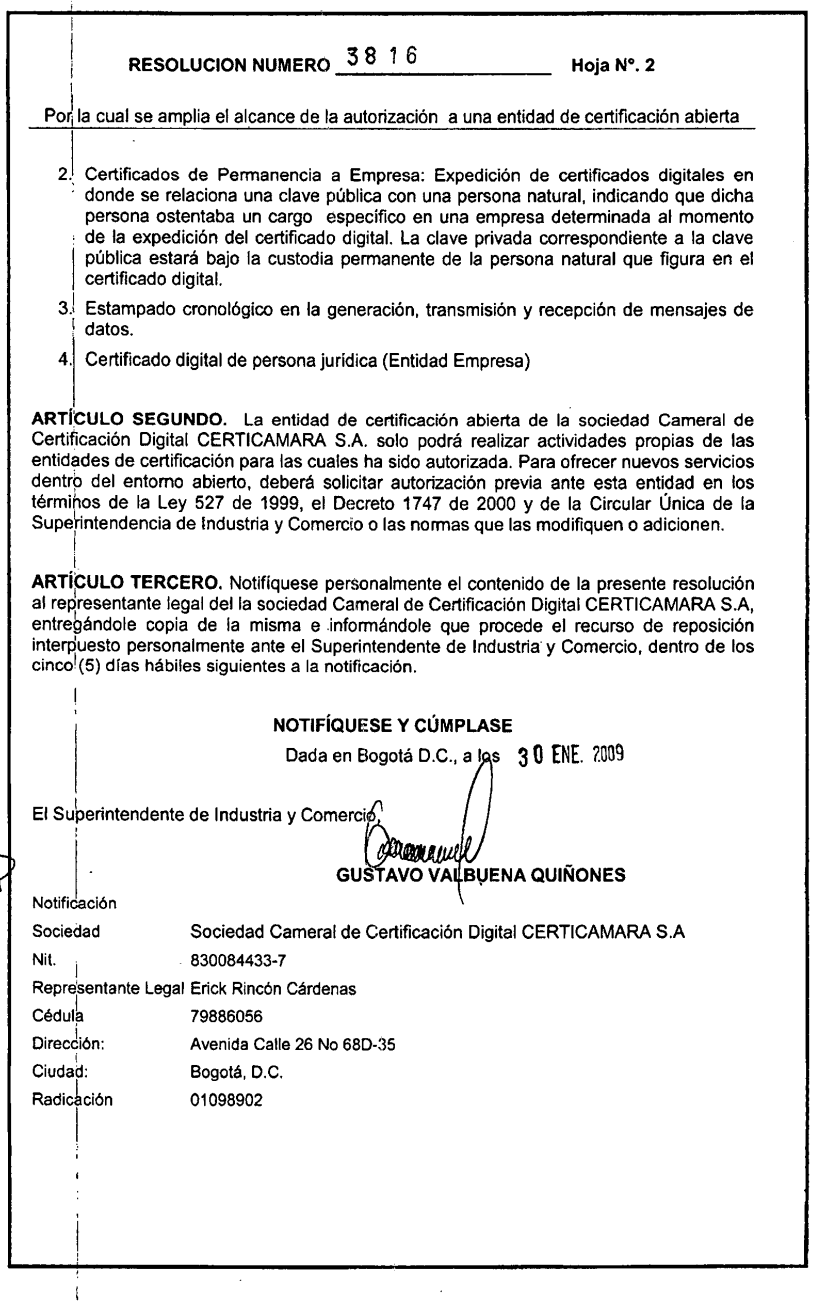
ARTÍCULO PRIMERO. Ampliar la autorización para prestar el servicio de certificado digital de persona jurídica (Entidad Empresa) , de la entidad de certificación abierta de la sociedad Cameral de Certificación Digital CERTICAMARA S.A.

En consecuencia, el alcance de la autorización quedara así:

1. Certificados de Representación de Empresa: Expedición de certificados digitales en donde se relaciona una clave pública con una persona natural, indicando que dicha persona ostentaba la calidad de representante legal de una persona jurídica determinada al momento de la expedición del certificado digital. La clave privada correspondiente a la clave pública estará bajo la custodia permanente de la persona natural que figura en el certificado digital.

