Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4

Arcos Poma, Jhon Darío y Espín Flores, Roberto José

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de titulación previo, a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Ron Egas, Mario Bernabé

08 de junio del 2022

COPYLEAKS

Tesis Firma Electrónica del ESPE-CERT en el DCCO con ITIL …

Scanned on: 0:21 August 11, 2022 UTC

Identical Words	2
Words with Minor Changes	0
Paraphrased Words	97
Omitted Words	4197

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de titulación, **"Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4"** fue realizado por los señores Arcos Poma, Jhon Darío y Espín Flores, Roberto José; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 05 de septiembre de 2022

Firma:

Firmado electrónicamente por:
MARIO
BERNABE RON

.....

Ing. Ron Egas, Mario Bernabé MSc.

C.C: 1704229747

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Nosotros, **Arcos Poma, Jhon Darío** y **Espin Flores, Roberto José**, con cédulas de ciudadanía N.° 1718323213 y N.° 1803641214, declaramos que el contenido, ideas y trabajo de titulación: **"Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4"**, es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 05 de septiembre de 2022

Arcos Poma, Jhon Darío

C.C.: 1718323213

Espin Flores, Roberto José

C.C.: 1803641214

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Nosotros, **Arcos Poma, Jhon Darío** y **Espín Flores, Roberto José**, con cédulas de ciudadanía N.° 1718323213 y N.° 1803641214, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 05 de septiembre de 2022

Arcos Poma, Jhon Darío

C.C.: 1718323213

Espín Flores, Roberto José

C.C.: 1803641214

Dedicatoria

Un día te prometí que lo lograría, para ti mamá.

Jhon Darío Arcos Poma

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme estar en este momento tan importante de mi formación profesional. A mis padres ya que con su comprensión y apoyo en todo momento ha sido muy importante para encarar las adversidades, a mi familia principalmente mis hijos Diego y Mathias ya que ustedes han sido mi inspiración y motivación diaria para llegar a este logro muy importante.

Roberto José Espín Flores

Agradecimientos

Agradezco a Dios, mis padres y hermanos de quienes he sentido su apoyo y aliento incondicional siempre, pero sobre todo agradezco a mi amada esposa Silvana, quien ha sido el engranaje fundamental en mi vida para cumplir todos mis propósitos.

Jhon Darío Arcos Poma

Primeramente, quiero expresar mi gratitud a Dios, quien con su bendición llena siempre toda mi vida y guía mi camino, a mis padres ya que han sido un ejemplo de lucha a nunca darme por vencido ante cualquier adversidad, y a mi familia amada ya que han sido un pilar fundamental con su amor, comprensión y apoyo incondicional diario en todos estos años de estudios, gracias a ustedes he logrado cumplir esta meta tan anhelada.

De igual manera mis agradecimientos a la Universidad Fuerzas Armadas “Espe” y a todos a mis profesores quienes con su enseñanza de sus valiosos conocimientos hicieron que pueda crecer diariamente como profesional, gracias a todos ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Roberto José Espín Flores

Índice de contenido

Índice de tablas

Índice de figuras

Resumen

En base del Proyecto de Investigación “Firma digital para asegurar la integridad y autenticación de origen de los documentos enviados por los estudiantes de la Universidad de las Fuerzas Armadas ESPE”, actualmente en ejecución, se ha procedido con la transición del servicio al CERT ESPE, en base a ITIL V4.

Se ha realizado la Operación del servicio PKI ESPE con la comunidad universitaria conformada por los estudiantes, docentes y personal administrativo del Departamento de Ciencias de la Computación generando los certificados digitales que les permiten legalizar y verificar de manera digital la autenticidad necesaria en cualquier proceso de gestión documental dentro de la Universidad.

Se realizó la evaluación de usabilidad y funcionalidad del servicio de firma digital aplicando encuestas a los usuarios finales, obteniendo recomendaciones y observaciones útiles que permitieron desarrollar un plan de mejora del servicio.

Las observaciones recopiladas en el periodo de evaluación fueron plasmadas en el plan de mejora del servicio, lo que permitió tomar las acciones pertinentes para mejorar el proceso del uso de la aplicación PKI ESPE y proceso de firma digital de un documento mediante la reducción en los tiempos de gestión en los procesos de certificación y mejorando la satisfacción de los usuarios.

Palabras clave: Biblioteca de Infraestructura de Tecnologías de Información, firma electrónica, Autoridad de Certificación de Enterprise JavaBeans, certificado digital.

Abstract

Based on the Research Project "Digital signature to ensure the integrity and authentication of origin of the documents sent by the students of the University of the Armed Forces ESPE", currently in execution, the service has been transitioned to the CERT ESPE, based on ITIL V4.

The Operation of the PKI ESPE service has been carried out with the university community made up of students, teachers and administrative staff of the Department of Computer Science, discovering the digital certificates that allow them to digitally legalize and verify the necessary authenticity in any management process. documentary within the university.

The evaluation of usability and functionality of the digital signature service was carried out by applying surveys to end users, obtaining useful recommendations and observations that allowed the development of a service improvement plan.

The observations collected in the evaluation period were reflected in the service improvement plan, which showed taking the pertinent actions to improve the process of using the PKI ESPE application and the process of digital signature of a document by reducing the costs of management in certification processes and improving user satisfaction.

Key words: Information Technology Infrastructure Library, electronic signature, Enterprise JavaBeans Certificate Authority, digital certificate.

Capítulo I

Introducción

En los últimos años, la naturaleza de los sistemas informáticos ha evolucionado rápidamente después de un gran progreso gracias al avance de la tecnología a partir de le segunda mitad del siglo XX. La Sociedad de la información no es un término sin contenido ni expectativa de impacto, al contrario, es noticia en nuestra vida diaria. La revolución social ha cambiado algunos de los hábitos más cotidianos y han logrado inculcar un sentido de cercanía en la humanidad con los servicios y datos en continua expansión en el mundo del Internet, medio con más movimiento e impacto, y quizás los más directos y dinámicos, ayudando a conectar a personas de todo el mundo a un costo razonable.

El continuo desarrollo de la tecnología ha llevado a la creación de sistemas con procesos más dinámicos mediante los cuales las organizaciones son más interoperables haciendo uso de la documentación digital. A raíz de la pandemia por el COVID-19 la exigencia de una firma hológrafa (firma manuscrita) para realizar el trabajo administrativo, dejó de ser tan indispensable en muchos países y regiones que están abandonando el uso del papel como asistir en la realización de sus trámites, y en su lugar, comenzaron a usar más herramientas automatizadas con sistemas avanzados que aseguran una mayor eficiencia en sus operaciones y menos tiempo de respuesta. Sin embargo, uno de los principales desafíos del uso mejorado de los documentos digitales es determinar su autenticidad, es decir, la capacidad de garantizar que una persona ha expresado su consentimiento sobre el contenido del documento.

Con la implementación de la firma digital, nos ayudará a resolver los problemas actuales para emitir documentos legales, ya que ayuda a garantizar la confidencialidad del autor y la seguridad de los documentos, permitirá producir documentos físicos. Los documentos digitales son como firmas 3D en documentos (Urrego, 2011).

Planteamiento del problema

El crecimiento constante del consumo de papel, junto con la necesidad de espacio físico para su propio almacenamiento, las dificultades de transporte, el lento acceso a la información y las actualizaciones tardías son inconvenientes que se presentan a diario dentro de la institución Universitaria. Si bien el uso de firmas tripartitas impide que el proceso se desarrolle sin problemas, el escaneo de documentos que contienen estas firmas solo tiene fines de archivo. Estos problemas crecen exponencialmente cuando se separan las sedes.

Justificación

En la actualidad toda organización requiere verificar la legalidad de los documentos que se usen dentro de la misma y, por ende, si no se cuenta con herramientas para la verificación de la autenticidad de estos documentos, se pueden dar vulneraciones a la integridad de los mismos. Debido a esta problemática se requiere de herramientas que permitan legalizar documentos de forma automática, rápida y segura, las mismas que serán de gran ayuda para que los miembros de la organización tengan la certeza de trabajar con documentos legítimos. Es deber de las organizaciones proveer de estas herramientas a todos sus integrantes y colaboradores, por ello es importante la implementación de un servicio de Firma Electrónica en el ESPE-CERT del Departamento de Ciencias de la Computación con la finalidad de prestar este servicio a la comunidad conformada por los estudiantes, docentes y personal administrativo del DCCO y estar en capacidad de extender el servicio a otros departamentos de la ESPE.

Objetivos

Objetivo general

Realizar la Transición, Operación y Evaluación y Mejora del Servicio de Firma Electrónica, por parte del CERT académico del DCCO, para prestar este servicio a la comunidad conformada por los estudiantes, docentes y personal administrativo del DCCO y estar en capacidad de extender el servicio a otros departamentos de la ESPE.

Objetivos específicos

- Establecer el estado del Arte
- Implementar el servicio de Firma Electrónica según ITIL V4 en los servidores del ESPE-CERT del DCCO.
- Operar el servicio de Firma Electrónica con los estudiantes, docentes y personal administrativo del DCCO en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos con la Dirección del DCCO e incorporándolo al catálogo de servicios del CERT-ESPE.
- Evaluar el servicio para determinar el cumplimiento de los objetivos del proyecto y la calidad de servicio prestado.
- Realizar la mejora del servicio en base a las recomendaciones de la evaluación y valorar el impacto en el funcionamiento del sistema.

Alcance

Implementar el servicio de Firma Digital en el CERT – ESPE para prestar este servicio a los estudiantes, docentes y personal administrativo del DCCO y estar en capacidad de extender el servicio a otros departamentos de la ESPE. Tomando a consideración los específicos del proyecto donde se establecerá el estado del arte la misma que contendrá las parte esencial de nuestro estudio para la implementación de Firma Electrónica, las misma que será de gran utilidad y será operada de una manera exitosa por todos los involucrados así teniendo un compromiso de disponibilidad y que sea incorporado al catálogo de servicio donde se podrá evaluar el mismo para posteriormente realizar mejoras según recomendaciones del funcionamiento del sistema.

La implementación del servicio de Firma Electrónica estará lista para ser entregado cuando cuente con los niveles adecuados de disponibilidad y una correcta operación y el proyecto se considerará finalizado cuando se realice la evaluación y mejora del sistema.

Los recursos necesarios para la implementación del servicio, serán provistos por el DCCO y operados directamente en el ESPE-CERT. Al tratarse de un proyecto que usa software libre, no se requiere de inversión económica por parte de la organización. El proyecto no iniciará sin la previa aprobación del CERT – ESPE, así como de la directiva del DCCO. Al finalizar el proyecto, los estudiantes, docentes y personal administrativo del DCCO contarán con una firma electrónica que podrán usar para legalizar documentos.

Para concluir de una forma más extensa la propuesta al alcance de este proyecto planteado, se propone preguntas para la investigación siendo así consideradas dos preguntas por cada objetivo específico, ya que las mismas serán las mínimas y servirá como base para el progreso de la investigación.

Tabla 1

Objetivos y preguntas

Objetivo específico	Pregunta de investigación
Establecer el estado del Arte	¿Cómo ayudará la implementación de una firma digital en el DCCO?
	¿De qué manera y en que se basará para la implementación de la firma digital?
Implementar el servicio de Firma Electrónica según ITIL V4 en los servidores del ESPE-CERT del DCCO.	¿Cómo se va a realizar la transición del servicio aplicando ITIL V4?
	¿De qué manera se va a realizar la implementación del servicio en los servidores del ESPE-CERT del DCCO?
Operar el servicio de Firma Electrónica con los	¿Como será la operación del servicio de

Objetivo específico	Pregunta de investigación
estudiantes, docentes y personal administrativo del DCCO en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos con la Dirección del DCCO e incorporándolo al catálogo de servicios del CERT-ESPE.	firma electrónica que se va implantar en DCCO? ¿Como se incorporará el servicio de firma electrónica al catálogo de servicios del CERT-ESPE del DCCO?
Evaluar el servicio para determinar el cumplimiento de los objetivos del proyecto y la calidad de servicio prestado.	¿Qué parámetros se tomarán a consideración para la evaluación del servicio? ¿Cómo se evaluará la calidad del servicio prestado?
Realizar la mejora del servicio en base a las recomendaciones de la evaluación y valorar el impacto en el funcionamiento del sistema.	¿Qué se tomará a consideración para realizar las mejoras del servicio? ¿Cómo será la evaluación de las acciones para evaluar el funcionamiento del sistema

Hipótesis

El uso de la firma electrónica por parte de los miembros del Departamento de Ciencias de la Computación permitirá la legalización digital de documentos para usarlos en los procesos de gestión documental interna de la Universidad de las Fuerzas Armadas ESPE. El servicio de emisión y validación de certificados digitales cumplirá con las etapas de operación, evaluación y mejora, permitiendo dejar la herramienta en capacidad de extender el servicio a otros departamentos de la ESPE.

Metodología

Para el desarrollo del presente proyecto, se ha escogido la metodología Desing Science Research la misma que está enfocada en la creación de productos enfocados a resolver problemas en el marco de las TI (Tuunanen, 2007).

Metodología Design Science Research

Según (Cataldo, 2015) la metodología que vamos a trabajar consta de siete pasos:

- Relevancia del problema
- Diseño como artefacto
- Rigor de la Investigación
- Diseño como un proceso de búsqueda
- Evaluación del diseño
- Contribuciones a la investigación
- Comunicación de la Investigación

Dentro del primer paso y segundo paso es dar solución problemática planteada del sistema que se va implementar y que sea de importancia para las TI mismo sea de gran ayuda para la comunidad, tomando como base una revisión literaria sobre la implementación de firma electrónica así con esto se abarcaría el primero y segundo objetivo específico planteado. En el tercero y cuarto paso se debe estar analizar todos los métodos para poder operar y aplicar la implementación de un artefacto, los mismos que deben estar respaldados en teorías y conocimientos utilizando todos los medios que se tenga a disposición. Tomando en referencia estos pasos estaríamos enmarcados con tercer objetivo específico.

En el quinto paso donde se refiere a la evaluación debemos considerar la eficacia, funcionalidad, rendimiento para que así todos los requerimientos de la organización sean solventados y sea de calidad el servicio que se va a brindar con esto estaríamos cumpliendo con lo que nos indica el curto objetivo específico. Por último, en sexto y séptimo paso se trata de realizar los estudios y según la evaluaciones y testeo

experimental analizar el impacto y la contribución del mismo, para así dar solución a las recomendaciones dadas. Con esto estamos alineados en el quinto objetivo específico.

Capitulo II

Fundamentación teórica y estado del arte

Fundamentación teórica

En el desarrollo de la investigación es fundamental tener conocimiento acerca de los principales conceptos afines como son certificados electrónicos, firmas electrónicas, seguridad de la información, conocimiento sobre que es ITIL, con esto es muy importante tener la fundamentación teórica y bibliográfica para el desarrollo de este proyecto

Cuando las personas necesitan los certificados digitales siempre será lo principal la certificación y una vez aprobado lo que se tiene que hacer es implementar aplicando un software. Siendo un principal obstáculo para las empresas que desean implementarlo el coste económico ya que su gato total será según el número de trabadores que se les va acreditar la firma, con esto tendrán que planificar el gasto mensual que se contraiga.

ITIL

ITIL significa Information Technology Infrastructure Library, en su traducción al español vendría a ser Biblioteca de Infraestructura de Tecnologías de la Información, la misma que es una estructura que en la actualidad es la más reconocida por ITSM. ITIL se inició 1989 para ayudar así en la evolución de habilidades de TI y en gestión de servicio. ITIL provee estructura y certifica a particulares. (Carquin, 2016). ITIL nos garantiza tener una buena calidad de servicio en TI, donde nos da in formación de los procesos que se destacan en determina organización, es por eso que abarca una gran extensión en su aplicación lo ayuda a las organizaciones a orientar nuevos objetivos (Bon, 2010).

Practicas ITIL

Con la aplicación de prácticas lo principal es colaborar con las organizaciones para que estas brinden un buen servicio de TI, para así optimizar el servicio y así poder cumplir con los convenios que se encuentran establecidos. Se divide en 3 partes importantes

- Prácticas de Gestión General. Son principalmente para la aplicación en gestión de servicios.

- Prácticas de Gestión de Servicios. Son aplicadas en empresas industriales donde se trabaja con gestión de servicios.
- Prácticas de Gestión Técnica. Son aplicadas con el principal fin de brindar soluciones de ámbito tecnológico enmarcadas en servicios de TI.

Sistema de valor del servicio ITIL

Cuando estimamos y hablamos de un sistema de servicio contiene lo preciso donde podemos establecer valor de los servicios. Donde el mercado que se brinda este servicio debe estar con todos los dispositivos donde irán de la mano con los clientes.

Enfocados en este sistema podemos referir sus componentes y actividades ya que cualquier organización donde están enlazados en su trabajo permitirá la creación de valor. Los recursos de cada organización involucrada deben estar alineados y coordinados de manera sólida, a pesar de ser los mismos componentes y actividades. Cada grupo tiene que trabajar en conjunto de manera dúctil, de acuerdo a sus situaciones.

Criptografía y cifrado

El hombre ha inventado métodos para ocultar información mientras viaja en el medio, para que solo el destinatario pueda verla. Esto se denomina criptografía (métodos para ocultar información) y se ha utilizado para enviar información que debe mantenerse en secreto o confidencial para otras personas.

Criptografía

La criptografía recibe su nombre de las palabras griegas kryptos, que significa ocultar, y graphos, que significa escribir. Literalmente, la criptografía es el arte de la escritura oculta.

A Claude Elwood Shannon se le atribuye la creación de la Teoría de la Información, una rama de las matemáticas, en 1948. Esta línea de ciencia se dividió en dos subramas más: criptografía y teoría de códigos. La criptografía se subdivide en criptoanálisis y criptografía.

Para garantizar que un mensaje o información solo sea leído por el destinatario

previsto, se cifra mediante algoritmos. Solo el destinatario conoce la clave necesaria para descifrar el mensaje, por lo que, aunque el medio de comunicación sea inseguro o interceptado, la información no puede ser entendida. Para evitar que la información se entienda, un algoritmo de cifrado cambia la información a números aleatorios. Estos algoritmos usan una o más claves, y la entrada del algoritmo es el mensaje que necesita protección, mientras que la salida es una confusión de información, se le llama información cifrada o criptograma.

La firma electrónica

Las firmas autógrafas tradicionales han sido validadas a través de métodos tales como copias de documentos y grafoscopios, que analizan las características físicas de una firma y texto. Estos métodos se centran en los trazos y otros aspectos estructurales de la firma para determinar su autenticidad. Se pueden usar para probar la autenticidad o la falsedad de un gráfico y, en algunos casos, ayudan a establecer quién es el autor de una persona en función de la evidencia física. Estos métodos son técnicas utilizadas en investigaciones forenses, que se ocupan de la ciencia de la criptografía, que identifica y autentica un documento y su autor.

La firma digital se crea mediante el cifrado de la información de los documentos. Autentica el documento, asegurando que no sea refutable, además de garantizar la integridad del documento.

Concepto de la firma electrónica

Las firmas electrónicas se utilizan para garantizar la autenticidad, integridad y confidencialidad de los documentos o transacciones en Internet. Ayudan a reducir el riesgo de alterar los documentos y se pueden utilizar de muchas maneras diferentes.

Una firma digital es un conjunto de datos digitales que indica una persona específica. Por lo general, se adjuntan a un documento enviado a través de medios digitales, como el correo electrónico, para que la persona que recibe el mensaje sepa quién lo envió y pueda estar seguro de que el mensaje no ha sido alterado (Formentín, 2012).

Según UNCITRAL los datos en formato electrónico que se adjuntan o vinculan a un

mensaje de datos, pueden usarse para indicar la aprobación del firmante en relación con el mensaje de datos y significar que se está identificando con los datos. La firma electrónica se considera un medio de expresión de la voluntad por vía electrónica, y es fundamental para la seguridad en las transacciones de comercio electrónico. Cuando las partes intercambian información en un flujo de transacciones en el que no tienen contacto físico entre sí, ¿cómo saben que están tratando con la persona adecuada? También tienen que preocuparse por la posibilidad de que personas ajenas hayan robado o cambiado la información, o incluso la posibilidad de que la información haya sido robada.

La Firma Electrónica identifica a la persona que realizó la transacción, brindando el servicio de autenticación y no permitiendo que la transacción sea denegada.

El artículo 13 de la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos establece que una firma electrónica es todo aquello que indica la aprobación y reconocimiento de la información contenida en un mensaje de datos, y puede ser utilizada para identificar a la persona que firma el mensaje. La firma está en formato electrónico y se adjunta o vincula al propio mensaje.

Concepto de Firma Electrónica en la legislación del Ecuador Consideramos importante

El artículo 13 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos define firma electrónica como el dato adjunto o vinculado de alguna forma a un mensaje de datos, que puede indicar la aprobación y reconocimiento de la información del mensaje por parte del titular de la firma.

El artículo 10 de la Ley ordena que el gobierno cree un Reglamento sobre la Firma Electrónica. En este Reglamento se determina que la Firma Electrónica puede ser aceptada sin sesgos tecnológicos. La Ley y su Reglamento no dan preferencia a un tipo de Firma Electrónica generada dentro de la infraestructura de clave pública, ni dictan qué acuerdos toman las partes sobre la validez y eficacia jurídica de una Firma Electrónica.

El Código Orgánico de Comercio e Inversiones COPCI prioriza la facilidad de los procesos comerciales, que es el objetivo principal de la firma electrónica.

Beneficios que genera la utilización de firmas electrónicas

Entre los beneficios que adquieren las personas al utilizar las firmas electrónicas tenemos:

Ahorro de dinero y tiempo.

Aporta al desarrollo de la Sociedad de la Información del Comercio Electrónico y el eGovernmet que es el que otorga la protección jurídica

Reducción de la utilización del papel, así contribuimos también en el cuidado del medio ambiente.

Mejora la competitividad.

¿Qué garantías nos ofrece el uso de la firma electrónica?

Como se mencionó anteriormente la firma electrónica nos brinda garantías que a continuación se detallan:

Autenticidad: “La información del documento y su firma electrónica se corresponden indudablemente con la persona que ha firmado” (García, 2018).

“Se refiere a la seguridad de que el remitente del mensaje es realmente quien dice ser. Una firma electrónica asegura la autenticación porque existe una autoridad certificadora que se encarga de asegurar que la pareja de claves, pública y privada pertenecen exclusivamente a una persona y dicha autoridad ha verificado su identidad. La firma electrónica garantiza la identidad digital del remitente de una comunicación” (Cadena,2015).

Integridad: “La información contenida en el documento electrónico, no será modificada o alterada luego de su firma” (López, 2016).

La integridad es la propiedad de la información que garantiza que no ha sido modificada intencionalmente, ni debido a errores, de transmisión o de almacenamiento en un período de tiempo determinado. Esta propiedad la asegura la firma electrónica, a través de la función de hash, porque si al verificar la firma y comparar el resultado de la función de hash calculada, con el que está adjunto a la firma se garantiza que la información no ha sido alterada desde que se firmó electrónicamente hasta el momento en que se vuelve a calcular el resumen, con la función de hash (López, 2016).

No repudio: “Es también conocido como la irrenunciabilidad, ya que una persona que ha firmado electrónicamente con un certificado emitido por una entidad de certificación acreditada no puede negar su autoría de haber firmado ante el receptor del documento.

El no repudio puede darse de las siguientes maneras” (Álvarez,2016).

No Repudio de origen: El emisor no puede negar que envió el mensaje, porque el destinatario tiene pruebas del envío.

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Confidencialidad: La información contenida ha sido cifrada y por voluntad del emisor, solo se permite que el receptor pueda descifrarla (Salgado, 2017).

“La confidencialidad de la información es la propiedad que garantiza que únicamente el o los destinatarios podrán tener acceso a ella” (Salgado, 2017). Según la norma ISO 17799, la confidencialidad es “garantizar que la información es accesible sólo para aquellos autorizados a tener acceso”

Requisitos para la firma electrónica

Funciones básicas de la firma electrónica

Las funciones básicas de una firma electrónica son:

• Identificar al firmante de manera inequívoca.

• Asegurar la integridad del documento firmado, asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación.

• Asegurar la integridad del documento firmado, los datos que utiliza el firmante para realizar el firmado son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

Procedimiento de creación de la firma electrónica

El procedimiento de creación y funcionamiento de Firma Electrónica, está basado en un sistema de encriptación asimétrica donde existe una clave pública y una clave privada, además de una entidad de certificación, donde:

“Cada parte tiene un par de claves, una se usa para cifrar y la otra para descifrar. Cada parte mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública)” (Cadena, 2017).

Al documento original se lo aplica una función llamada “hash” (resumen). Esta función devuelve un conjunto de datos, que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que genera el mismo resultado al aplicar la función “hash”.

El emisor cifra el resumen del mensaje con su clave privada; esta es la firma electrónica que se añada al mensaje original.

Para realizar la verificación del mensaje, el receptor genera el resumen digital del mensaje recibido, luego descifrará la firma electrónica y obtendrá de esa forma el resumen del mensaje original; si ambos resúmenes coinciden, significa que no hubo alteración y que el firmante es quien dice serlo (López, 2018).

Certificado electrónico

Certificado Electrónico

Un certificado es unión entre la clave pública de una entidad y los atributos respectivos a su identidad. Esto es avalado por una clave pública que corresponde a una entidad identificada y que la entidad posee la correspondiente clave privada. Cuando hablamos de certificados que tienen una clave pública se lo llama Certificado Digital, los certificados digitales solo tienen validez cuando es avalado por alguna Autoridad Certificadora (Certification Authority). La misma que dará fe de su validez, algo que se debe tener en consideración y que es transcendental para impedir la adulteración de un certificado el sujeto certifica luego de verificar la identidad de un sujeto, firma el certificado digitalmente (Talens, 2008).

Los certificados digitales nos ayudan nos ayuda a proveer un componente criptográfico mediante el cual realiza una asistencia perfecta en la implementación de la autentificación; también suministrando seguridad al momento que realicemos la distribución de claves públicas a los usuarios (Talens, 2008).

Estándar X 509

- Versión. Este sujeta el número de versión del certificado codificado y se puede obtener valores 1 al 3.
- Número de serie del certificado. Se toma un entero el mismo que se establece y es asignado a una autoridad y conserva una serie única.
- Identificador del algoritmo de firmado. Se selecciona un algoritmo puede ser RSA o el DSA.
- Nombre del emisor. Identificamos la CA donde se ha firmado y poder emanar el certificado.
- Periodo de validez. Aquí se establece el tiempo dura y tiene validez el certificado. Donde se tomará la fecha que se inicia, fecha donde el certificado es legítimo y fecha cuando ya no tiene validez.
- Nombre del sujeto. Se identifica la identidad donde clave pública debe estar certificada.
- Información de clave pública del sujeto. Posee la clave pública, así como el identificador del algoritmo con el mismo que se debe utilizar la clave.
- Identificador único del emisor. Se puede utilizar los nombres anteriores de emisor.
- Identificador único del sujeto. Se puede volver a utilizar nombres del sujeto.

Certificado de Firma Electrónica

"Los certificados son documentos electrónicos que incluyen ciertos datos de su titular y su llave pública, y están validados por una Entidad Certificadora. Este documento permite utilizar la firma electrónica y contiene una serie de datos como son: el Código Único de Identificación, el periodo de validez, los datos del titular del certificado (NOMBRE, RFC), así como la llave pública" (Landeros, 2017).

Proceso básico de Firma Electrónica

El proceso básico que se sigue para la firma electrónica es el siguiente:

- El usuario dispone de un documento electrónico y de un certificado que le

pertenece y le identifica.

• La aplicación utilizada para firmar electrónicamente realiza un resumen del documento, el cuál es único y cualquier modificación del documento implica también una modificación del resumen.

• La aplicación utiliza la clave contenida en el certificado para codificar el resumen.

• La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

Certificado de la firma electrónica

"Los certificados son documentos electrónicos que incluyen ciertos datos de su titular y su llave pública, y están validados por una Entidad Certificadora. Este documento permite utilizar la firma electrónica y contiene una serie de datos como son: el Código Único de Identificación, y los datos del titular del certificado" (García, 2018).

Tipos de Certificados:

Certificados Persona Natural: "Certificados reconocidos de persona física que identifican al suscriptor como una persona natural que puede usar estos certificados para temas tributarios, legales y personales".

Certificados Corporativos de Persona Jurídica - Empresa: "Certificados reconocidos de persona jurídica que identifican al suscriptor como Empresa Privada" (Muñoz, 2016).

Certificado de Funcionario Público: "Son certificados reconocidos de persona física que identifican al suscriptor como Administración Pública y al firmante como empleado de la Administración" (Muñoz, 2016).

Certificados de Servidor Seguro (SSL): "Son certificados que relacionan un dominio de Internet con una persona jurídica o un comerciante registrado determinado" (Muñoz, 2016).

Certificados Corporativos de Representante Legal: **“**Son certificados reconocidos de persona física que identifican al suscriptor como una corporación y al firmante como representante legal de dicha corporación” (Muñoz, 2016).

Certificados Corporativos de Miembro de Empresa: **“**Son certificados reconocidos de persona física que identifican al suscriptor como Corporación y al firmante como vinculado a esa corporación, ya sea como empleado, asociado, colaborador, cliente o proveedor” (Security Data, 2015).

Requisitos para obtener el Certificado de Firma Electrónica

Persona Natural

- Digitalizado de cédula o pasaporte a color.
- Digitalizado de papeleta de votación actualizada.
- Digitalizado de la última factura de pago de luz, agua o teléfono.

Persona Jurídica

- Digitalizado de cédula o pasaporte a color.
- Digitalizado de papeleta de votación actualizada.
- Digitalizado del nombramiento o certificado laboral firmado por el representante legal.
- Autorización firmada por el representante legal.

Entidad Certificadora

Una persona autorizada conforme a esta ley puede prestar servicios de registro y sellado de tiempo para la transmisión y recepción de mensajes de datos, así como otras funciones de comunicación utilizando firmas digitales. Esta persona puede emitir certificados relativos a las firmas digitales de personas, y puede ser una persona física o jurídica.

El departamento universitario que tiene la autoridad para dar, quitar, pausar o

cancelar certificaciones de Firma Electrónica se denomina Entidad Certificadora. La labor más importante de la Entidad de Certificación es asegurar la identidad de la persona que obtiene un certificado, antes de otorgárselo, así como conservar y gestionar los certificados una vez emitidos.

“Las entidades certificadoras sin empresas o personas jurídicas que emiten certificados de firmas electrónicas y pueden prestar otros servicios relacionados con la firma electrónica” (Rubio, 2015).

“En Ecuador existen las siguientes entidades certificadoras acreditadas ante el CONATEL” (Consejo Nacional de Telecomunicaciones, 2016).

“El banco Central de Ecuador y Registro Civil: son entidades de certificación de información acreditada por el consejo nacional de telecomunicaciones. Emite certificados digitales de firma electrónica y otros servicios relacionados con la certificación electrónica para el sector público, personas jurídicas y personas naturales; garantizando la seguridad jurídica y tecnológica en entornos electrónicos” (García, 2018).

Los certificados de firma electrónica que ofrece son:

Token: “Es un dispositivo seguro USB que es ideal para transacciones en donde el usuario a través de una clave de mínimo 8 dígitos (PIN Token), posee físicamente dicho dispositivo al momento de hacer cada transacción funciona en ambientes Windows preferentemente, en otras plataformas es necesario conocer su compatibilidad de acuerdo al modelo y versión de sistema operativo” (Ortega, 2016).

“HSM (Hardware Security Module), es un dispositivo de alta seguridad el cual permite realizar varias transacciones por segundo, cumple con altos estándares de seguridad” (Dámaso, 2017).

“ROAMING, le permite realizar operaciones mediante el uso del applet publicado por la ECIBCE o un aplicativo opcional llamado ESP (Control de estabilidad)” (Banco Central del Ecuador, 2019).

“Las entidades que certifican las firmas digitales son empresas avaladas jurídicamente las mismas que expiden los certificados de firmas electrónicas” (Rubio,

2015).

Docker

La tecnología Docker es una aplicación que permite visualizar un Linux en las que incluyen todas las aplicaciones del sistema operativo Linux para empaquetarlos y desplegarlos en cualquier otro Linux sin tener la necesidad de introducir más que solo algunos comandos (Nuñez, 2014).

Docker es uno de los proyectos que cuenta con código abierto con el que resulta bastante fácil crear “contenedores”, estos contenedores de Docker se los puede definir como ligeras máquinas virtuales con menor exigencia con las memorias y chips de los equipos donde se los programa, dentro de estas se puede encontrar las siguientes características principales:

- Portabilidad
- Ligereza
- Autosuficiencia

Según González (2021) define a Docker como una plataforma que tiene como objetivo implemtar y desarrollar aplcaciones dentro de contenedores, los cuales permitiran a los desarrolladores realizar un empaquetado de aplicaciones en conjunto con sus correspodientes dependencias dentro de las unidades estandarizadas reconocidad bajo el termino de contenedores de software.

Docker es uno de los contenedores de Softare mas reconocidos ya que mediante la arquitectura de microservicios permite que Docker encapsule los servicios, en otras palabras permite empaquetar un sofware dentro de un contenedor (González, 2021).

Docker y su funcionamiento

Docker es una tecnología que es utiliza las funciones de Kernel de Linux, como lo son los espacios de nombre, los grupos de control, para poder dividir los procesos y de esta manera ejecutarlos de una manera independiente, el propósito de estos contenedores es poder ejecutar distintas aplicaciones y procesos de manera separada aprovechando la

infraestructura con la que cuenta y al mismo tiempo mantener la seguridad que se puede obtener con los sistemas individuales (Red Hat, 2018).

Los instrumentos de contenedores como Docker añades un modelo de implementación fundamentado en imágenes y así permitir la compartición de un conjunto de servicios o una aplicación con todas las dependencias en varios ambientes. Otra de las funciones de Docker es la implementación y la automatización de las aplicaciones en los ambientes de contenedores (Red Hat, 2018).

Ventajas de Docker

El modularidad: Se caracteriza por centrarse en la capacidad de poder separar una de las partes de la aplicación para repararla o actualizarla, sin tener la obligación de deshabilitar completamente la aplicación.

Control y capas de versiones de imágenes: Los archivos de imágenes de Docker esta estructuradas por capas adaptándose para conformar una sola imagen, esto sucede cuando el usuario o desarrollador ejecuta el comando, copiar o ejecutar la imagen, de esta manera la imagen cambiara y se formara una nueva capa.

Restauración: El mayor de los beneficios de las capas es la suficiencia y capacidad de poder restaurarse, ya que todas las imágenes están conformadas con capaz, es decir que si no le gusta la repetición que se genero puede volverla a su estado anterior, esta manera promueve un desarrollo ágil que permite lograra una implementación e integración continua desde la perspectiva de una herramienta.

Docker y sus contenedores se pueden llevar a cabo en cualquier lugar ya sea a nivel local en el centro de datos del cliente, Azure, así como también en la nube o un proveedor de servicio externo.

Se puede ejecutar de manera propia ya sea en Windows o Linux, estos contenedores de Docker, pero las imágenes de la plataforma de Windows solo se los puede llevar a cabo

Estos contenedores de imágenes a través de Host (máquina virtual o servidor) de Windows y por otro lado las imágenes de Linux se pueden llevar a cabo en los Host de

Windows y Linux sin problema alguno (Microsoft, 2022).

Cuenta con varias particularidades bastante llamativas según Alzate (2020) ya que se puede implementar de alto nivel una API que pueda proporcionar contenedores livianos, en donde cada contenedor que se crea y ejecuta transcurre de una manera aislada en Kernel de Linux, ya que resulta que los contenedores son mucho mas livianos a diferencia de las maquinas virtuales y no nesecitan tener un sistema operativo para cada contenedor ademas, cuenta con la capacidad o suficiencia de extender en un mismo equipo fisico varios contenedore, este sistema cuenta con la facilidad de desplegarse en diferente plataformas, finalmente ofrece la capacidad de aumentar los repositorios de Docker al compartirlo.

Marco legal

"Es muy importante conocer y mantener un marco legal regulatorio sobre comercio electrónico, firmas digitales y certificados electrónicos, con esto el país recibe la nueva era de la tecnología y la transferencia de información de forma segura.

En la legislación del Ecuador constan varios proyectos que hacen tomar conciencia de la importancia de las políticas y procedimientos en torno a la seguridad como por ejemplo el denominado Correo Seguro.

Regulaciones sobre Firma Digital

La legislación ecuatoriana estable la equiparación y validez de la firma manuscrita con la firma digital, para ser presentada en actos judiciales. A continuación, se presenta la ley y sus artículos relacionados con la firma digital y los mensajes de datos.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos

"La Ley de Comercio Electrónico de 2002 establece las normas para las transacciones comerciales realizadas a través de medios electrónicos" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002). En sus primeros artículos señala como aspectos principales el reconocimiento jurídico de los mensajes de datos que son equivalentes a documentos escritos. Estos mensajes de datos están sujetos a todas las leyes relativas a la propiedad intelectual, así como a los principios de confidencialidad y reserva. Como resultado, la intrusión electrónica, la transferencia ilegal de mensajes o la

violación de un secreto profesional están prohibidas por ley, y los mensajes de datos deben conservarse con condiciones específicas, es necesario el consentimiento del titular para su elaboración. Una base de datos sólo puede ser transferida o utilizada con la autorización del propietario o de la autoridad competente, y los datos personales recogidos y utilizados a través de las bases de datos sólo pueden ser transferidos o utilizados con la autorización del propietario o de la autoridad competente, finalmente, esta ley indica que cada mensaje de dato es considerando diferente y se puede pedir confirmación y verificación técnica de la autenticidad del mismo.

TITULO II: De las firmas electrónicas, certificados de firma electrónica, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.