Fuente: Superintendencia de Industria y Comercio

Resolución N°. 3816 (30/01/2009) superintendencia de industria y comercio pagina 2 de 2



RESOLUCION NUMERO 3816 **Hoja N°. 2**

Por la cual se amplia el alcance de la autorización a una entidad de certificación abierta

2. Certificados de Permanencia a Empresa: Expedición de certificados digitales en donde se relaciona una clave pública con una persona natural, indicando que dicha persona ostentaba un cargo específico en una empresa determinada al momento de la expedición del certificado digital. La clave privada correspondiente a la clave pública estará bajo la custodia permanente de la persona natural que figura en el certificado digital.
3. Estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
4. Certificado digital de persona jurídica (Entidad Empresa)

ARTÍCULO SEGUNDO. La entidad de certificación abierta de la sociedad Cameral de Certificación Digital CERTICAMARA S.A. solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Para ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta entidad en los términos de la Ley 527 de 1999, el Decreto 1747 de 2000 y de la Circular Única de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTÍCULO TERCERO. Notifíquese personalmente el contenido de la presente resolución al representante legal del la sociedad Cameral de Certificación Digital CERTICAMARA S.A, entregándole copia de la misma e informándole que procede el recurso de reposición interpuesto personalmente ante el Superintendente de Industria y Comercio, dentro de los cinco (5) días hábiles siguientes a la notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 30 ENE. 2009

El Superintendente de Industria y Comercio,

GUSTAVO VALBUENA QUIÑONES

Notificación	
Sociedad	Sociedad Cameral de Certificación Digital CERTICAMARA S.A
Nit.	830084433-7
Representante Legal	Erick Rincón Cárdenas
Cédula	79886056
Dirección:	Avenida Calle 26 No 68D-35
Ciudad:	Bogotá, D.C.
Radicación	01098902

Fuente: Superintendencia de industria y comercio

Anexo I Resolución N°. 23344 del 2 de mayo de 2009 superintendencia de industria y comercio pagina 1 de 2

REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 23344
(12 MAYO 2009)

Por la cual se concede la autorización a una entidad de certificación abierta

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

En ejercicio de sus facultades legales, en especial las que se le confirieron en la Ley 527 de 1999, el Decreto 1747 de 2000, y

CONSIDERANDO

PRIMERO. Que mediante comunicación radicada en esta Superintendencia el 06 de noviembre del año 2008 bajo el número 08118413, el señor Hugo Alejandro Saavedra León, en su calidad de representante legal de la sociedad GESTIÒN DE SEGURIDAD ELECTRÒNICA S.A GSE S.A., solicitó la autorización para su entidad de Certificación abierta.

SEGUNDO. Que una vez revisada la documentación anexa a la solicitud de autorización, esta Superintendencia ordenó una visita de evaluación en las instalaciones de la sociedad GESTIÒN DE SEGURIDAD ELECTRÒNICA S.A GSE S.A. ubicadas en la Carrera 21A No 124 -55 Oficina 303 de la ciudad de Bogotá, la cual se llevó a cabo los dias 27 de febrero y 20 de marzo de 2009.

TERCERO. Que el resultado del informe rendido por los evaluadores comisionados el 27 de abril del año 2009, permitió concluir que la entidad de certificación abierta de la sociedad GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A GSE S.A., cumple con los requisitos señalados en la Ley 527 de 1999, Decreto 1747 de 2000 y el Capítulo VIII del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO. Autorizar a la entidad de certificación abierta de la sociedad GESTIÒN DE SEGURIDAD ELECTRÒNICA S.A GSE S.A., identificada con Nit No. 900.204.272-8 para ofrecer los siguientes servicios:

Servicios de emisión de Certificado de Pertenencia Empresa
Servicios de emisión de Certificado de Representación Empresa
Servicios de emisión de Certificado de Función Pública

Fuente: Superintendencia de Industria y Comercio

RESOLUCION NUMERO 23344 **Hoja N°. 2**

Por la cual se concede la autorización a una entidad de certificación abierta

Servicios de emisión de Certificado de Profesional Titulado

Servicios de emisión de Certificado de Persona Natural

Servicios de emisión de Certificado de Factura Electrónica

ARTÍCULO SEGUNDO. La entidad de certificación abierta de la sociedad GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A GSE S.A., solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Cualquier cambio de los servicios ofrecidos o cuando pretenda ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta entidad en los términos de la Ley 527 de 1999, el Decreto 1747 de 2000 y de la Circular Única de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTÍCULO TERCERO. Notifíquese personalmente el contenido de la presente resolución a la representante legal de la sociedad GESTION DE SEGURIDAD ELECTRONICA S.A GSE S.A., entregándole copia de la misma e informándole que procede el recurso de reposición interpuesto personalmente ante el Superintendente de Industria y Comercio, dentro de los cinco (5) días hábiles siguientes a la notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 12 MAYO 2009

El Superintendente de Industria y Comercio,

GUSTAVO VALBUENA QUIÑONES

Notificación

Entidad	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A GSE S.A.
Nit.	900.204.272-8
Representante Legal	Hugo Alejandro Saavedra León
Cédula	19.490.950
Dirección:	Carrera 21 A No 124-55 Oficina 303
Ciudad:	Bogotá, D.C.
Radicación	08-118413

Fuente: Superintendencia de industria y comercio

Anexo J Resolución N°. 1194 (21/01/2010) superintendencia de industria y comercio pagina 1 de 2

REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 1194
(21 ENE. 2010)

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

En ejercicio de sus facultades legales, en especial las que se le confirieron en la ley 527 de 1999, el decreto 1747 de 2000, y

CONSIDERANDO

PRIMERO. Que mediante comunicación radicada en esta Superintendencia el 30 de octubre del año 2009, el señor Felipe Sánchez Ireguí, en su calidad de representante legal de la Sociedad Gestión de Seguridad Electronica S.A – GSE S.A., solicitó la ampliación del alcance de la autorización de la entidad de certificación abierta, otorgada mediante resolucion 23344 del 12 de mayo de 2009.