De las firmas electrónicas

En el Ecuador y en varias partes del mundo, la firma electrónica es definida como datos electrónicos que definen a una persona o usuario en específico y que usualmente están unidos a documentos digitales que se envían telemáticamente obteniendo el mismo valor de una firma manuscrita" (Zayas, 2013).

En la actualidad se usa comúnmente en trámites públicos, privados y administrativos teniendo como por ejemplo declaraciones de impuestos, solicitud de documentos personales e inclusive procesos administrativos judiciales. Con esto se cumple ampliamente el objetivo de impulsar el acceso a servicios electrónicos a la población mejorando el desarrollo comercial educativo y cultural. Los artículos que establece la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos con respecto a las firmas electrónicas son:

Art 13.- "Firma electrónica un concepto idóneo en el cual se norma a la firma electrónica como un conjunto de datos electrónicos que asocia a un usuario, los mismos que pueden ser usados de igual forma que una firma manuscrita, con sus responsabilidades y derechos que esta posee además con este instrumento tecnológico mejora y agilita los procesos" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 14.- “Efectos de la firma electrónica, se detalla que la firma electrónica tiene la misma validez y efectos jurídicos que la manuscrita así mismo puede ser aceptada como prueba en juicios” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 15.- Requisitos de la firma electrónica, es necesario que se cumplan ciertos requisitos para su validez como:

- “Debe ser individual y estar vinculada solo al titular.
- Permitir verificar sin ambigüedad la identidad del firmante mediante los métodos técnicos reglamentarios.
- Que exista plena confianza con el método de creación seguro e inalterable para el cual el mensaje fue generado” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).
- Los datos al momento de su creación se encuentran bajo control exclusivo del signatario.
- La firma debe ser controlada por el usuario al cual pertenece.

Art 16.- “La firma electrónica en un mensaje de datos. Esto debe enviarse al mismo tiempo que el mensaje, como parte de él, o asociarse a él, con lo cual se entiende que el emisor da su consentimiento y responsabilidad estando sometido a lo que establece la ley contenida en el mensaje” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 17.- Obligaciones del titular de la firma electrónica el mismo deberá:

- “Cumplir con obligaciones que deriven del empleo de la firma electrónica.
- Tomar medidas de seguridad que requiera para conservar el control de la firma digital evitando la utilización no autorizada.
- Dar aviso cuando la firma pueda ser usada o controlada indebidamente por terceros.

- Responder al uso no autorizado de su firma cuando no ha tomado medidas razonables para impedirlo" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 18.- Duración de la firma electrónica; tienen una duración indefinida y están sujetos a la revocación, cancelación o suspensión en virtud de la ley.

Art 19.- Extinción de la firma electrónica la cual se podrá extinguir por:

- Acción voluntaria del titular.
- La muerte o la discapacidad del titular.
- Disolución o liquidación de la entidad legal.
- Por causa jurídicamente declarada.

De los certificados de firma electrónica

"Las instituciones de certificación utilizan los certificados digitales para dar fe de los datos de los usuarios que en ellos constan, generando confianza en la comunicación y en el intercambio de información telemáticamente entre las dos personas" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

"Un certificado de firma electrónica es un registro donde consta una clave pública de una persona, así como distintos datos que permiten la identificación de este usuario, el mismo que ha pasado por un proceso de verificación ante una parte de confianza" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002). Con el fin de garantizar que la firma electrónica pertenezca a una persona específica. Los artículos a los cuales hace referencia la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos son:

Art 20.- "Certificado de firma electrónica. - son los datos que, a través de un proceso, certifican el vínculo entre una persona y su respectiva firma electrónica" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 21.- "Uso del certificado de firma electrónica. - Se utilizará para verificar la

identidad del titular de una empresa electrónica, entre otras cosas, de conformidad con la ley" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 22.- Requisitos del certificado de firma electrónica. - los certificados para ser válidos deberá contener lo siguiente:

- Información de la entidad de certificación.
- Domicilio legal de la entidad de certificación.
- Información sobre el titular del certificado, como su nombre y dirección.
- El método para la verificación de la firma del titular del certificado.
- Las fechas tanto de emisión como de expedición del certificado.
- El número de serie único que identifica el certificado.
- La firma electrónica de la entidad de certificación.
- Las limitaciones para el uso del certificado.

Art 23.- Duración del certificado de firma electrónica. - el plazo del certificado será el establecido por esta ley, salvo exista algún acuerdo contractual" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 24.- "Extinción del certificado de firma electrónica. - llegan a su extinción por las siguientes causas:

- Solicitud del titular.
- Extinción de la firma electrónica de acuerdo a lo establecido en el Art 19 de esta ley.

Art 25.- Suspensión del certificado de firma electrónica. – el certificado de firma electrónica es suspendido temporalmente por las entidades de certificación cuando:

- Este dispuesto por el consejo nacional de telecomunicaciones, conforme con lo previsto en la ley.

- La entidad certificadora compruebe falsedad en los datos asignados por el titular del certificado.
- Violación del contrato entre el titular de la firma electrónica y la entidad certificadora.

Art 26.- Revocatoria del certificado de firma electrónica. – puede ser anulado por el Consejo Nacional de Telecomunicaciones de lo conforme a la ley por:

- El cese de la actividad de la entidad de certificación y nadie asuma los certificados emitidos.
- La entidad de certificación este en quiebra técnica judicial declarada.

Art 27.- “La suspensión temporal y la revocatoria surtirá efecto desde el momento en que se comunica al titular, y desde el momento en que se publica que deberá efectuarse con forme a lo establecido en el presente reglamento” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 28.- “Reconocimiento internacional de certificados de firma electrónica. - las entidades de certificación extranjeras que cumplan los requisitos de la ley y demuestren un nivel equivalente de garantía tendrán el mismo valor legal que los certificados acreditados de Ecuador” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

De las entidades de certificación de información

“El Consejo Nacional de Telecomunicaciones (CONATEL) es el ente encargado de regular y acreditar a las entidades de certificadoras de información. La función principal de estas entidades es la entrega de certificados y firmas electrónicas además de toda la actividad que conlleva las firmas digitales, una vez que han cumplido con todos los requisitos establecidos en la Ley” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Los artículos que establece la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos en lo referente a las entidades de certificadoras son los siguientes:

Art 29.- “Entidades de certificación de la información. - son empresas unipersonales

o entidades jurídicas autorizadas por el Consejo Nacional de Telecomunicaciones a expedir certificados de firma electrónica y otros servicios de firma electrónica" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 30.- Las responsabilidades de las entidades acreditadas de certificación de información - son obligaciones las siguientes:

- Encontrarse inscritas en el Consejo Nacional de Telecomunicaciones y encontrarse legalmente constituidas.
- Evidenciar solvencia técnica, logística y financiera para la prestación servicios a los usuarios.
- Asegurar prestación constante, inmediata confidencial, oportuna y certera del servicio de certificación de la información.
- Conservar servicios de respaldo de la información, relativa a los certificados.
- Sustentar la publicación de estados de los certificados electrónicos emitidos.
- Proporcionar a los titulares de certificados de firma electrónica un método efectivo y oportuno para notificarles que un certificado de firma electrónica corre el riesgo de ser utilizado indebidamente.

Art 31.- Responsabilidades de las entidades de certificación de información acreditadas. - Las entidades de certificadoras de información serán responsables hasta de culpa leve y atienden por los daños que causen a cualquier persona natural o jurídica, cuando incumplan las obligaciones impuestas en la ley o actúen con negligencia, sin atención a las sanciones previstas en la Ley Orgánica del Consumidor. Además, serán responsables por el uso inadecuado del certificado de firma electrónica acreditado.

Art 32.- "Protección de Datos para la Entidad de Acreditación de Formación Acreditada. - La unidad de certificación de la información velará por la protección de los datos personales que obtenga con motivo de sus actividades de conformidad con lo dispuesto en el artículo 9 de esta Ley" (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 33.- “Los servicios de autenticación son proporcionados por terceros. - Los servicios de certificación pueden ser prestados y gestionados total o parcialmente por terceros. Para hacer provisión, deben acreditar su relación con la entidad de autenticación de la información” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 34.- “Termino del contrato. - La extinción del contrato entre la entidad de certificación acreditada y el suscriptor se regirá por lo dispuesto en la Ley de Organismos de Protección al Consumidor” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Art 35.- “Una notificación para detener la actividad. - Una entidad de autenticación de información acreditada deberá notificar al organismo de control con al menos noventa días de anticipación al cese de sus actividades y seguirá las reglas y procedimientos establecidos para tal efecto” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Entidades de certificación

“El artículo 29 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos define a las entidades de certificación como "empresas o entidades legales que generan certificados de firma electrónica y prestan servicios relacionados. La ARCOTEL será la organización de autorización, registro y control para entidades de certificadoras” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Acreditadas

“Se puede definir a una entidad acreditada como aquella que ha sido evaluada y ha superado exitosamente estándares y criterios de calidad y su cumplimiento le permiten realizar una actividad con distinción. En el Ecuador de acuerdo con la Agencia de Regulación y Control de Telecomunicaciones se tiene las siguientes entidades acreditadas para la emisión de certificados” (Ley de comercio electrónico, firmas electrónicas y mensaje de datos, 2002).

Banco Central del Ecuador. – “esta entidad fue acreditada mediante resolución del

481-20-CONATEL de 8 de octubre de 2008 y renovada el 25 de octubre de 2018, tiene como objetivo emitir certificaciones de firma digital y de servicios relacionados con certificación electrónica, cumple con todas las normas y estándares nacionales e internacionales en lo referente a certificación electrónica. El Banco Central emite políticas de certificación claras y actualizadas que le permiten al usuario final conocer el uso, procedimientos, obligaciones y responsabilidades de los certificados electrónicos" (Certificación Electrónica, 1997).

Consejo de la Judicatura. – "la entidad de certificación del Consejo de la Judicatura fue creada a partir del año 2014 afianzándose hasta la actualidad con más de 18.000 firmas electrónicas entregadas, entre algunas ventajas que ofrece están la compatibilidad con algunos otros sectores públicos como el Servicio de Rentas Internas (SRI) y el Sistema Documental del Consejo de la Judicatura y la Corte Nacional de Justicia (SIGED). Posee puntos de emisión de certificados en cada dirección provincial del Consejo de la Judicatura, ayudando al acceso de la ciudadanía" (Judicatura, 2008).

Security Data Seguridad en Datos y Firma Digital. – "es la entidad certificadora de carácter privada para la emisión de certificados digitales y servicios a fines, tiene como visión generar identidades digitales a los ciudadanos cuyo objetivo es brindar seguridad jurídica y electrónica el intercambio de información dentro del ámbito tecnológico. Dentro de su gama de servicios ofrece contrato electrónico, póliza electrónica, facturación electrónica y sellado de tiempo" (SecurityData, 2007).

ANFAC Autoridad de Certificación del Ecuador. – "para 1997 previo a la presentación de un informe sobre el impacto del internet en el ámbito comercial, ya para el 2000 ANF AC está en condiciones de emitir certificados electrónicos inscrito como entidad privada en los registros de Autoridades de certificación reconocida por los países de la unión europea y también algunos países de Sudamérica entre ellos Ecuador, tiene como visión ayudar con estas herramientas tecnológicas a la seguridad de las personas y organizaciones en general, para que tengan mayor confianza en su participación en el mundo del comercio electrónico. Posee varios servicios de certificación electrónica a su

haber” (ANF AC, 2000).

Uanataca Ecuador S.A. – “Diseñada para generar soluciones que ayuden a la transformación digital con los más altos estándares de seguridad, acreditada por la ARCOTEL para la emisión de certificados y servicios relacionados. Se encuentran a la vanguardia con las necesidades de seguridad de los clientes, además, cuenta con personal altamente calificado para una atención completa y oportuna, posee varias oficinas en el país y el mundo para prestar los servicios entre los cuales están la de firma electrónica, firma electrónica avanzada, firma longeva, sellado de tiempo, y certificados digitales” (AS_ADAM Adam Datacenter, 2000).

No acreditadas

“En el Ecuador existen entidades de certificación no acreditadas que están registradas y prestan sus servicios, pero no han sido acreditadas por el CONATEL por lo cual deben probar fiabilidad y corroborar la seguridad y eficiencia técnica de los procesos de vida de los certificados emitidos”.

Estado del Arte

En la presente investigación se realiza la búsqueda de información relevante referente al uso de la firma digital como medio de certificación en la gestión documental de instituciones educativas. Para la búsqueda de esta información se considera las etapas de definición de las preguntas de investigación, revisión de los objetivos, conducción de la búsqueda, presentación de información y selección de investigaciones relevantes, las mismas que se proponen por (Petersen, Vakkalanka, & Kuzniarz, 2015).

Planteamiento de la revisión de literatura preliminar

El objetivo de la presente revisión de literatura es determinar parámetros adecuados para realizar el estado del arte: pregunta de investigación, estrategia de búsqueda y selección de estudios primarios.

Preguntas de investigación

Este estudio pretende identificar información sobre el uso de la firma digital como medio de certificación en la gestión documental de instituciones educativas, por ello

planteamos la siguiente pregunta de investigación: ¿Cuál es el impacto de la firma electrónica en la gestión documental de las instituciones educativas? Con esto se resumirá el conocimiento actual sobre la certificación digital de documentos y su valides para instituciones educativas como la Universidad de las Fuerzas Armadas ESPE.

Estrategia de búsqueda

En busca de estudios primarios se utilizó el repositorio digital Google Schoolar. En la búsqueda se usó la siguiente cadena de búsqueda: (implementación OR despliegue) AND (infraestructura de clave pública OR PKI) AND (firma digital OR certificado digital) AND (software libre). Donde el término OR se usa para unir palabras similares y el término AND para unir palabras diferentes.

Tabla 2

Palabras clave de búsqueda de literatura

Concepto	Términos alternativos	Conector
implementación	(implementación OR despliegue)	AND
infraestructura de clave pública	(infraestructura de clave pública OR PKI)	AND
firma digital	(firma digital OR certificado digital)	AND
software libre	(software libre)	

Selección de estudios primarios

Los resultados de la búsqueda se evaluaron por los autores considerando el título, resumen y palabras clave para seleccionar los artículos válidos. Se incluyó estudios que cumplan con uno o más de los criterios de inclusión detallados a continuación:

- Artículos que exhiban metodologías de implementación de una firma electrónica con uso de software libre.
- Artículos donde se muestre la implementación de un sistema de certificación electrónica.
- Artículos donde se muestre las políticas de uso de la firma electrónica.

- Artículos que presenten resultados del uso de un aplicativo de infraestructura de clave pública.
- Artículos publicados entre 2017 a 2022.

Se descartó artículos que cumplan con al menos uno de los criterios de exclusión expuestos a continuación:

- Artículos donde no se realice la implementación de una infraestructura de clave pública para el uso de firma electrónica
- Artículos que no presenten una propuesta de implementación con el uso de software libre.
- Artículos publicados antes del 2017
- Artículos escritos en otros idiomas que no sea el español o inglés.
- Artículos que únicamente muestren definiciones o descripciones de alguna de las palabras clave.

Evaluación de la calidad

Se aplicó un cuestionario para evaluar la calidad de los estudios seleccionados, el mimo consta de cuatro preguntas cerradas (afirmación o negación):

- El estudio muestra la implementación de una infraestructura de clave pública.
- El estudio muestra el uso de la firma digital para la gestión documental.
- El estudio muestra el uso de software libre.
- El estudio presenta la implementación en alguna institución educativa.

Los artículos deben cumplir con al menos tres de las cinco preguntas de forma afirmativa para ser considerados, esto permite determinar los artículos representativos y posteriormente abordar cada pregunta de investigación.

Estrategia de extracción de datos

Se busca proporcionar posibles respuestas para la pregunta de investigación planteada, asegurando la aplicación de un mismo criterio de extracción de datos en todos los trabajos que se seleccionó:

La pregunta planteada: ¿Cuál es el impacto de la firma electrónica en la gestión documental de las instituciones educativas? puede clasificarse dentro de las opciones planteadas en la tabla X.

Tabla 3

Clasificación de las investigaciones

Opción	Descripción
Positiva	La implementación de infraestructura de clave pública para el uso de firma digital muestra un impacto positivo en la gestión documental de una institución educativa.
Incierta	No se muestran resultados de la implantación de la infraestructura de clave pública para el uso de firma digital
Negativa	La implementación de infraestructura de clave pública para el uso de firma digital no soluciona problemas de certificación de documentos o su uso es desfavorable para la institución.

Métodos de síntesis

La metodología implementada usa datos cuantitativos para el número de trabajos encontrados y datos cualitativos para definir la calidad de los resultados obtenidos.

Etapa de conducción

En la conducción de la revisión del estado del arte mediante la búsqueda en la fuente Google Académico permitió encontrar 50 estudios potenciales que luego de una revisión adecuada permitió seleccionar 5 estudios primarios.

Resumen de los Estudios Primarios

Plan de implementación de Firma Digital en la Universidad Nacional de Río Negro (Sanhueza, 2018)

Este trabajo plantea la implementación de la Firma Digital en la Universidad

Nacional de Río Negro constituyendo una Autoridad de Registro dependiente de la Oficina Nacional de Tecnologías de Información. Se realiza la valoración del impacto del uso de la firma digital en los procesos de la Universidad. Se define el proceso de solicitud y otorgamiento de certificados digitales y las herramientas para firmar digitalmente.

Firma Digital (Anghillantte & Romero, 2017)

Se busca la implementación de firma digital considerando que es apropiado para garantizar la integridad de los documentos digitales, por lo que propone la implementación de un esquema de firma digital para garantizar la autenticidad del usuario final y la integridad de los documentos usados en el Instituto Universitario Aeronáutico (IUA).

Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente (Carrera & Celi, 2022)

En este trabajo se realiza una revisión de la literatura de proyectos relacionados a firmas digitales, determina políticas de funcionamiento de la Infraestructura de Llave Pública (PKI) en el Departamento de Ciencias de la Computación en la Universidad de las Fuerzas Armadas ESPE. Realiza el desarrollo de la aplicación web para gestionar certificados digitales y evaluar los niveles de integridad y autenticación de los documentos.

Paquete de Servicios para el Portafirmas Digital de la Universidad de las Ciencias Informáticas (Cordovi, 2018)

En este estudio se toma en cuenta aplicaciones que facilitan la autenticación de documentos digitales mediante APIS-REST para un aplicativo llamado Portafirmas UCI. Esto permite garantizar la autenticidad, integridad y no repudio de la información de cualquier documento, con la finalidad de entregar este servicio a la universidad y sus miembros.

Desarrollo e implementación del Sistema de Firmas Electrónicas y Certificados Digitales del Estado e implantación de la autoridad administrativa competente (Vermejo, 2020)

Este proyecto implementa la infraestructura oficial del Sistema Nacional de Firma Electrónica y Certificados Digitales con la finalidad de realizar transacciones digitales de documentos en forma confiable. La Autoridad Administrativa Competente será la encargada de aprobar y aplicar normas para posteriormente iniciar su operación. Con esto se generan certificados digitales para ser usados dentro de la institución.