SEGUNDO. Que una vez revisada la documentación anexa a la solicitud, esta Superintendencia ordenó una visita de evaluación en las instalaciones de la Sociedad Gestión de Seguridad Electronica S.A – GSE S.A., ubicadas en la Calle 118 No 19-52 Oficina 504-de la ciudad de Bogotá, la cual se llevó a cabo el 09 de diciembre del año 2009 en las instalaciones de la sociedad.

TERCERO. Que el resultado del informe rendido por los evaluadores comisionados el 18 de diciembre del año 2009, permitió concluir que la Sociedad Gestión de Seguridad Electronica S.A – GSE S.A., cumple con los requisitos señalados en la Ley 527 de 1999, el Decreto 1747 de 2000 y el capitulo Octavo del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO. Ampliar la autorización para prestar el servicio de estampado cronológico, de la entidad de certificación abierta de la Sociedad Gestión de Seguridad Electronica S.A – GSE S.A.,

En consecuencia, el alcance de la autorización quedara así:

- Servicio de emisión de certificado de pertenencia empresa
- Servicio de emisión de certificado de representación empresa
- Servicio de emisión de certificado de función pública
- Servicio de emisión de certificado de profesional titulado
- Servicio de emisión de certificado de persona natural

Fuente: Superintendencia de Industria y Comercio

Resolución N°. 1194 (21/01/2010) superintendencia de industria y comercio pagina 2 de 2

RESOLUCION NUMERO 1194 **Hoja N°. 2**

Por la cual se amplia el alcance de la autorización a una entidad de certificación abierta

- Servicio de emisión de certificado de factura electrónica
* Servicio de estampado cronológico

NOTA *Corresponde al servicio ampliado

ARTÍCULO SEGUNDO. La entidad de certificación abierta de la Sociedad Gestión de Seguridad Electronica S.A – GSE S.A., solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Para ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta entidad en los términos de la Ley 527 de 1999, el Decreto 1747 de 2000 y de la Circular Única de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTÍCULO TERCERO. Notifíquese personalmente el contenido de la presente resolución al representante legal de la Sociedad Gestión de Seguridad Electronica S.A – GSE S.A., entregándole copia de la misma e informándole que procede el recurso de reposición interpuesto personalmente ante el Superintendente de Industria y Comercio, dentro de los cinco (5) días hábiles siguientes a la notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 21 ENE. 2010

El Superintendente de Industria y Comercio,

GUSTAVO VALBUENA QUIÑONES

Notificación	
Sociedad	Gestión de Seguridad Electrónica S.A. GSE S.A.
Nit.	900204272-8
Representante Legal	Hugo Alejandro Saavedra León
Cédula	19490950
Dirección:	Calle 118 No 19-52 Oficina 504
Ciudad:	Bogotá, D.C.
Radicación	08118413

Fuente: Superintendencia de industria y comercio

Anexo K Resolución 14349 del 23 de marzo de 2002 superintendencia de industria y comercio pagina 1 de 4

REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 14349 1
(23 MAR 2011)

Por la cual se concede la autorización a entidad de certificación abierta

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DEL CONSUMIDOR Y METROLOGÍA

En ejercicio de sus facultades legales, en especial las que se le confirieron en la Ley 527 de 1999, el Decreto 1747 de 2000 y en el numeral 11 del artículo 9 del Decreto 3523 de 2009 y

CONSIDERANDO

PRIMERO: Que mediante comunicación radicada en esta Superintendencia el 01 de diciembre de 2010 con el número 10-151334, el señor Juan David Castillo Garcia, en su calidad de representante legal de la sociedad ANDES SERVICIO DE CERTIFICACIÓN DIGITAL S.A. ANDES SCD, en adelante ANDES SCD, presentó solicitud de autorización para prestar servicios como Entidad de Certificación Abierta en el territorio nacional.

SEGUNDO: Que con la solicitud de autorización se allegó la documentación correspondiente, en cumplimiento de los requisitos previstos en La Ley 527 de 1999, el Decreto 1747 de 2000 y en el Capítulo VIII del Título V de la Circular Única de la Superintendencia de Industria y Comercio, para ser objeto de evaluación.

TERCERO: Que el artículo 29 de la Ley 527 de 1999, establece las características y requerimientos de las entidades de certificación, para obtener la autorización por parte de la Superintendencia de Industria y Comercio:

> *"a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;*
> *b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;*
> *c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo periodo que la ley penal o administrativa señale para el efecto."*

CUARTO: Que mediante oficio radicado con el No. 10-151334 del 7 de enero de 2011, este Despacho remitió un requerimiento de información a la sociedad ANDES SCD, con el fin de que allegara la información relacionada con el cumplimiento de los requisitos necesarios para la evaluación de la solicitud de autorización como Entidad de Certificación, que no fue aportada inicialmente.

Fuente: Superintendencia de Industria y Comercio

RESOLUCION NUMERO 14349 23 MAR 2011 Hoja N°. 2

Por la cual se concede la autorización a una entidad de certificación abierta

QUINTO: Que mediante comunicación del 14 de enero de 2011, la sociedad ANDES SCD a través de su representante legal contestó el requerimiento, allegando para tal efecto la información solicitada.

SEXTO: Que el 2 de febrero de 2011 esta Superintendencia realizó a través de los funcionarios asignados, una visita a las instalaciones de la sociedad ANDES SCD en la ciudad de Bogotá D.C., con el fin de verificar los aspectos legales, técnicos, económicos y de funcionamiento del esquema de operación del modelo de certificación de la Entidad solicitante. Durante el transcurso de la diligencia se requirió una información la cual fue allegada por la sociedad ANDES SCD el 9 de febrero de 2011.

SÉPTIMO: Que el 21 de febrero de 2011, esta Superintendencia a través de sus funcionarios delegados, realizó una visita a las instalaciones de la Entidad solicitante, que incluyó una inspección a la infraestructura computacional en el Data Center Triara de la sociedad TELMEX COLOMBIA S.A., de conformidad con el documento de solicitud de autorización.

OCTAVO: Que el 3 de marzo del presente año, la Entidad solicitante a través de su representante legal, dio alcance a la solicitud de autorización, incluyendo para tal efecto las modificaciones al documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.

NOVENO: Que el 4 de marzo de 2011 esta Superintendencia realizó a través de los funcionarios asignados una visita a una de las instalaciones de la sociedad ANDES SCD ubicada en la ciudad de Bucaramanga, con el fin de verificar los aspectos legales, técnicos, económicos y de funcionamiento del esquema de operación del modelo de certificación de la Entidad solicitante, de conformidad con el documento de solicitud de autorización.

Durante el transcurso de la diligencia se requirió una información la cual fue allegada por la sociedad ANDES SCD el 11 de marzo de 2011.

DÉCIMO: Que la Entidad solicitante presentó el correspondiente Informe de auditoría inicial satisfactorio, en el cual se dictamina que la sociedad ANDES SCD está en capacidad de actuar de acuerdo con los requerimientos de la ley 527 de 1999, lo previsto en el decreto 1747 de 2000 y la Circular Única de la Superintendencia de Industria y Comercio.

DECIMOPRIMERO: Que el numeral 11 del artículo 9 del Decreto 3523 de 2009, establece que es función del Superintendente Delegado para la Protección del Consumidor y Metrología, autorizar las entidades de certificación para prestar sus servicios en el país, de acuerdo con lo previsto en la Ley 527 de 1999 y ejercer respecto de éstas las funciones previstas en dicha ley o en las demás normas que la modifiquen o adicionen.

DECIMOSEGUNDO: Que de conformidad con la información allegada al trámite administrativo, se considera que la sociedad ANDES SCD, dio cumplimiento a los requerimientos señalados en la Ley 527 de 1999, acreditó el cumplimiento de los requisitos señalados en el artículo 5° del Decreto 1747 de 2000 y en el Capítulo VIII del Título V de la Circular Única de la Superintendencia de Industria y Comercio y por tal motivo deberá procederse a otorgarle la autorización.

En mérito de lo expuesto, este Despacho,

Fuente: Superintendencia de Industria y Comercio

RESOLUCION NUMERO 14349 Hoja N°. 3

Por la cual se concede la autorización a una entidad de certificación abierta

RESUELVE

ARTÍCULO PRIMERO. Autorizar a la sociedad ANDES SERVICIO DE CERTIFICACIÓN DIGITAL S.A. ANDES SCD, identificada con Nit No. 900210800-1, para realizar las siguientes actividades como Entidad de Certificación Abierta en el país:

- Servicios de emisión de certificados digitales para acreditar la identidad y condición del suscriptor ante terceros mediante:

  - Certificados personales (Persona Natural)
  - Certificado de Profesional Titulado
  - Certificado de Miembro de Comunidad Académica
  - Certificado de Pertenencia a Empresa
  - Certificado de Representante Legal

PARÁGRAFO: La sociedad ANDES SCD, deberá cumplir los deberes previstos en el artículo 32 de la Ley 527 de 1999 y 13 del Decreto 1747 de 2000, en relación con el servicio de emisión de certificados en relación con las firmas digitales de personas naturales o jurídicas, para el cual está siendo autorizado.