Resumen general y conclusión del estado del arte

Resumen General

Se realizó la búsqueda de información relevante referente al uso de la firma digital como medio de certificación en la gestión documental de instituciones educativas.

Se consideró las etapas de definición de las preguntas de investigación, donde se planteo el cuestionamiento que guía la investigación literaria y por lo tanto es la base de esta revisión del estado del arte.

Posteriormente se planteó objetivos de la revisión literaria, con la finalidad de definir un alcance de la revisión y aportar a la delimitación de la búsqueda realizada.

En la conducción de la búsqueda se aplicó técnicas de selección y validación de artículos primarios, logrando descartar información irrelevante o redundante de los artículos encontrados.

Finalmente se presenta la información y se selecciona las investigaciones relevantes que permitan el aprovechamiento de la misma, apoyando de manera positiva al desarrollo del proyecto.

Conclusión del estado del arte

Luego de realizar la revisión literaria referente al uso de la firma digital como medio de certificación en la gestión documental de instituciones educativas, se encontró artículos que muestran la implementación de una infraestructura de clave pública usando software

libre y obteniendo resultados positivos al momento de su operación con miembros de la institución, por lo que se tomará este material bibliográfico como referencia para el desarrollo e implementación de nuestro trabajo de investigación.

Capítulo III

Transición y Operación

Transición

Plan de transición

Objetivos

- Replicar el servicio de Firma Electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación.
- Poner en operación el servicio de Firma Electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación.

Alcance

Replicar el servicio de Firma Electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación, en un plazo de 2 meses desde el inicio de la transición, debiendo encontrarse operable y listo para prestar este servicio a la comunidad conformada por los estudiantes, docentes y personal administrativo del DCCO. La transición se considerará finalizada cuando el DCCO cuente con el servicio de Firma Electrónica y la transición no iniciará sin previa autorización.

Indicadores de cumplimiento

- Porcentaje de disponibilidad del servicio.
- Entrega a tiempo
- Cumplimiento de términos y condiciones de acuerdo a trabajos anteriores.
- Porcentaje de errores y fallos.

Recursos

Humanos

Se cuenta con el docente tutor y los alumnos que se encuentran desarrollando el proyecto de titulación.

Financieros

No se requiere de recursos financieros en la fase de transición.

Materiales

Servidor en el laboratorio H202, computadoras personales.

Tecnológicos

Servicios de internet, repositorios e información disponible.

Tareas a realizar

Se ha definido tareas mediante un cronograma que abarca las actividades necesarias para la transición del servicio.

Tabla 4

Tareas y responsables del plan de transición

Tarea	Responsable	Duración	Comienzo	Fin
Preparación del HW e infraestructura física.	Estudiantes	5 días	21 mar	25 mar
Capacitación técnica para el uso de la infraestructura.	Estudiantes	2 días	28 mar	29 mar
Implantación de la herramienta de administración.	Estudiantes	30 días	30 mar	10 may
Capacitación de usuarios.	Estudiantes	10 días	11 may	24 may
Evaluación de la herramienta.	Estudiantes	5 días	25 may	31 may

Implantación

Recursos

Personas / Equipo de proyecto

- Ing. Mario Ron (Tutor académico)
- Jhon Arcos (Estudiante)
- Roberto Espín (Estudiante)

Equipos, instalaciones y materiales

- Servidor Kali

- Intel Core i7 3930k
- 16 GB RAM
- 1 TB de disco duro
- SO Kali Linux 64 bits
- Laboratorio ESPE-CERT
- 2 laptops

Conocimiento / Experiencia

- Documentación previa

Software, Hardware

- EJBCA Community versión 7.9
- Docker
- MySQL
- Any Desk

Ejecución del plan de transición

Preparación del Hardware e infraestructura física

Para el funcionamiento de EJBCA existen ciertos prerrequisitos, cumplidos a cabalidad en el ESPE-CERT, los mismos que permitieron la adecuada instalación y funcionamiento del servicio PKI-ESPE. En un inicio se realizó pruebas con la instalación del aplicativo directamente en el servidor, pero debido a otros servicios que se encuentran funcionando en el mismo se decidió optar por contenedores Docker.

Docker permite simplificar y acelerar el flujo de trabajo ya que brinda la libertad de innovar con diferentes herramientas a disposición, diversas aplicaciones y entornos de implementación válidos para este proyecto.

Docker simplifica la instalación del aplicativo, pudiendo realizarlo en cualquier servidor y permite migrar el servicio a necesidad del administrador, permitiendo levantar el servicio de forma rápida y eficiente, además los recursos consumidos son menores y ya vienen preconfigurados facilitando su uso.

Capacitación técnica para el uso de la infraestructura

Los miembros del ESPE CERT, el tutor del proyecto, así como el personal involucrado en el proyecto “Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente”, desarrollado en febrero de 2022, realizó una capacitación orientada al manejo y administración de los servidores

Implantación de la herramienta de administración

1. Instalación de la base de datos

Debido a la necesidad del acceso a la base de datos de manera externa para funciones de supervisión y administración, se decidió usar la base de datos MySQL alojada directamente en el servidor, la misma que cuenta con los datos necesarios para levantar el servicio EJBC en cualquier lugar de la intranet y permitirle el acceso a la misma de forma inmediata.

Los pasos seguidos para la instalación de MYSQL en el servidor se detallan a continuación.

1.1. Se realiza una actualización del sistema mediante el comando: sudo apt update.

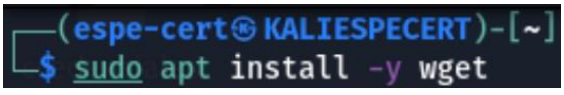
Figura 1

Actualización del sistema

1.2. Se instala el servicio wget con el comando: sudo apt install -y wget

Figura 2

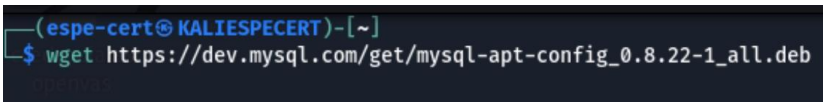
Servicio wget



1.3. Se agrega el repositorio APT de MYSQL mediante el comando: wget https://dev.mysql.com/get/mysql-apt-config_0.8.22-1_all.deb

Figura 3

Repositorio APT



1.4. Se configura el repositorio MySQL mediante el comando: sudo apt install./mysql-apt-config_0.8.22-1_all.deb

Figura 4

Comando apt install

1.5. Debido a que no existe una versión compatible se debe elegir la versión Debian Bullseye.

Figura 5

Debian Bullseye

1.6. Se debe seleccionar la opción Server y Cluster y posteriormente OK.

Figura 6

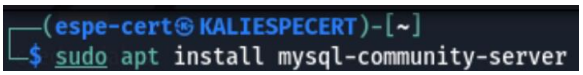
Server y Cluster

1.7. Se realiza una actualización del sistema mediante el comando: sudo apt update.

1.8. Una vez agregado el repositorio, se instala mysql-server mediante el comando: sudo apt install mysql-community-server.

Figura 7

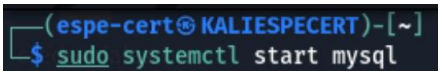
Comando sudo apt



1.9. Se realiza la instalación de MySQL con los parámetros por defecto, y cuando se encuentre instalado en su totalidad se debe levantar el servicio mediante el comando: sudo systemctl start mysql.

Figura 8

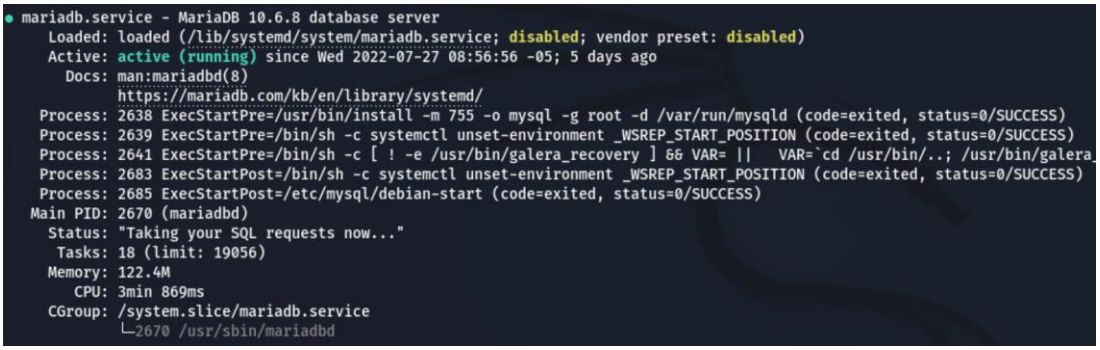
comando sudo systemctl



1.10. Se puede verificar el estado del servicio mediante el comando: sudo systemctl status mysql.

Figura 9

sudo systemctl



1.11. Se procede a ingresar al servicio MYSQL y crear el usuario de EJBCA mediante los comandos:

mysql -u root -p

CREATE USER 'ejbca'@'localhost' IDENTIFIED BY 'password';

1.12. Se debe crear la base de datos mediante el siguiente comando: CREATE DATABASE ejbca CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

1.13. Finalmente se agregan los privilegios para el acceso por parte del usuario “ejbca” mediante el comando: GRANT ALL PRIVILEGES ON ejbca.* TO 'ejbca'@'localhost';

1.14. Se ejecuta el comando necesario para usar la base de datos “ejbca”: USE jbca;

2. Instalación de Docker

2.1. Se debe añadir la clave PGP de Docker mediante el comando: curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -

2.2. Configurar el repositorio de Docker mediante la instrucción: echo 'deb https://download.docker.com/linux/debian stretch stable' > /etc/apt/sources.list.d/docker.list

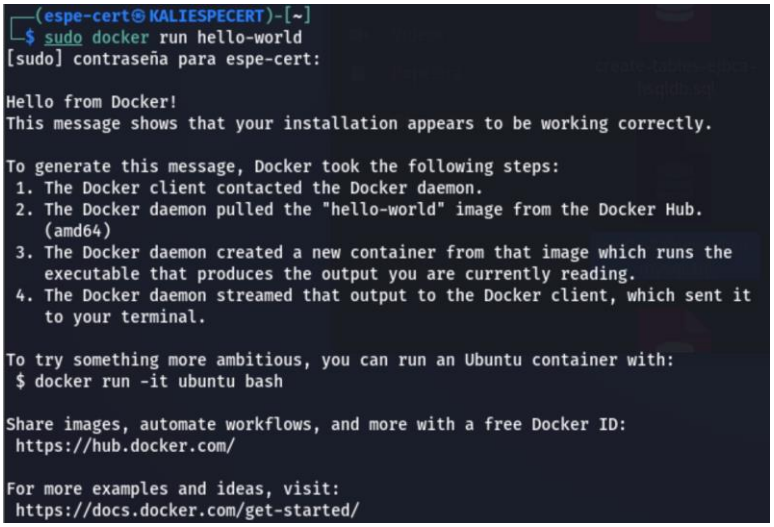
2.3. Es necesario actualizar el sistema mediante el comando: apt-get update

2.4. Se procede a instalar Docker mediante el comando: apt-get install docker-ce

2.5. Comprobar si Docker se instaló correctamente mediante el comando: docker run hello-world.

Figura 10

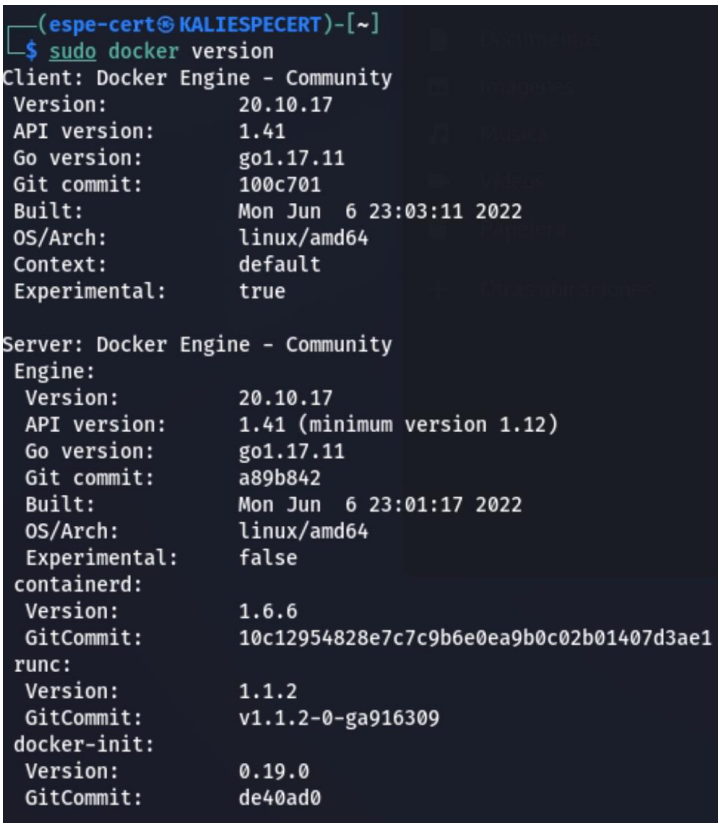
comando docker



2.6. Comprobar la versión de Docker instalada mediante el comando: docker versión.

Figura 11

comando docker



3. Levantamiento del contenedor con EJBCA

Para ejecutar el contenedor EJBCA, un sistema debe contar con al menos dos núcleos de CPU y al menos 1 GB o RAM por lo que en el servidor destinado no existe ningún inconveniente.

3.1. Se debe ejecutar el comando Docker en el que se descarga la imagen de EJBCA y se configura las variables de entorno correspondientes a la base de datos para levantar el contenedor: sudo docker run -it --rm -p 80:8080 -p 443:8443 -h mycahostname -e "DATABASE_JDBC_URL=jdbc:mysql://10.9.9.243:3306/ejbca" -e "DATABASE_USER=ejbca" -e "DATABASE_PASSWORD=password" keyfactor/ejbca-ce.

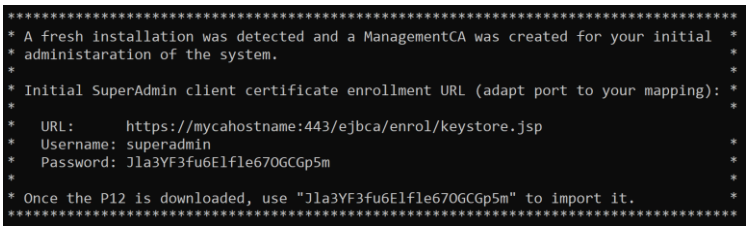
Figura 12

Levantamiento contenedor

3.2. En la consola de ejecución se presentará la información referente a la primera vez que se carga el sistema EJBCA.

Figura 13

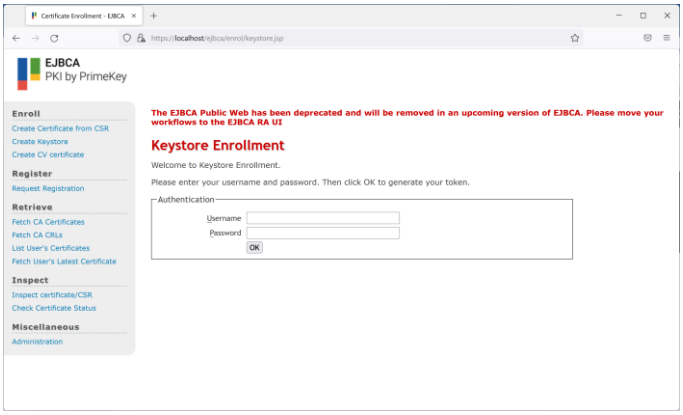
sistema EJBCA



3.3. Se debe copiar la URL, sin embargo, direccionarla a la dirección local.

Figura 14

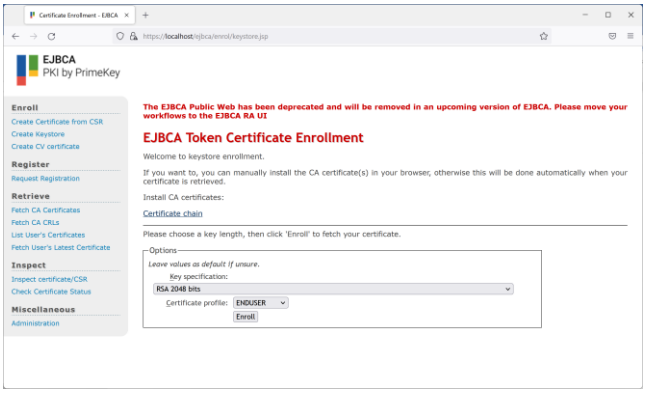
dirección local



3.4. Se debe ingresar el usuario y contraseña de superadmin mostrada en la consola de ejecución y cuando permita descargar el certificado se debe seleccionar el algoritmo RSA 2048.

Figura 15

Algoritmo RSA



3.5. Se descargará el certificado “Superadmin.p12”.

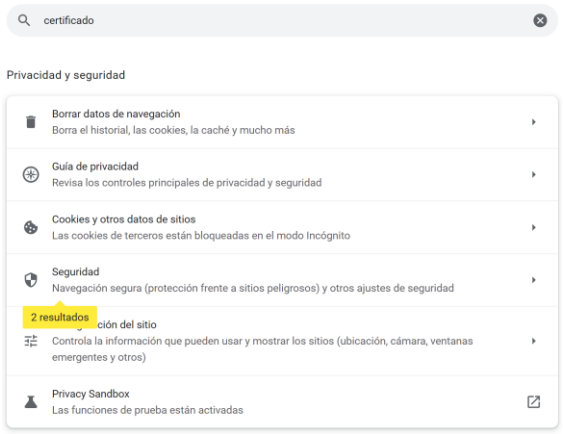
Figura 16

Descarga

3.6. Se debe agregar este certificado al navegador, por lo que se abre la configuración del navegador y se busca “certificado”.

Figura 17

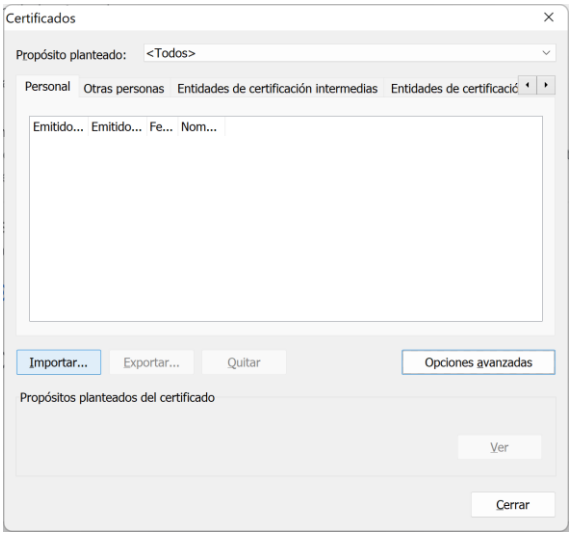
Configuración



3.7. En el apartado de seguridad se accede a “Gestionar certificados” y se da clic en “Importar”.

Figura 18

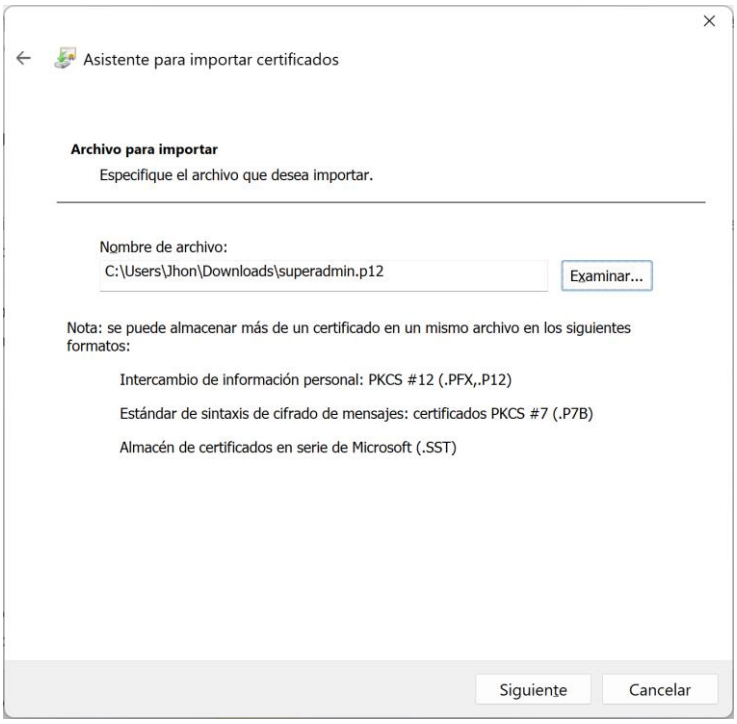
Gestión de certificados



3.8. Se selecciona el archivo descargado “superadmin.p12”.

Figura 19

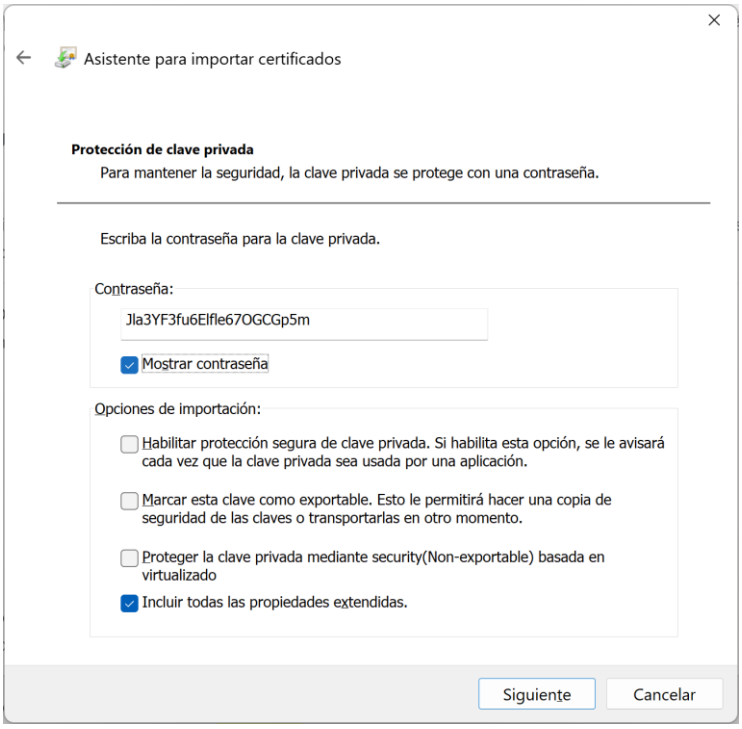
superadmin.p12



3.9. Se coloca la contraseña provista para el superadmin en la consola de ejecución.

Figura 20

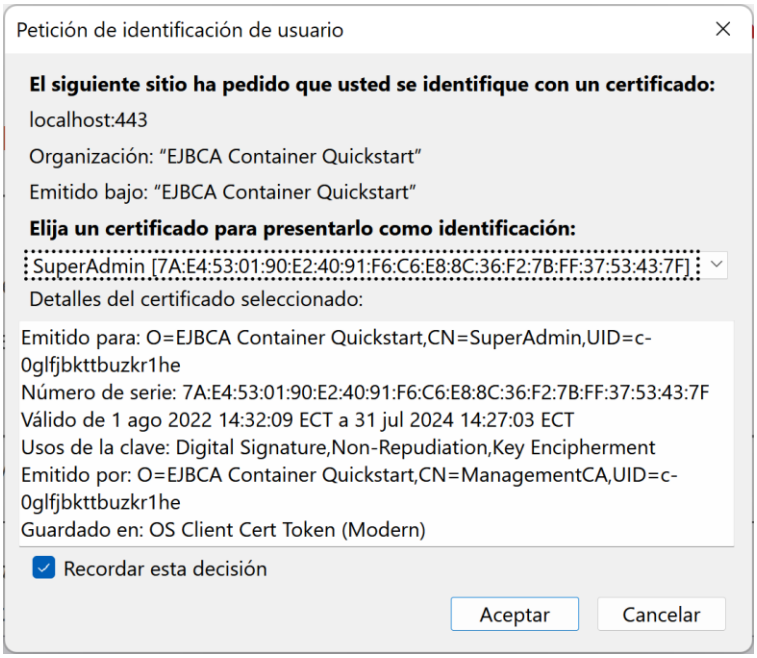
superadmin consola



3.10. Una vez agregado el certificado, este se encontrará disponible para su uso, se debe acceder a la dirección: https://localhost/ejbca/adminweb/, aquí se pedirá un certificado por lo que se debe seleccionar Superadmin y aceptar.

Figura 21

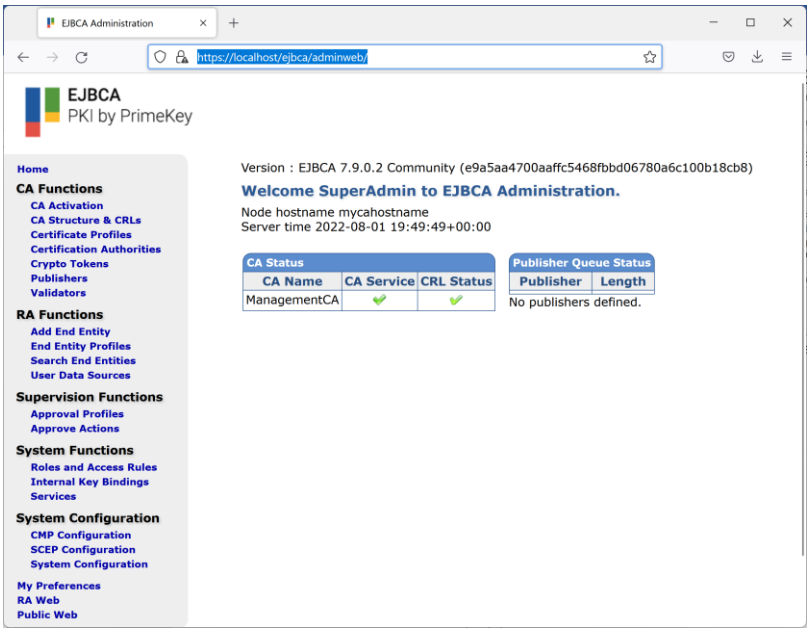
Superadmin y aceptar



3.11. Se ingresará a la consola de administración.

Figura 22

consola de administración



3.12. Se accede al menú y se selecciona la opción de Perfiles de Certificado.

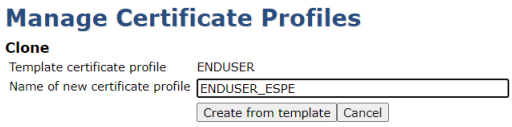
Figura 23

Perfiles de Certificado

3.13. Se procede a clonar el perfil ENDUSER con el nombre de ENDUSER_ESPE.

Figura 24

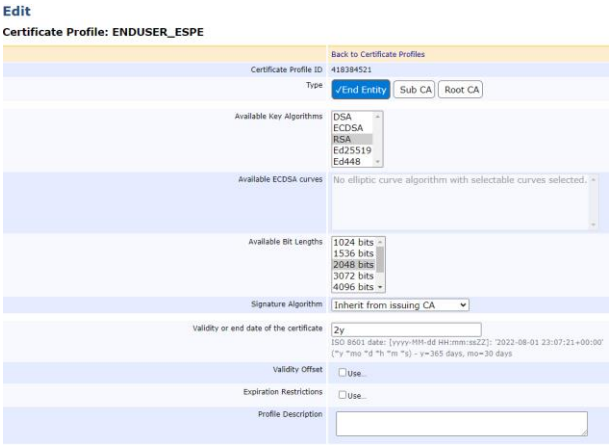
ENDUSER_ESPE



3.14. Se debe completar los datos en la opción de editar el perfil del certificado.

Figura 25

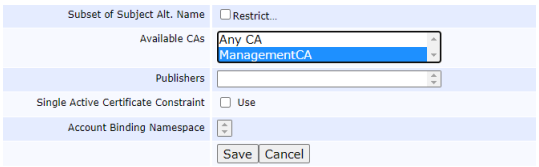
perfil del certificado



3.15. En la opción de CAs disponibles se selecciona la Autoridad de Registro ManagementCA.

Figura 26

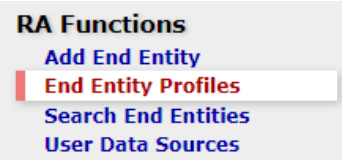
Registro ManagementCA



3.16. En el menú se selecciona Perfiles de Entidad Final.

Figura 27

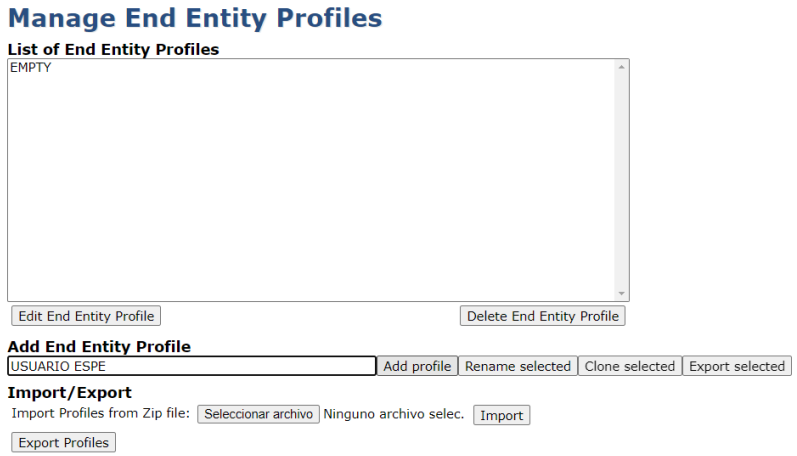
Perfiles de Entidad



3.17. Se agrega un nuevo perfil llamado USUARIO ESPE.

Figura 28

USUARIO ESPE



3.18. Se debe editar el perfil creado recientemente.

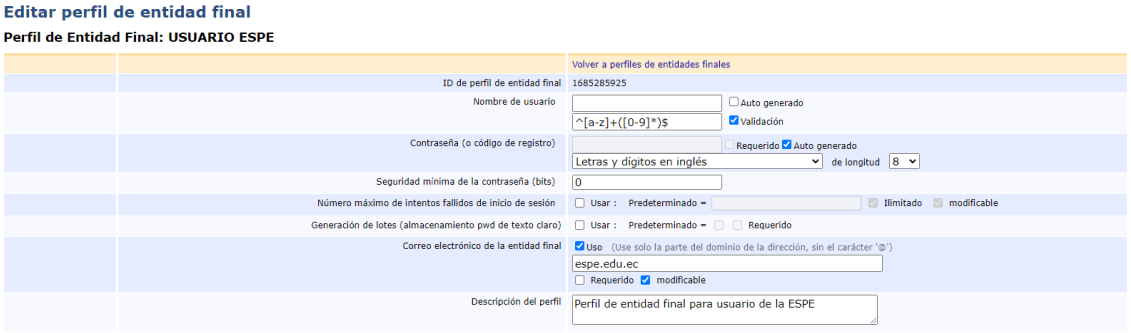
Validación del nombre de usuario: ^[a-z]+([0-9]*)$

Correo electrónico de entidad final: espe.edu.ec

Descripción del perfil: Perfil de entidad final para usuario de la ESPE

Figura 29

usuario de la ESPE



3.19. Para los campos de distinción debe tener las siguientes características.

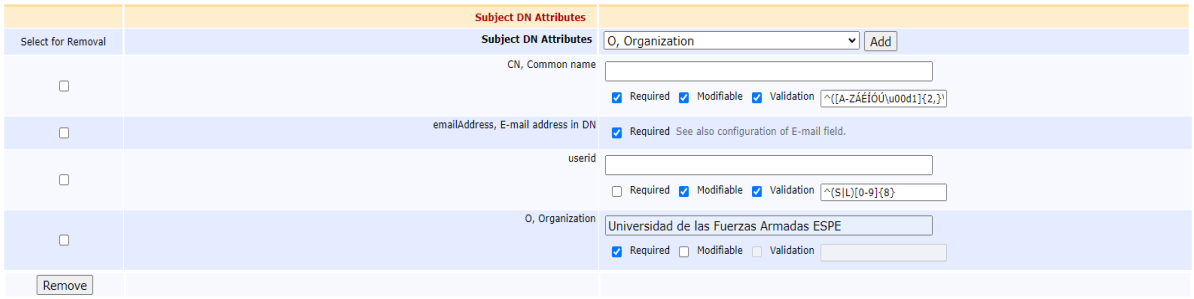
Validación de nombre común: ^([A-ZÁÉÍÓÚ\u00d1]{2,}\s[A-ZÁÉÍÓÚ\u00d1]{2,}\s[A-ZÁÉÍÓÚ\u00d1]{2,}\s[A-ZÁÉÍÓÚ\u00d1]{2,}\s)

Validación de identificador único: ^(S|L)[0-9]{8}

Organización: Universidad de las Fuerzas Armadas ESPE

Figura 30

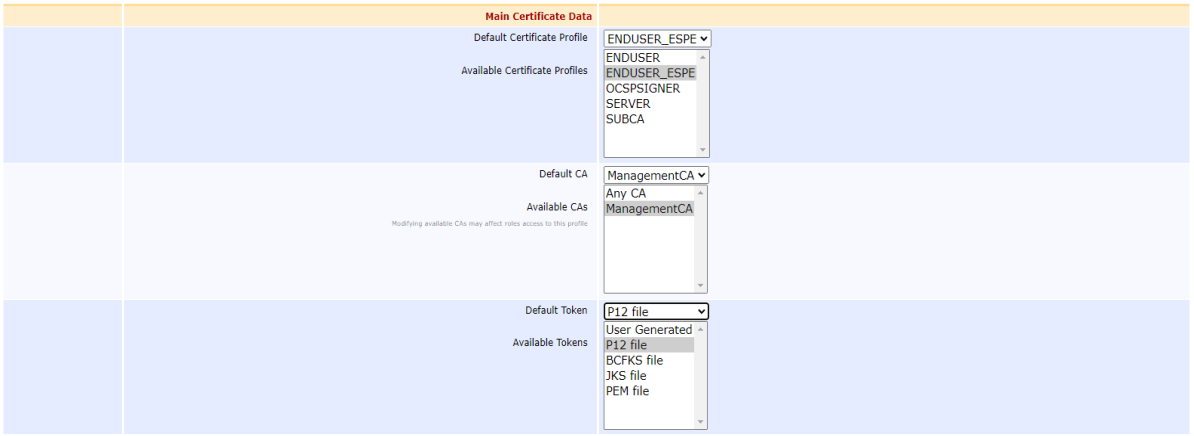
campos de distinción



3.20. En los datos del certificado se debe seleccionar ENDUSER_ESPE, ManagmentCA y P12 file.

Figura 31

ENDUSER_ESPE



3.21. Se configura el envío por correo electrónico donde la notificación puede ser la siguiente:

Estimado(a) Usuario(a) ${CN}

Su certificado digital en ESPE PKI ha sido generado, su contraseña es: ${PASSWORD}

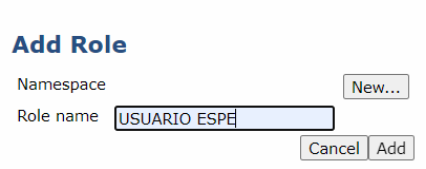
Figura 32

ESPE PKI

3.22. En el menú se debe agregar un nuevo rol con el nombre USUARIO_ESPE.

Figura 33

agregar un nuevo rol



3.23. Se debe dar clic en Miembros.

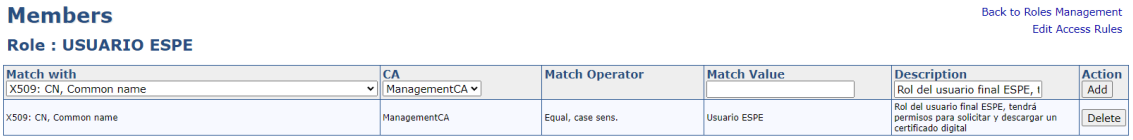
Figura 34

clic en Miembros

3.24. Se agrega un nuevo miembro, con el nombre común, valor de coincidencia Estudiante ESPE y la descripción.

Figura 35

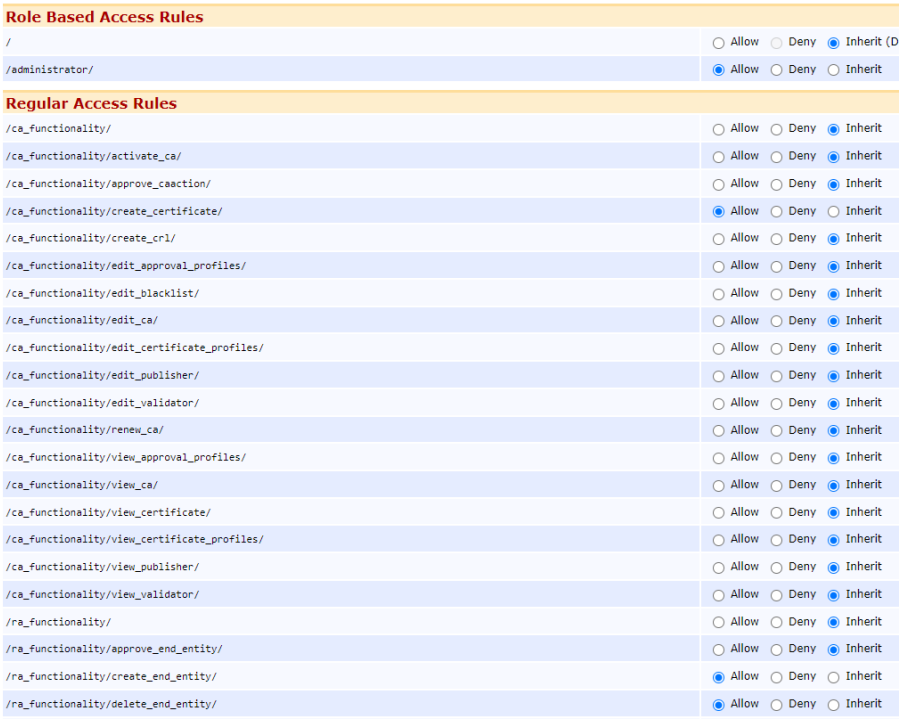
valor de coincidencia Estudiante



3.25. Se da clic en Editar reglas de acceso en modo avanzado y se le asignan los permisos de administrador, así como la creación, eliminación y visualización de entidades finales.