ARTICULO SEGUNDO: La Sociedad ANDES SERVICIO DE CERTIFICACIÓN DIGITAL S.A. ANDES SCD, como Entidad de Certificación abierta, solo podrá realizar actividades propias de las entidades de certificación para las cuales ha sido autorizada. Cualquier cambio de los servicios ofrecidos o cuando pretenda ofrecer nuevos servicios dentro del entorno abierto, deberá solicitar autorización previa ante esta entidad en los términos de la Ley 527 de 1999, el Decreto 1747 de 2000 y de la Circular Única de la Superintendencia de Industria y Comercio o las normas que las modifiquen o adicionen.

ARTÍCULO TERCERO. Notifíquese personalmente el contenido de la presente resolución al representante legal de la sociedad ANDES SERVICIO DE CERTIFICACIÓN DIGITAL S.A. ANDES SCD, entregándole copia de la misma e informándole que procede el recurso de reposición interpuesto personalmente ante el Superintendente Delegado de Protección del Consumidor y Metrología y de apelación ante el Superintendente de Industria y Comercio, dentro de los cinco (5) días hábiles siguientes a la notificación.

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., a los 23 MAR 2011

El Superintendente Delegado para la Protección del Consumidor y Metrología,

ALEJANDRO GIRALDO LÓPEZ

Fuente: Superintendencia de Industria y Comercio

Resolución 14349 del 23 de marzo de 2002 superintendencia de industria y comercio pagina 4 de 4

RESOLUCION NUMERO 14349 23 MAR 2011 Hoja N°. 4

Por la cual se concede la autorización a una entidad de certificación abierta

Notificación

Entidad	:	ANDES SERVICIO DE CERTIFICACIÓN DIGITAL S.A. ANDES SCD
Nit.	:	900210800-1
Representante Legal	:	JUAN DAVID CASTILLO GARCIA
Cédula	:	79.687.441
Dirección:	:	Calle 26 A No. 13 – 97 Oficina 703
Ciudad:	:	Bogotá, D.C.
Radicación	:	10-151334

AGL/Jemh/Jfic

Fuente: Superintendencia de industria y comercio

Guía de Implementación y Uso de Certificados y Firmas Digitales para las MIPYMES que Permitan Garantizar Integridad, Autenticidad y No Repudio en los Documentos Electrónicos

Castillo Penagos, William Francisco, Correa Cortes, Hair Diyosset y Muñoz Silva, Jorge Enrique.
liloo6retug@gmail.com, diyocorrea@gmail.com, joenmusi@gmail.com
Universidad Piloto de Colombia

Resumen—Los diferentes tipos de transacciones electrónicas ofrecen beneficios como reducción de tiempos, costos de operación, eliminación de las distancias y hasta las fronteras geográficas, pero a su vez representan riesgos que deben ser tratados mediante herramientas ofrecidas actualmente por la criptografía como lo son los certificados y firmas y digitales, que protegen y aseguran tanto los sitios web que ofrecen cualquier tipo de transacción electrónica como los diferentes archivos de usuario en formato electrónico que soportan las mismas los que poseen valor probatorio y requieren que se garantice su confidencialidad, integridad, autenticidad y no repudio.

Abstrac—The different types of electronic transactions offer benefits such as reduced time, cost of operation, elimination of distances and even geographical boundaries, but in turn represent risks that must be addressed by tools currently offered by cryptography such as certificates and and digital signatures, which both protect and secure websites that offer any type of electronic transaction as different user files in electronic format supporting those who have the same probative value and need to ensure confidentiality, integrity, authenticity and non-repudiation.

Índice de Términos—Certificado digital, Cifrado, Comercio electrónico, Confidencialidad, Criptografía, Disponibilidad, Documento electrónico, Firma digital, Integridad, No Repudio.

I. Introducción

La constante evolución de las nuevas tecnologías que ofrecen un universo de posibilidades para la realización de todo tipo transacciones electrónicas, las cuales se han incrementado y esa tendencia es cada vez más creciente, de aquí que el concepto e integración de firma digital son necesarios para garantizar la autenticidad, la integridad y el no repudio de dichas transacciones a través de medios de transmisión no seguros como internet, que a su vez, representa nuevos riesgos y constantes amenazas que hoy en día se logran tipificar como delitos informáticos que afectan derechos consagrados en la constitución colombiana, como lo es, la intimidad.