Figura 36

eliminación y visualización de entidades finales



3.26. Se modifican las reglas de acceso de perfiles de entidades Finales.

Figura 37

reglas de acceso de perfiles

3.27. Se deja por defecto el resto de opciones y se guarda los cambios

Capacitación de usuarios

Para los usuarios finales del sistema se generó un certificado genérico que permita la generación de un certificado personal descargado de manera automática, estas instrucciones fueron remitidas al correo electrónico de cada usuario.

1. Correo electrónico recibido por el usuario

Estimados docentes y estudiantes.

Como parte del Proyecto de Investigación: “Firma digital para asegurar la integridad y autenticación de origen de los documentos enviados por los estudiantes de la Universidad de las Fuerzas Armadas ESPE” y el Trabajo de Titulación: “Transición, Operación y Mejora del Servicio de Firma Electrónica en el Departamento de Ciencias de la Computación”, se ha iniciado la fase de implementación de este servicio para docentes y estudiantes del Departamento de Ciencias de la Computación (Matriz – Sangolquí), por tanto su participación en esta fase es muy importante para la transformación digital de nuestra Universidad.

Participar en la fase de implementación le permitirá generar un certificado con el que podrá firmar documentos digitales, cabe considerar que la certificación es interna por lo que no servirá para trámites fuera de la institución. La firma electrónica será aceptada internamente en el Departamento de Ciencias de la Computación.

El servicio de firma digital, permite mejorar la seguridad de la información y facilitar los trámites internos. En el futuro se pretende conseguir la certificación que establece la Ley de Comercio Electrónico para los entes proveedores de firma electrónica.

Los beneficios de usar una firma electrónica son los siguientes:

Una firma electrónica identifica y certifica al autor del documento electrónico y protege la integridad de la información contenida en él, de esta manera quien recibe está seguro del origen y contenido del documento y quien la envía no puede negar su autoría.

El uso de la firma electrónica permitirá un ahorro significativo de tiempo en procesos, papel, espacio y transporte.

Adjuntamos el manual de uso de la firma electrónica mediante el sistema PKI para los miembros de la Universidad de las Fuerzas Armadas ESPE. Además, también le enviamos un archivo con su certificado de acceso a la plataforma (Usuario ESPE.p12) para que active el proceso de obtención de su firma electrónica.

Puede encontrar un video Tutorial explicativo en el siguiente link:

https://drive.google.com/file/d/1v-Pglhwj16NFN78aMA4gJzCDNhAud5Jw/view?usp=sharing

La aplicación para manejo de pdf (PDF-XChange) puede encontrar en el siguiente link:

https://drive.google.com/file/d/1Lz8fLlMoK4sqM9bLVr4lc3Tpf1XdS3oI/view?usp=sharing

El acceso al servicio PKI ESPE, lo puede hacer a través del link:

https://10.9.9.243/ejbca/ra

NOTA: Es necesario que se encuentre conectado a la intranet de la Universidad de las Fuerzas Armadas ESPE (Matriz – Sangolquí) para realizar el proceso de creación de su certificado.

En caso de cualquier duda, sugerencia o requerimiento de soporte, comuníquese con el equipo PKI ESPE mediante el correo electrónico de soporte: jdarcos@espe.edu.ec

Agradecemos por el tiempo destinado a la participación en este proyecto de gran importancia para nuestra querida Universidad.

PROYECTO DE FIRMA DIGITAL ESPE

2. Pasos a seguir por el usuario

Como parte del Proyecto de Investigación: “Firma digital para asegurar la integridad y autenticación de origen de los documentos enviados por los estudiantes de la Universidad de las Fuerzas Armadas ESPE” y el Trabajo de Titulación: “Transición, Operación y Mejora del Servicio de Firma Electrónica en el Departamento de Ciencias de la Computación”, se ha iniciado la fase de implementación de este servicio para docentes y estudiantes del Departamento de Ciencias de la Computación (Matriz – Sangolquí), por tanto su participación en esta fase es muy importante para la transformación digital de nuestra Universidad.

Participar en la fase de implementación le permitirá generar un certificado con el que podrá firmar documentos digitales, cabe considerar que la certificación es interna por lo que no servirá para trámites fuera de la institución. La firma electrónica será aceptada

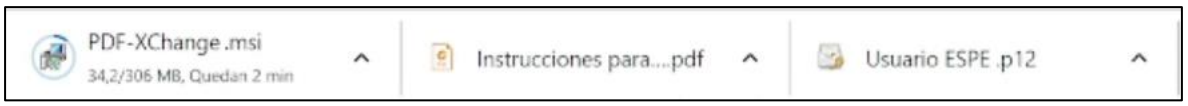
internamente en el Departamento de Ciencias de la Computación.

El servicio de firma digital, permite mejorar la seguridad de la información y facilitar los trámites internos. En el futuro se pretende conseguir la certificación que establece la Ley de Comercio Electrónico para los entes proveedores de firma electrónica. A continuación, encontrará las instrucciones para acceder a su certificado de firma digital:

2.1. Descargue el certificado de “Usuario ESPE.p12”, el aplicativo PDF-XChange y las instrucciones para el uso.

Figura 38

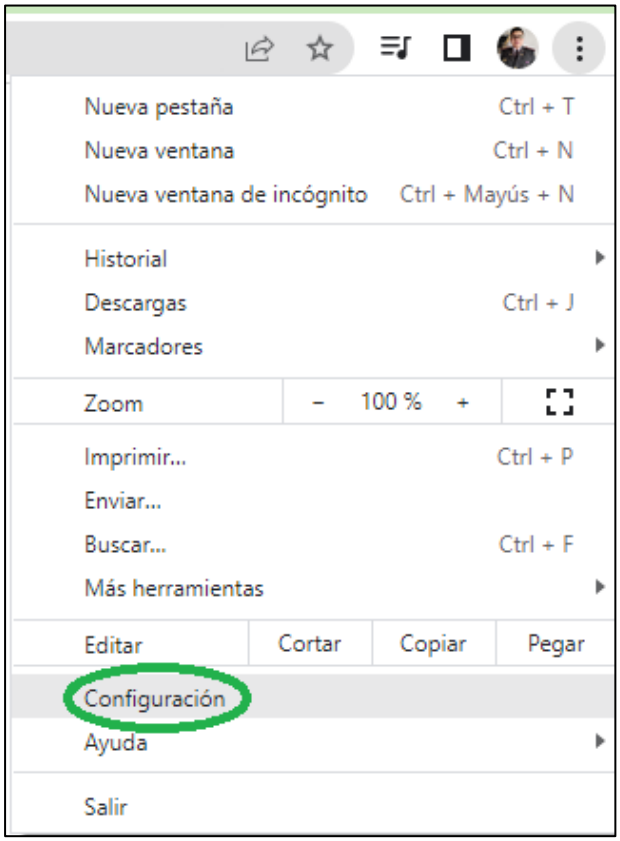
Usuario ESPE.P12



2.2. En una nueva pestaña en su navegador (Google Chrome para este ejemplo), ingrese a la opción de configuración.

Figura 39

pestaña en su navegador



2.3. En la barra de búsqueda en la configuración se ingresa la palabra “certificado” y busque el apartado de “Seguridad” y dé clic.

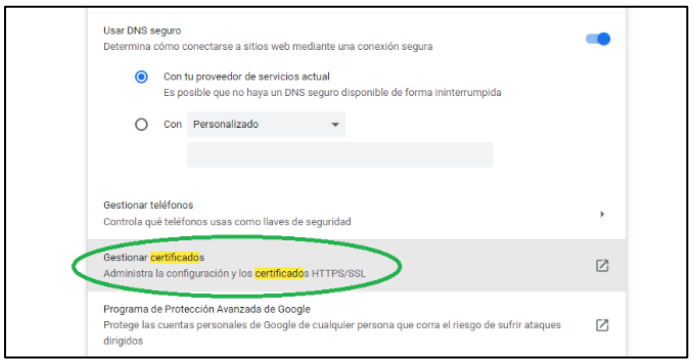
Figura 40

palabra “certificado”

2.4. Dentro de este submenú busque la opción de “Gestionar certificados” y dé clic.

Figura 41

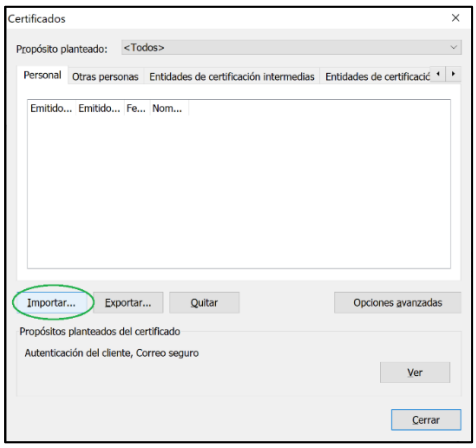
Gestionar certificados



2.5. Seleccione la opción de importar certificado.

Figura 42

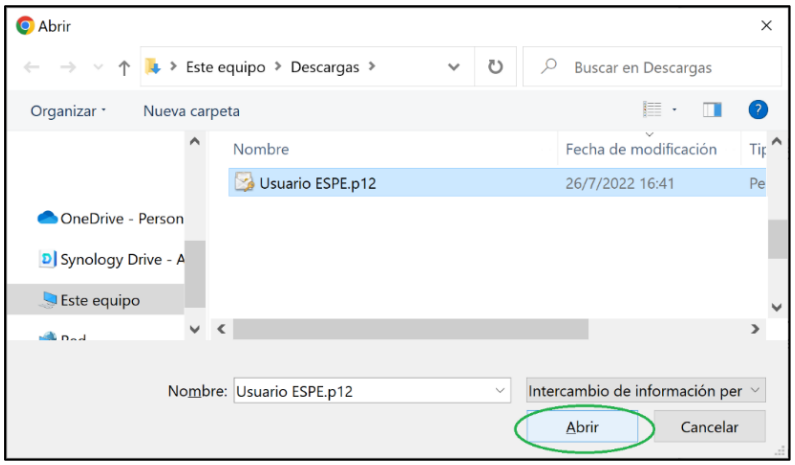
importar



2.6. Seleccione el certificado correspondiente y de clic en “Abrir”.

Figura 43

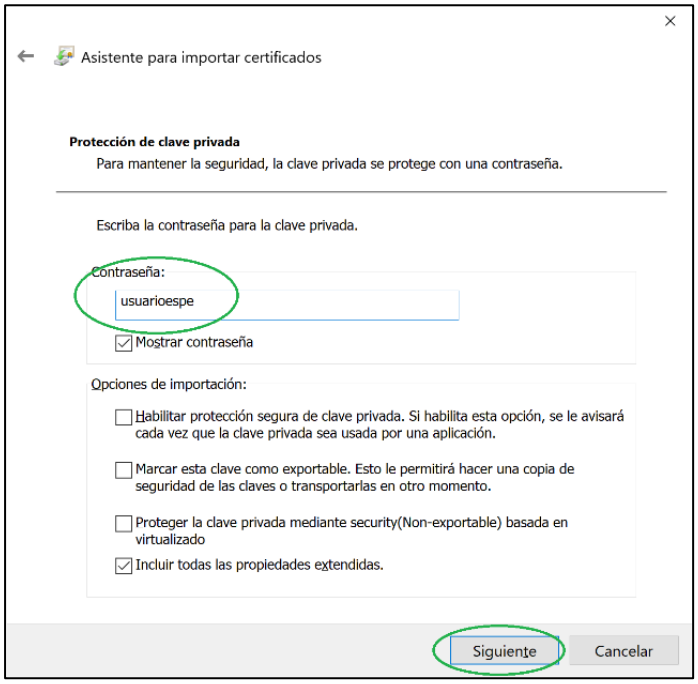
Abrir



2.7. Ingrese la contraseña “usuarioespe” y luego clic en Siguiente.

Figura 44

ingreso de contraseña



2.8. Conectado a la intranet de la ESPE, es decir, conectado a la red inalámbrica “ESPE”, “ESPE-WIFI” o red alámbrica, ingrese al link https://10.9.9.243/ejbca/ra/, en caso de que su navegador no permita el acceso debido al tipo de conexión ingrese a configuración avanzada y posteriormente acceda al sitio.

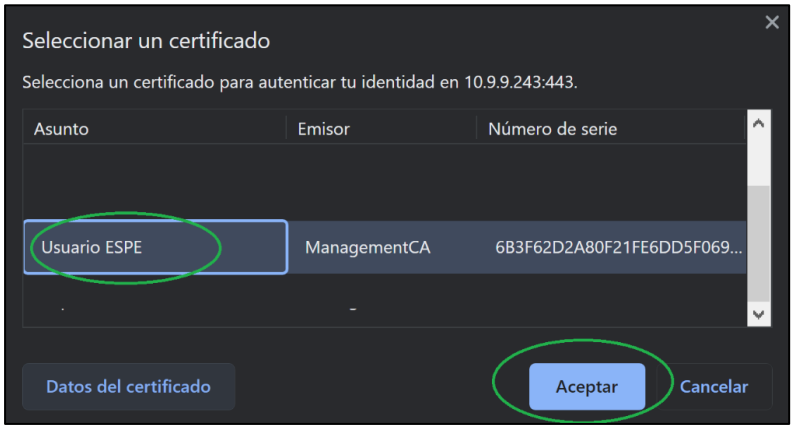
Figura 45

acceso

2.9. Se debe seleccionar un certificado, para lo que debe seleccionar el certificado instalado previamente.

Figura 46

seleccionar certificado



2.10. Seleccione “Hacer nueva solicitud”

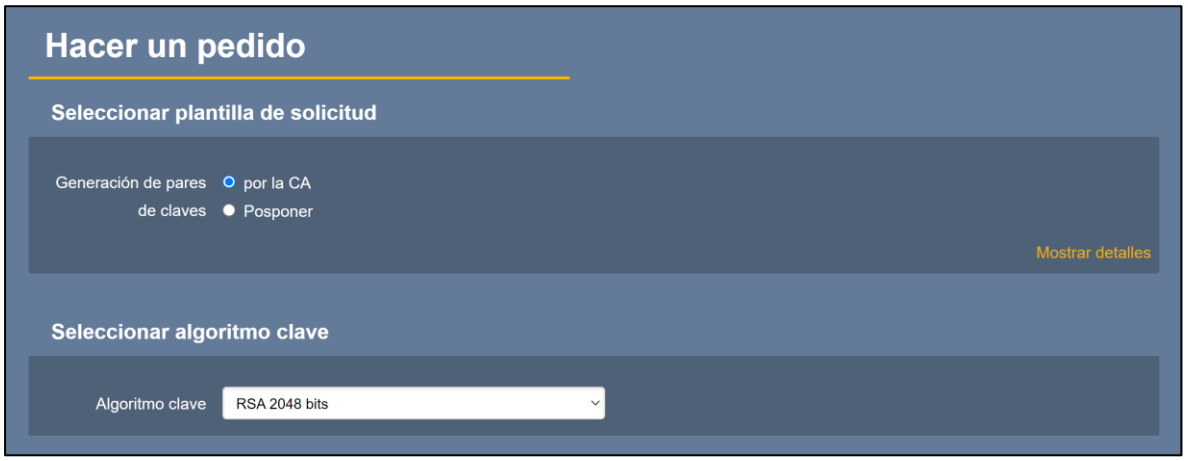
Figura 47

Nueva solicitud

2.11. Seleccione las opciones de “por la CA” y algoritmo RSA 2048 bits

Figura 48

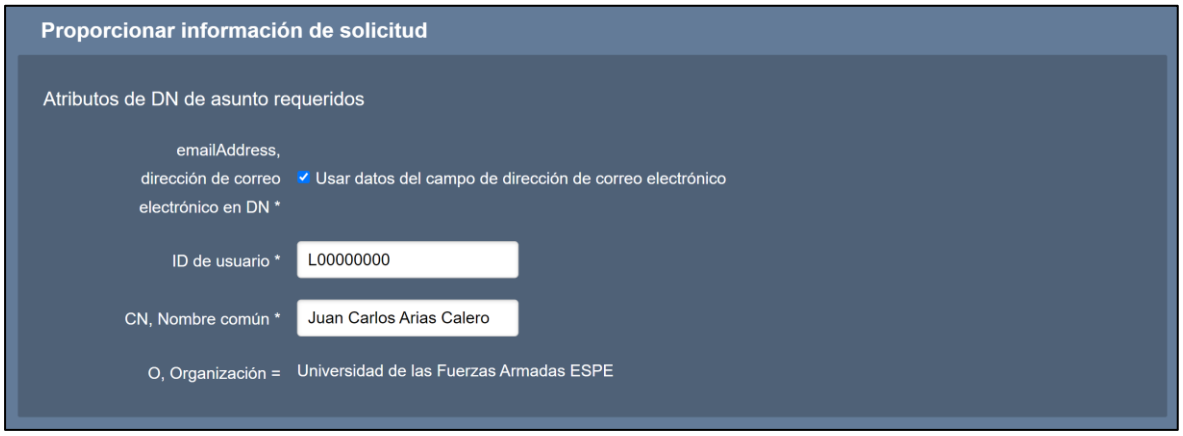
Hacer pedido



2.12. Ingrese las credenciales personales de la ESPE (ID Banner y Nombres completos).

Figura 49

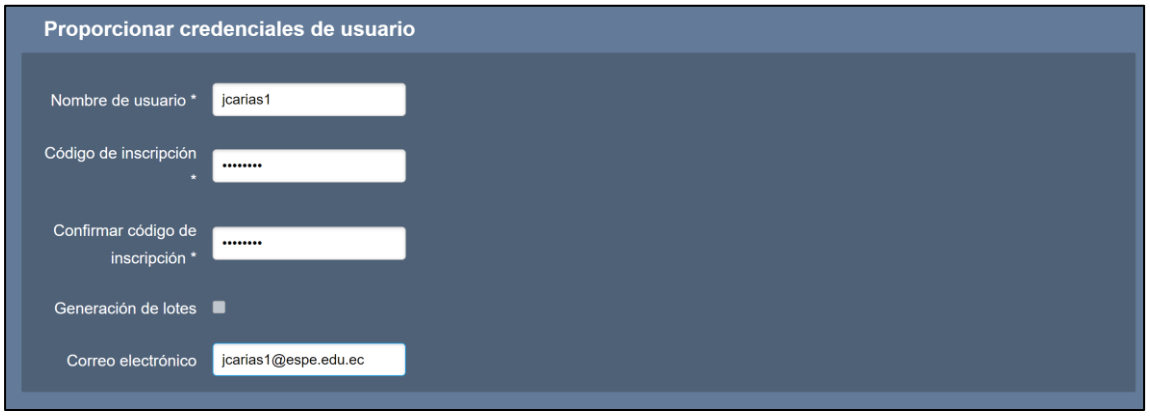
ID Banner



2.13. Ingrese las credenciales del usuario, usando el usuario de la UFA ESPE, una contraseña que recuerde (será usada con su firma digital en el futuro) y correo electrónico institucional.