Los diferentes tipos de transacciones electrónicas brindan beneficios como reducción de tiempos, costos de operación, eliminación de las distancias y hasta las fronteras geográficas, pero a su vez, representan riesgos que deben ser tratados mediante herramientas ofrecidas actualmente por la criptografía, como lo son los certificados y firmas digitales, que protegen y aseguran tanto los sitios web que prestan cualquier tipo de transacción electrónica como los diferentes archivos de usuario en formato electrónico que soportan las mismas, los que poseen valor probatorio y requieren que se garantice su confidencialidad, integridad, autenticidad y no repudio.

II. Justificación

Los constantes avances en la tecnología representan riesgos inherentes a los ambientes digitales, que se evidencian en las nuevas modalidades de delitos informáticos como el Fishing, la suplantación de identidad, interceptación (Eavesdropping) sobre medios de información tanto cifrada como no cifrada, entre otros. Surgen todo un nuevo mundo para los ciber delincuentes que tienen motivaciones como la ausencia de daños a su

integridad física, ingenuidad de los usuarios y la falta de seguridad; quienes no solo buscan motivaciones económicas y pueden mediante diversas modalidades delictivas lograr afectación a la integridad, autenticidad y no repudio de la información.

La firma digital ofrece ventajas inmejorables como la reducción del riesgo legal mediante ahorro de largas, complejas e inciertas etapas probatorias en trámites judiciales y administrativos para demostrar que la firma electrónica es efectivamente equivalente, se evitan desplazamientos y colas de las personas involucradas en los procesos de firma, los documentos firmados pueden recogerse y archivarse en formato digital, sin tener que trasladarse nunca al papel, la distancia deja de ser un problema, por lo que cualquier documento quedará firmado por todas las partes, mucho más rápidamente, y de forma más eficiente que si se firmara a mano, al quedar archivados en formato digital, su posterior localización también es mucho más fácil y rápida, gracias a las herramientas informáticas de búsqueda, es una tecnología más segura que la firma manuscrita, por lo que suplantar una identidad resulta mucho más complejo, ahorros de costes tangibles, evitando envíos, o reduciendo el consumo de tinta o papel.

III. Planteamiento del problema

¿Cómo garantizar la integridad, autenticidad y no repudio de los archivos en formatos digitales generados por las Micro, Pequeñas y Medianas Empresas (MiPymes) del departamento de Casanare que formen parte del proyecto "ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE" en desarrollo por parte de La Cámara de Comercio de Casanare e Imagina Soluciones S.A.S.?.

IV. Objetivo general

Elaborar una guía de implementación y uso de certificados y firmas digitales para archivos en formatos digitales generados por las Micro, Pequeñas y Medianas Empresas (MiPymes) del departamento de Casanare pertenecientes al proyecto "ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE" en desarrollo por parte de La Cámara de Comercio de Casanare e Imagina Soluciones S.A.S.

A. OBJETIVOS ESPECÍFICOS

- Capturar los requerimientos técnicos para la implementación de certificados y firmas digitales.
- Establecer el contexto jurídico para la implementación de certificados y firmas digitales en Colombia.
- Ejecutar una estrategia de capacitaciones que permitan fortalecer las capacidades en el uso de certificados y firmas digitales.
- Crear y ejecutar pruebas piloto para evaluar la guía de implementación de certificados y firmas digitales.

V. Tipos de certificados

A. Certificado digital de función pública

Este certificado se expide a una persona que ejerce un cargo de carácter público.

B. Certificado digital de representación legal

Este certificado se expide a un representante legal principal o suplente de una sociedad o empresa.

C. Certificado digital de pertenencia a empresa

Este certificado se expide a la persona que demuestra pertenecer a una empresa.

D. Certificado digital de profesional titulado

Este certificado se expide a las personas que demuestran haber obtenido un título profesional.

E. Certificado digital de persona natural

Certificado expedido a cualquier persona natural. Solo certifica su identidad.

F. Certificado digital SSL

Este certificado se emite para instalar en un servidor web y brinda una seguridad técnica de la comunicación que se establece con este.

G. Certificado digital de firma de código

El certificado de firma se emite a las casas desarrolladores de software y da fe de la autenticidad de las piezas de código y confiabilidad a nivel de componentes de software para instalación dentro de un sistema operativo y dar fe de su origen.

H. Certificado digital de persona jurídica

Este certificado se emite a una razón social específica. Toda la carga legal y probatoria asociada a este certificado recaerá sobre el representante legal de la entidad a la cual se emite.

VI. Obtención de certificados de firma digital

Para la obtención de los certificados de firma digital, el procedimiento se debe seguir ante una autoridad de certificación digital autorizada por la Organización Nacional de Acreditación (ONEC). Las etapas para la obtención del certificado son:

A. Generación de certificado de firma digital

En la página de internet suministrada por la entidad de certificación encontrará un formulario con el que podrá hacer la generación y descarga del certificado de firma digital en formato “p12”8. PKCS#12 “Este estándar especifica un formato portátil para transportar llaves privadas de un usuario”.

B. Instalación de certificado de firma digital

En el equipo de cómputo procederá a realizar la instalación del certificado de firma digital, el asistente solicitará la contraseña del certificado de firma digital, el cual fue asignado al momento de la generación y que protege la información de identificación aquí contenida, adicionalmente debemos digitar una contraseña de protección de la llave privada y confirmarla. Esta contraseña será solicitada cada vez que se desee firmar digitalmente o cifrar empleando la llave privada correspondiente al certificado digital

C. Instalación de certificado raíz

En el equipo de cómputo se procederá a realizar la instalación del certificado raíz emitido por la entidad de certificación y son los que dan confianza al certificado de usuario generado anteriormente.

VII. Firma digital

Con el objetivo de incentivar el uso de las nuevas tecnologías, sus beneficios y así mismo contrarrestar los riesgos inherentes a los constantes avances y nuevos desarrollos de la misma, las firmas digitales son una herramienta fundamental en el comercio electrónico de hoy y soporte para todas las transacciones electrónicas con total validez y valor probatorio, NO por ello implica el contar con conocimientos avanzados para su adecuado uso, a continuación se desarrollan los pasos para realizar la instalación de las herramientas software necesarias y los pasos para ejecutar la firma digital sobre todos los documentos electrónicos que así lo requieran.

VIII. Herramientas software para firma digital

A. Certitool

Es una herramienta desarrollada por CERTICÁMARA con el objetivo de realizar la firma digital de documentos electrónicos.

B. Xolidosign

Herramienta gratuita utilizada para la firma electrónica y el sellado de tiempo para asegurar la identidad del firmante y garantizar que tus documentos no han sido modificados desde su firma o sellado.

C. Andes Signer

Es una herramienta desarrollada por AndesSCD (Andes Servicios de Certificación Digital) con el objetivo de realizar la firma digital de documentos

electrónicos.

IX. MARCO LEGAL

En Colombia los certificados y firmas digitales están enmarcadas sobre un conjunto de leyes que se detallan a continuación:

- Ley 270 de 1996 o Ley Estatutaria de la administración de justicia, donde se establece la autorización general siempre vigente para propender por la incorporación de tecnología avanzada al servicio de la Administración de justicia, y regular los trámites judiciales y administrativos que se adelanten en los despachos judiciales, en los aspectos no previstos por el legislador.
- Ley 527 de 1999 de 18 de agosto, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales(las cuales poseen plena presunción de autenticidad amparada bajo una entidad de certificación), y se establecen las entidades de certificación y se dictan otras disposiciones, logro puntualmente la consolidación del principio de equivalencia funcional con los medios tradicionales, otorgando total validez probatoria y jurídica de los mensajes de datos, actualmente esta ley posibilita iniciar una causa ante la justicia al contar con las garantías ofrecidas por la equivalencia funcional que elimino la necesidad de estatutos especiales para este tipo de actividades.
- Ley 794 de 2003: Actos de comunicación procesal por medios electrónicos.
- Ley 962 de 2005: Actuaciones administrativas por medios electrónicos.
- Ley 1150 de 2007: Contratación del Estado por medios electrónicos.
- Decreto 1747 de 2000: reglamenta parcialmente la Ley 527 de 1999 en aspectos relacionados con las entidades de certificación, los certificados y las firmas digitales.
- Decreto 1929 de 2007: por el cual se reglamenta el artículo 616-1 del Estatuto Tributario.
- Decreto 12 de 2002: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. Este decreto asigno las funciones que tenía la Superintendencia de Industria y Comercio (SIC) en materia de entidades de certificación de firmas digitales al Organismo Nacional de Acreditación de Colombia (ONAC).
- Resolución 26930 de 2000 de la Superintendencia de Industria y Comercio: referencia los requisitos que deben cumplir las entidades de certificación abiertas o cerradas para solicitar su autorización y funcionamiento, clasificación que depende de los servicios que prestan y finalmente se desarrolla el tema de las firmas auditoras para las entidades de certificación y el contenido del informe de auditoría necesario para la autorización, el cual debe ser actualizado por lo menos anualmente.