Figura 50

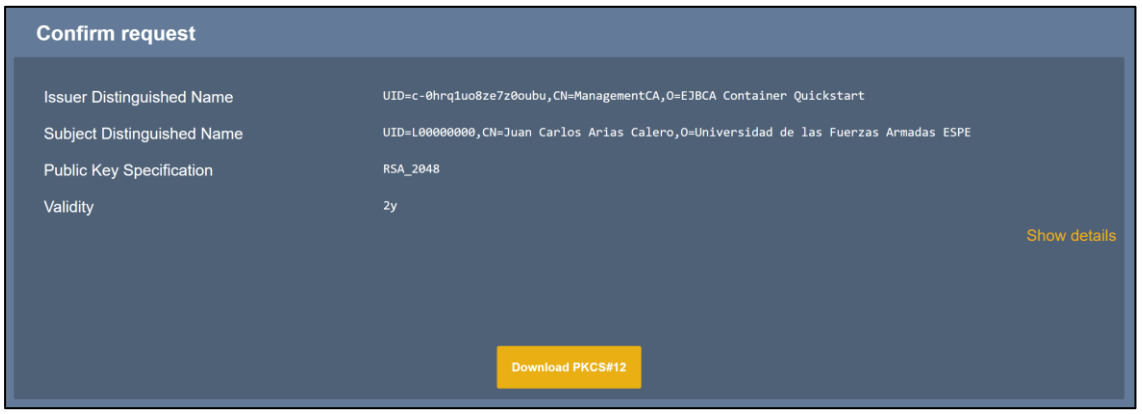
UFA ESPE



2.14. Confirme la petición y proceda con la descarga.

Figura 51

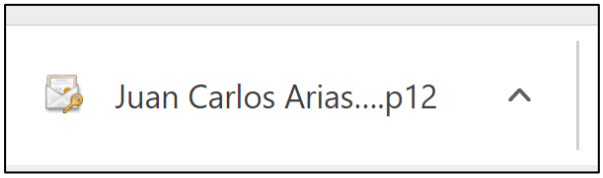
Petición



2.15. Ya cuenta con el certificado digital del usuario.

Figura 52

Certificado digital



2.16. Proceda a la instalación del aplicativo PDF-XChange ejecutando el archivo adjunto al correo y seleccionando las opciones por defecto.

Figura 53

PDF-Xchange

2.17. Una vez finalizada la instalación ya puede ejecutar la aplicación.

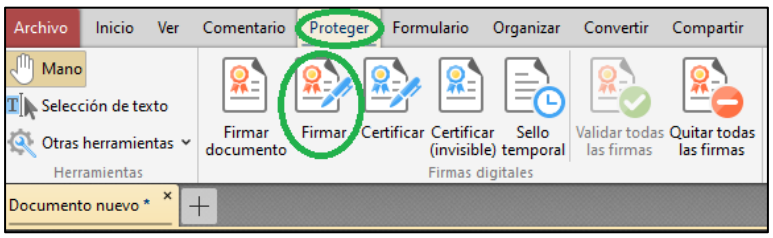
Figura 54

Instalación

2.18. En la aplicación, abra el documento que requiere firmar digitalmente, busque el apartado de “Proteger” y presione “Firmar”.

Figura 55

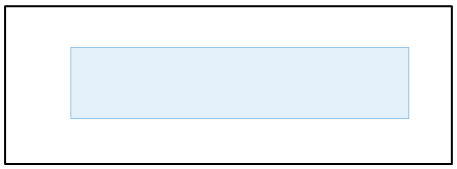
Proteger” y presione “Firmar”



2.19. Seleccione el área donde requiere la firma digital.

Figura 56

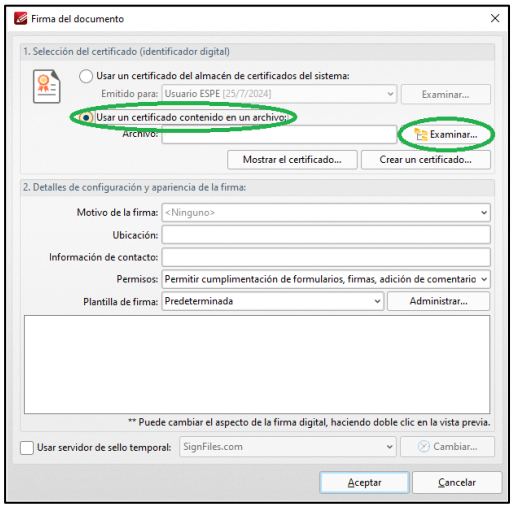
firma digital



2.20. Seleccione la opción “Usar un certificado contenido en un archivo” y posteriormente dé clic en “Examinar”.

Figura 57

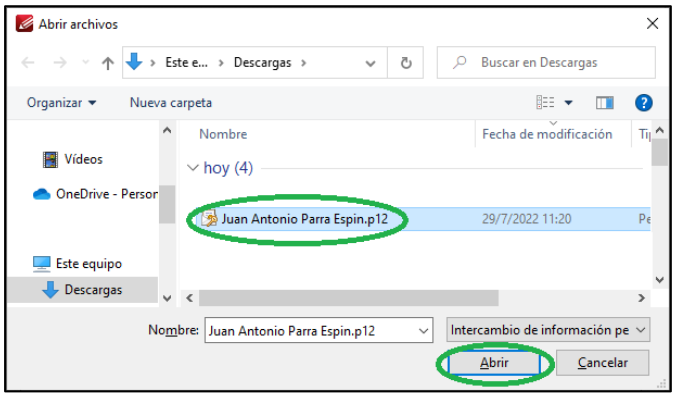
Examinar



2.21. En la ventana emergente seleccione el certificado personal y dé clic en “Abrir”.

Figura 58

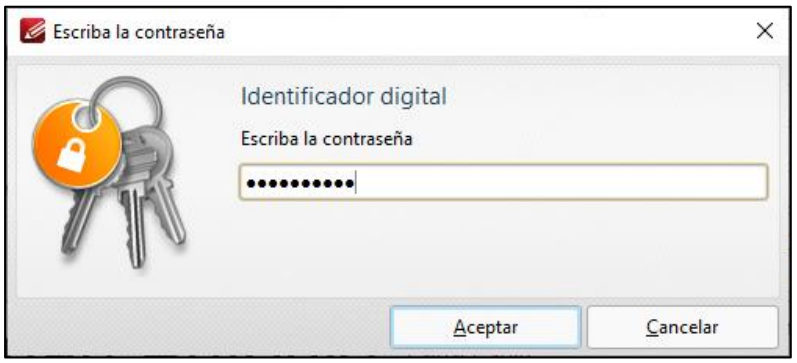
seleccione el certificado personal



2.22. Ingrese la contraseña configurada inicialmente al momento de descargar el certificado y dé clic en “Aceptar”.

Figura 59

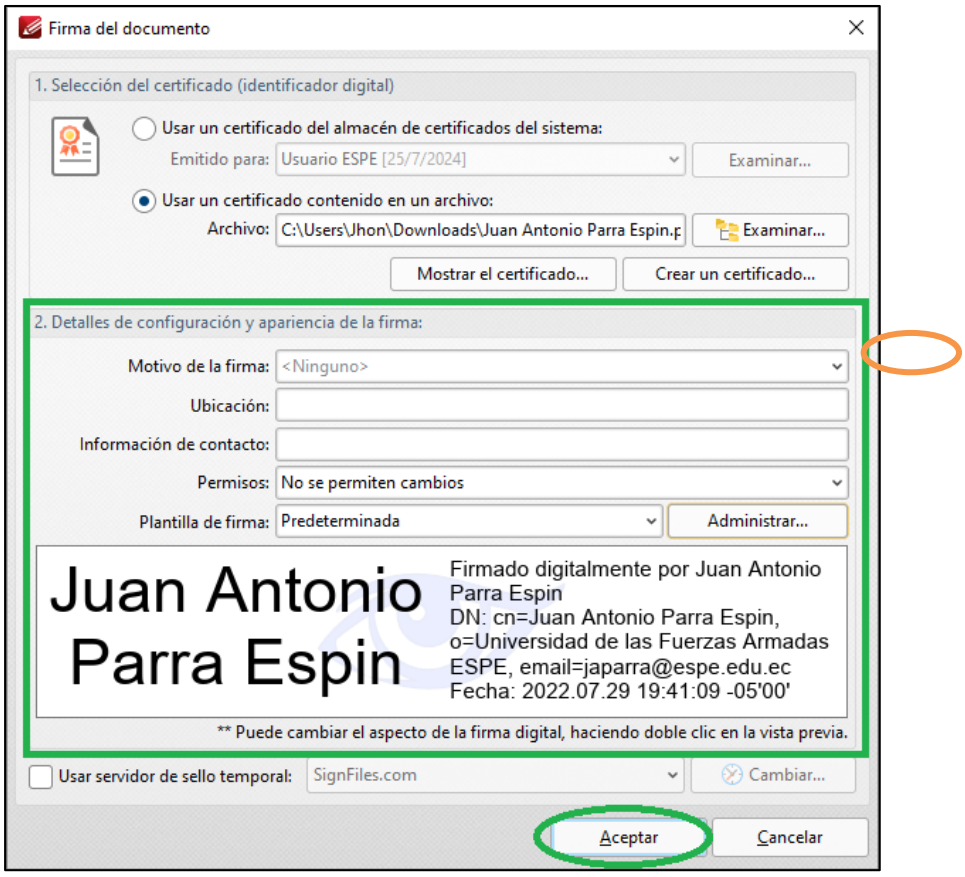
descargar el certificado



2.23. La firma se encontrará disponible para usarse y agregar opciones adicionales o cambiar el formato en la que quiere que se visualice en el documento, puede dar clic en “Aceptar”.

Figura 60

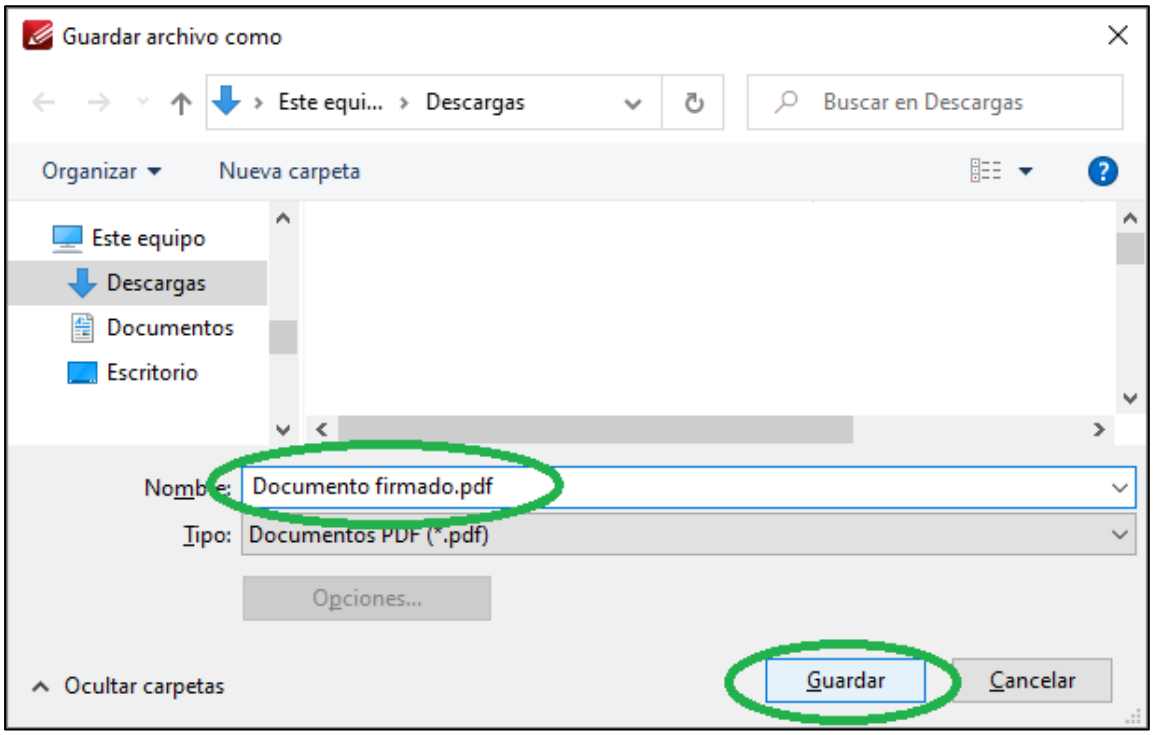
opciones adicionales



2.24. Le pedirá que guarde el documento.

Figura 61

Guardar documento



2.25. El documento se encuentra firmado y de acuerdo a la configuración seleccionada.

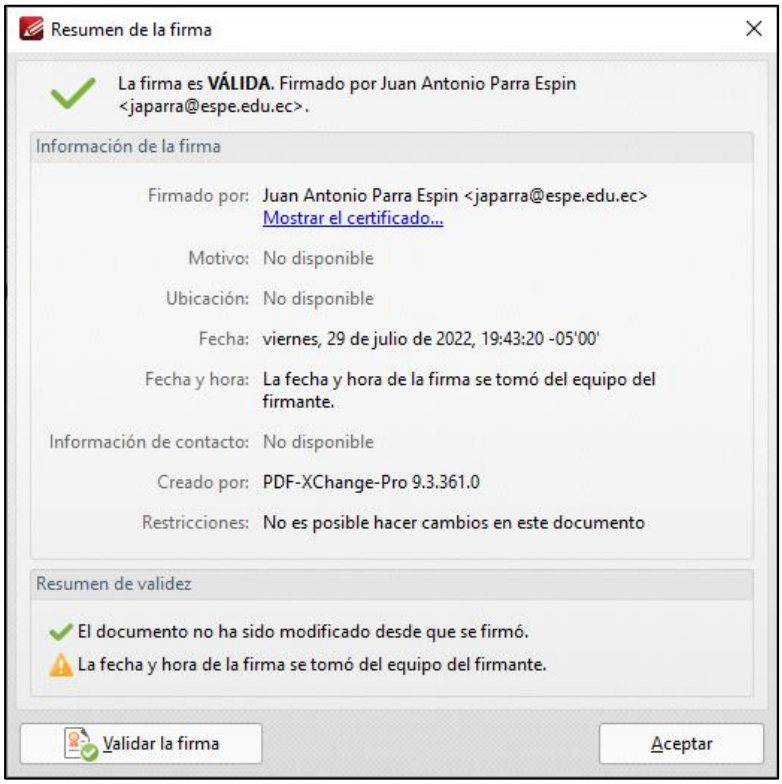
Figura 62

configuración

2.26. Al momento en que cualquier usuario abra el documento y de clic sobre la firma, está se encontrará validada.

Figura 63

validación de firma



Evaluación de la herramienta

Se realizó diversos despliegues previos para evaluar el funcionamiento de la herramienta, así también se puso a prueba el video tutorial y el manual del usuario final con usuarios que desconocían totalmente el uso de la herramienta, llegando a desarrollar un manual de usuario bastante claro y de fácil utilización.

Como parte de esta evaluación previa al despliegue final se consideró la posibilidad de la pérdida total del sistema debido al apagado o reinicio del servidor, por lo que se realizó un simulacro de esta posibilidad, donde se procede a levantar nuevamente los servicios necesarios y ejecución del aplicativo en no más de 10 minutos.

La falencia descubierta es que el laboratorio del ESPE CERT no cuenta con sistemas UPS o de respaldo de energía, los mismos que serían de gran utilidad para mantener el flujo de trabajo y realizar cualquier actividad necesaria para evitar el daño de los equipos o de los aplicativos desplegados.

Pruebas del sistema

Una vez puesto en ejecución la fase de despliegue y operación del servicio PKI ESPE se consideró la interoperabilidad necesaria con otras aplicaciones o programas, por lo que se probó el certificado emitido para la firma digital en diferentes lectores PDF y en diferentes sistemas operativos, siendo legible cualquier documento firmado con el certificado emitido por el sistema.

Figura 64

Validez de la firma en el aplicativo PDF-Xchange Editor en el Sistema Operativo Windows 11

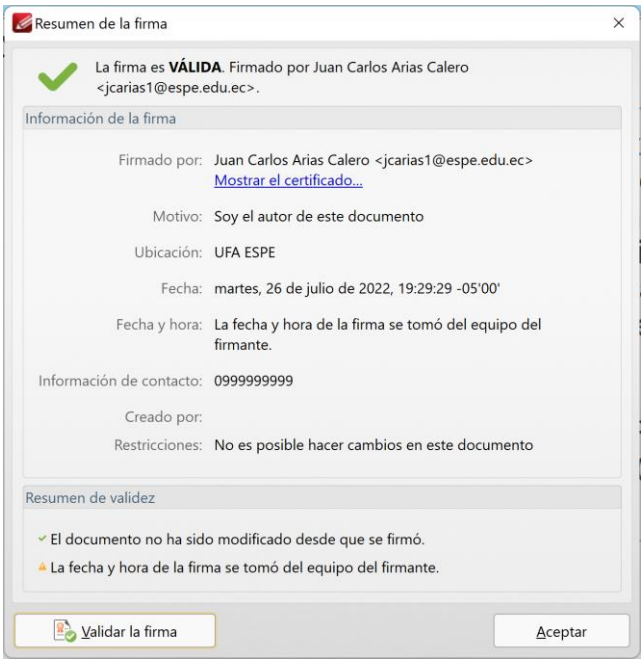


Figura 65

Validez de la firma en el aplicativo Acrobat Reader en el Sistema Operativo MacOS Monterrey versión 12.4.

En lo referente a seguridad, se estableció mecanismos en la herramienta para proteger la información contenida en ella mediante contraseñas seguras para el acceso al servidor, la aplicación y la base de datos. En vista que la herramienta es accesible mediante el protocolo HTTP y HTTPS, para ingresar a la aplicación únicamente se puede acceder desde la intranet (para el proceso de adquisición del certificado), además existe la restricción para que únicamente las personas que cuenten con el certificado genérico inicial puedan tener los permisos necesarios para su correcto acceso.

Una vez generado el certificado digital ya no es necesario estar conectado a la intranet de la Universidad.

Para la escalabilidad de la herramienta se tomó en cuenta que en el futuro se busca implementar la herramienta para todos los miembros de la Universidad de las Fuerzas Armadas ESPE, incluyendo a las diferentes sedes. El servidor asignado es capaz de soportar un alto flujo de peticiones y se ha considerado que es factible instalar un balanceador de carga para direccionar las peticiones entre el servidor actual y el otro disponible en el laboratorio ESPE CERT (Centos), esto solo en caso de ser necesario.