Las entidades de certificación digital autorizadas por la SIC antes de la promulgación del decreto 12 de 2002 se encuentran establecidas mediante actos administrativos los cuales fueron suministrados por la SIC a los autores de la presente guía mediante radicado “14-187143- -4- 1” (Ver Anexo A) donde se define:

- Sociedad Cameral de Certificación Digital Certicámara, S.A., Autorizada mediante resolución N°. 1007 del 24 de enero de 2002
    - Autorización de nuevos servicios – Ampliación de la autorización
        - Resolución N°. 22456 (10/09/2004)
        - Resolución N°. 28012 (12/11/2004)
        - Resolución N°. 9887 (12/04/2007)
        - Resolución N°. 3816 (30/01/2009)
- Gestión de Seguridad Electrónica S.A. – GSE S.A., Autorizada mediante resolución N°. 23344 del 2 de mayo de 2009

    - Autorización de nuevos servicios – Ampliación de la autorización
        - Resolución N°. 1194 (21/01/2010)
- Andes Servicio de Certificación Digital S.A. – ANDES SCD, Autorizada mediante resolución 14349 del 23 de marzo de 2002

X. Conclusiones

La captura de los requerimientos técnicos permitió a los autores del proyecto establecer el ecosistema Microsoft Windows como el entorno computacional para implementación de firmas digitales, basado en las herramientas de firma digital suministradas por las entidades de certificación que solo están disponibles para esta plataforma, la de mayor uso a nivel mundial y la que adquieren la mayor cantidad de empresarios por su facilidad y simplicidad en su uso.

El establecimiento del contexto jurídico para la implementación de firmas digitales en Colombia permitió a los autores del proyecto determinar las organizaciones establecidas para la autorización de las entidades de certificación digital, adicionalmente establecer la validez probatoria y el alcance legal dado por las leyes del país a estos mecanismos criptográficos.

La ejecución de una estrategia de capacitaciones permitió a los autores del proyecto trasmitir a los empresarios la facilidad de uso y las ventajas tecnologías y legales que ofrece la implementación de certificados y firmas digitales en el desarrollo de los diferentes procesos de sus MiPymes tanto en sus actividades digitales propias, como en el desarrollo del comercio electrónico que se realizará de la mano del proyecto marco ESTRATEGIA INTERINSTITUCIONAL PARA EL FORTALECIMIENTO EMPRESARIAL, MEDIANTE EL USO Y APROPIACIÓN DE LAS TIC Y LA DISMINUCIÓN DE LA BRECHA DIGITAL EN EL DEPARTAMENTO DE CASANARE.

La creación y ejecución de pruebas piloto permitió a los autores del proyecto evaluar el producto final de este proyecto, la guía de implementación de certificados y firmas digitales que evidencio que los empresarios con conocimientos básicos y las herramientas de tecnológicas adecuadas pueden incorporar estos mecanismos criptográficos en los procesos internos y externos que desarrolle la empresa con archivos electrónicos los cuales poseen total validez legal y características matemáticas que garanticen su integridad, autenticidad y no repudio.

Referencias

[1] FUSTER SABATER, Amparo. HERNÁNDEZ ENCINAS, Luis. MARTIN MUÑOZ, Agustín. MONTOYA VITINI, Fausto. MUÑOZ MASQUE. Jaime. Criptografía protección de datos y aplicaciones: Guía para estudiantes y profesionales. México: Alfaomega grupo editor, 2013.

[2] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Glosario de términos. [en línea]. <http://www.inteco.es/glossary/Formacion/Glosario/>. [citado en 24 de marzo de 2014].

[3] SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL. Manuales de soporte técnico. [en línea]. <https://web.certicamara.com/soporte-tecnico/manuales-de-soporte-t%C3%A9cnico/>. [citado en 10 de febrero de 2014].

[4] SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL. Marco legal. [en línea]. < https://web.certicamara.com/marco-legal/>. [citado en 25 de enero de 2014].

[5] SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL. Centro de descargas. [en línea]. < https://web.certicamara.com/centro-de-descargas/>. [citado en 10 de febrero de 2014].

[6] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Chat gobierno en línea. [en línea]. <http://chat.gobiernoenlinea.gov.co/webchat/sic/>. [citado en 29 de enero de 2014].

[7] ALCALDÍA DE BOGOTÁ. Ley 527 de 2009. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276>. [citado en 9 de noviembre de 2013].

[8] ALCALDÍA DE BOGOTÁ. Ley 794 DE 2003. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6922>. [citado en 9 de noviembre de 2013].

[9] ALCALDÍA DE BOGOTÁ. Ley 962 DE 2005. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17004>. [citado en 9 de noviembre de 2013].

[10] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Decreto 1747 de 2000. [en línea]. <http://www.sic.gov.co/documents/10157/397811/Decreto_1747_2000.pdf/1bbcb205-a35c-435b-a5ba-413c641f4f86>. [citado en 9 de noviembre de 2013].

[11] ALCALDÍA DE BOGOTÁ. Decreto 1929 de 2007. [en línea].

<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=25311>. [citado en 9 de noviembre de 2013].

[12] ALCALDÍA DE BOGOTÁ. Decreto 2474 de 2008. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31185>. [citado en 9 de noviembre de 2013].

[13] ALCALDÍA DE BOGOTÁ. Decreto 2150 de 1995. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1208>. [citado en 9 de noviembre de 2013].

[14] ALCALDÍA DE BOGOTÁ. Ley 270 de 1996. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6548>. [citado en 9 de noviembre de 2013].