La disponibilidad de la herramienta se puso a prueba midiendo las peticiones realizadas al servidor en relación a las respuestas dadas en un periodo de tiempo, esto se puso a prueba con un curso de 25 estudiantes, los mismos que realizaban peticiones continuas durante un periodo de una hora, aproximadamente hubo un total de 2975 peticiones, respondiéndose adecuadamente 2968, obteniendo una disponibilidad de un 99.76%.

Hay que considerar que las peticiones al servidor se realizan únicamente al momento de generar un certificado y de validarlo, por lo que una vez esté generado el mismo, ya no es necesaria ninguna petición por lo que la disponibilidad no es un factor que puede llegar a afectar sustancialmente las operaciones de certificación de firmas, en todo caso el nivel de disponibilidad es alto, pero se requiere una test de disponibilidad durante un periodo de tiempo mayor para llegar a determinar posibles falencias.

Operación

Prestación del servicio

Prestación del Servicio, se ejecutan los procesos establecidos de acuerdo a la disponibilidad y niveles de servicio establecidos, se mantienen los registros de operación y los reportes correspondientes.

Resolución de incidentes y registro

En base del proceso de resolución de incidentes, se resuelven los incidentes, se actualiza la base de datos de conocimiento y se registra su resolución y escalamiento si fuere del caso.

Capítulo IV

Evaluación y Mejora

Evaluación del servicio

Plan de evaluación

Objetivo

Evaluar el servicio de Firma Electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación.

Alcance

Evaluar el servicio de Firma Electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación, a fin de determinar la funcionalidad y usabilidad del aplicativo PKI ESPE por parte de los estudiantes, docentes y personal administrativo del DCCO. La evaluación se considerará finalizada cuando se emitan los resultados de las evaluaciones a fin de proceder a la elaboración y ejecución de un plan de mejora.

Indicadores de cumplimiento

- Funcionalidad del servicio.
- Usabilidad del servicio.
- Facilidad de aprendizaje.
- Preferencia del servicio.

Recursos

- Humanos

Se cuenta con el docente tutor y los alumnos que se encuentran desarrollando el proyecto de titulación.

- Financieros

No se requiere de recursos financieros en la fase de evaluación del servicio.

- Materiales

Servidor en el laboratorio H202, computadoras personales.

- Tecnológicos

Servicios de internet, repositorios e información disponible.

Tareas a realizar

Se ha definido tareas mediante un cronograma que abarca las actividades necesarias para la evaluación del servicio.

Tabla 5

Tareas y responsables del plan de evaluación

Tarea	Responsable	Duración	Comienzo	Fin
Preparación del método de evaluación.	Estudiantes	3 días	26 jul	28 jul
Aplicación de la evaluación.	Estudiantes	5 días	30 jul	03 ago
Recopilación de resultados.	Estudiantes	2 días	04 ago	05 ago
Realización del informe.	Estudiantes	2 días	06 ago	07 ago

Ejecución de la evaluación

Como parte de la evaluación y a fin de valorar los indicadores de cumplimiento planteados se elaboró una encuesta para medir la funcionalidad y usabilidad del aplicativo PKI ESPE con el certificado digital y su uso para la firma de documentos donde los datos recopilados sirvan para mejorar los procedimientos de obtención del certificado digital se aplicó una encuesta a los usuarios finales.

En esta encuesta se presentan diez preguntas con un sistema de puntuación de 5 puntos (desde “completamente de acuerdo” hasta “Completamente en desacuerdo”), donde se plantean las siguientes interrogantes.

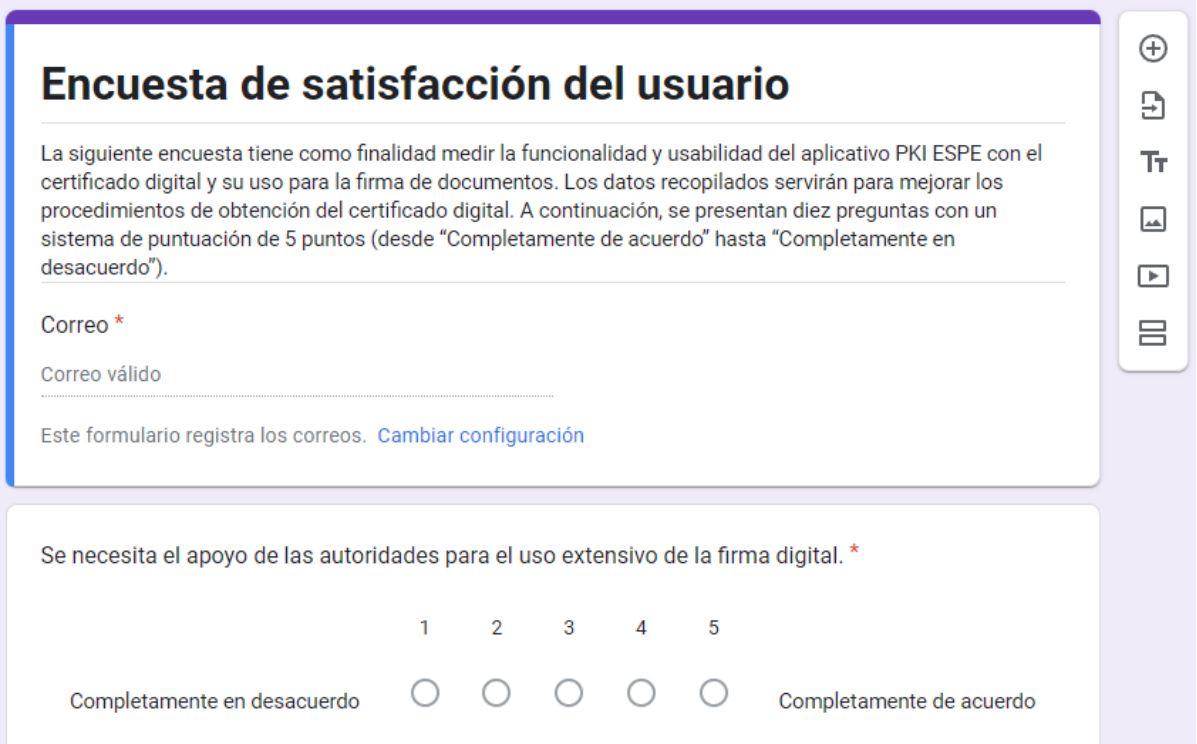
- Se necesita el apoyo de las autoridades para el uso extensivo de la firma digital.
- El sistema para obtener la firma digital me resultó innecesariamente complejo.
- La firma digital es fácil de utilizar.

- Necesitaría el soporte de un técnico para poder utilizar la firma digital.
- La firma digital es de gran utilidad en los procesos internos de la ESPE.
- Hubo dificultades al descargar mi certificado digital.
- Es posible aprender a utilizar la firma digital en forma rápida.
- Prefiero utilizar la firma manuscrita.
- La firma digital es un método seguro para tramitar legalmente un documento.
- Necesito aprender muchas otras cosas antes de utilizar la firma digital.

Para implementar esta encuesta se usó la plataforma de Google Forms, la misma que permite ejecutar la encuesta y recopilar los resultados de manera interactiva, intuitiva y segura.

Figura 66

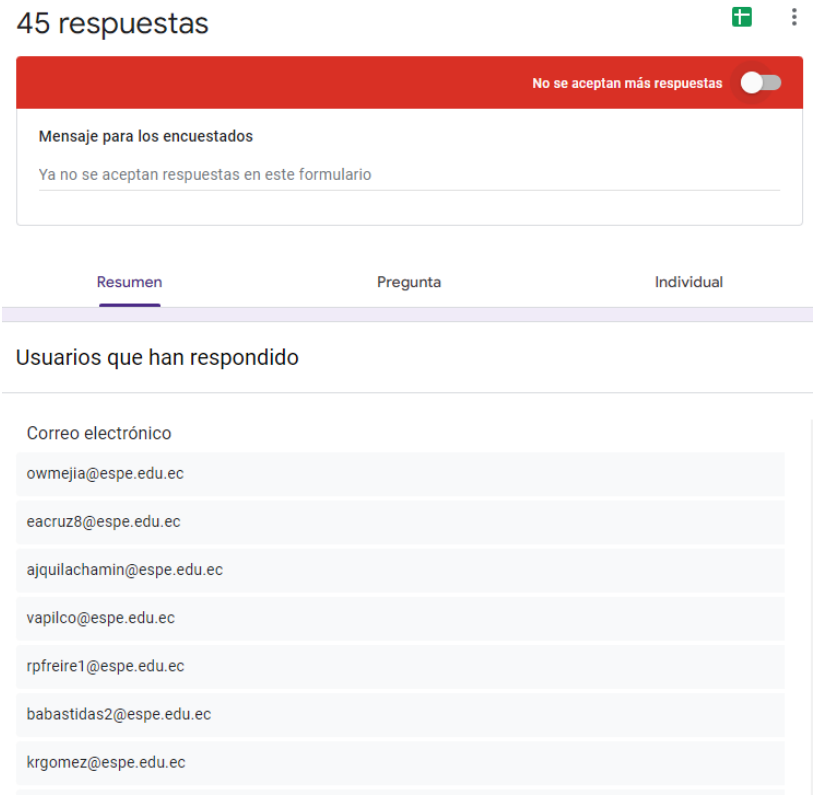
Realización de encuesta en Google Forms



La aplicación de la herramienta de evaluación se realizó mediante el envío por correo electrónico a los docentes y alumnos del DCCO, logrando recopilar 45 encuestas realizadas.

Figura 67

Datos recopilados mediante la aplicación de la encuesta



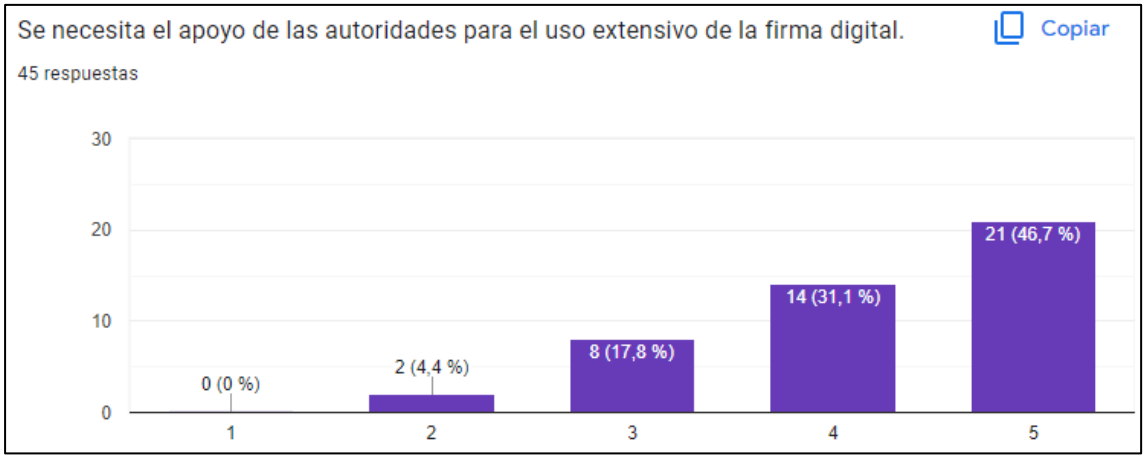
Cada una de las interrogantes planteadas permitió determinar diversos resultados concluyentes referentes a funcionalidad y usabilidad del aplicativo PKI ESPE.

Pregunta 1

Se necesita el apoyo de las autoridades para el uso extensivo de la firma digital.

Figura 68

Resultados de la pregunta 1 de la evaluación



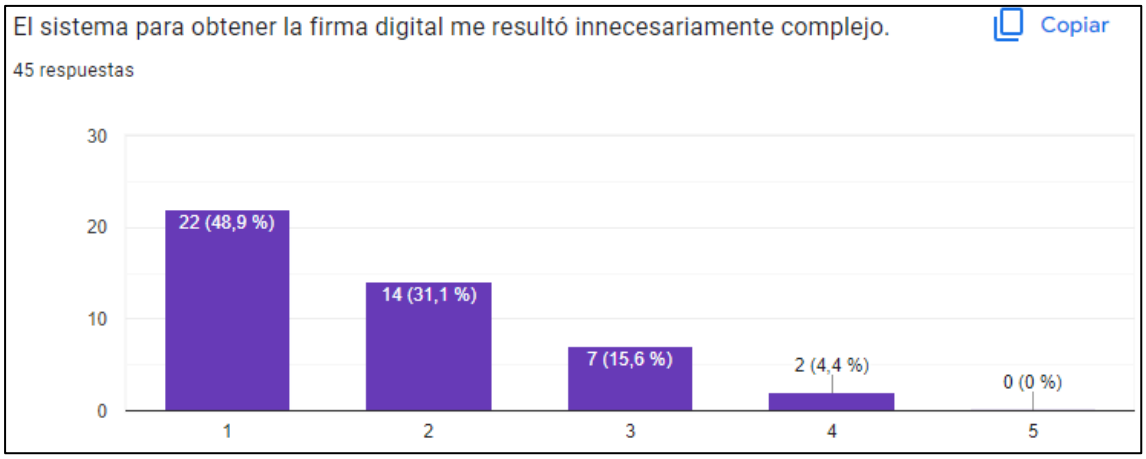
El 46.7% de los usuarios del sistema PKI ESPE consideran que se requiere el apoyo total de las autoridades para el uso extensivo de la firma digital, un 31.1% se encuentran de acuerdo en que las autoridades deben apoyar el proceso, el 17.8% de los usuarios se sienten indiferentes y únicamente un 4,4% están en desacuerdo en que las autoridades deben apoyar el uso de la firma electrónica. Esto pone en evidencia la necesidad de promover el uso de los certificados digitales, por parte de las autoridades de la Universidad, con ello los usuarios podrán usar la firma digital como un medio adecuado para la certificación de cualquier documento.

Pregunta 2

El sistema para obtener la firma digital me resultó innecesariamente complejo.

Figura 69

Resultados de la pregunta 2 de la evaluación



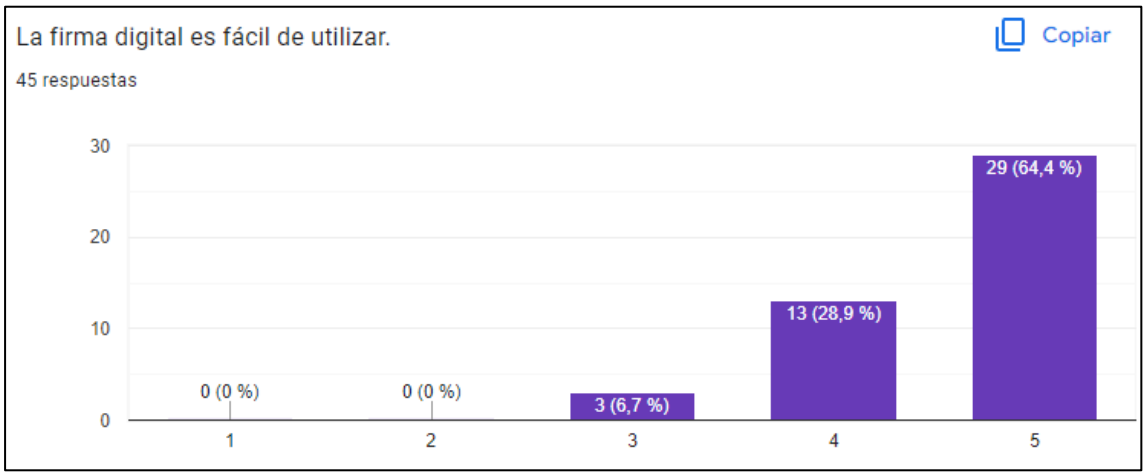
El 48.9% de los usuarios del sistema PKI ESPE consideran que el sistema para obtener la firma digital no resulta innecesariamente complejo, el 31.1% de los usuarios consideran que el sistema es poco complejo innecesariamente y un 15.6% consideran que el sistema es algo complejo innecesariamente, únicamente un 4.4% considera que el sistema es innecesariamente complejo. Esto demuestra que el sistema no es complejo de manera innecesaria y que existe la suficiente información en el manual de usuario para la generación del certificado. Esto también permite denotar que de ser posible se debería simplificar aún más el proceso de generación de un certificado digital.

Pregunta 3

La firma digital es fácil de utilizar.

Figura 70

Resultados de la pregunta 3 de la evaluación.



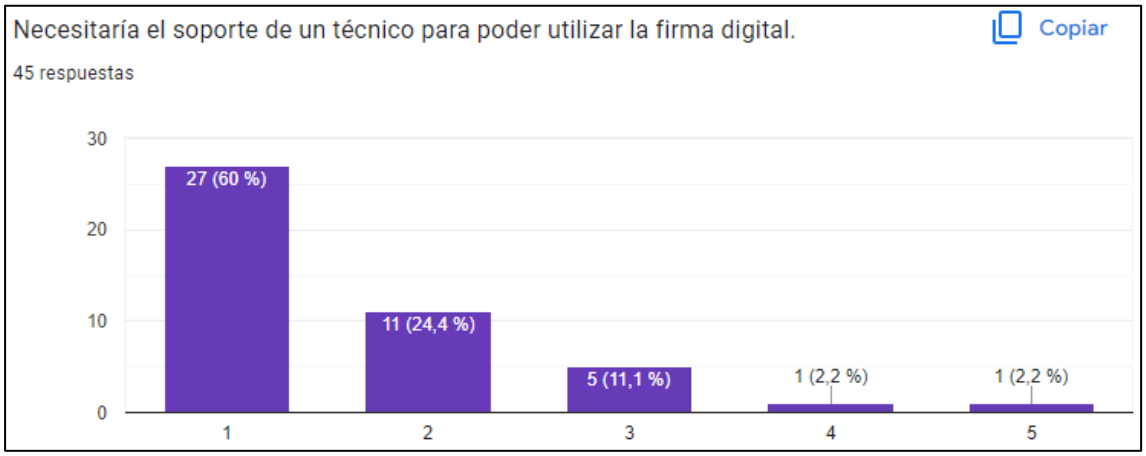
El 64.4% de los usuarios del sistema PKI ESPE consideran que absolutamente la firma digital es fácil de usar, el 28.9% consideran de fácil uso la firma digital y solo el 6.7% de los usuarios consideran una dificultad media en el uso de la firma digital. Esto muestra la acogida que tiene el sistema de certificación y su facilidad de aplicación por parte del usuario. También se puede observar que pese a ser mínimo, existe ciertos usuarios que consideran ciertas dificultades al momento de usar su firma electrónica, por lo que sería recomendable aplicar métodos de difusión de las ventajas y correcto uso de una firma digital.

Pregunta 4

Necesitaría el soporte de un técnico para poder utilizar la firma digital.

Figura 71

Resultados de la pregunta 4 de la evaluación



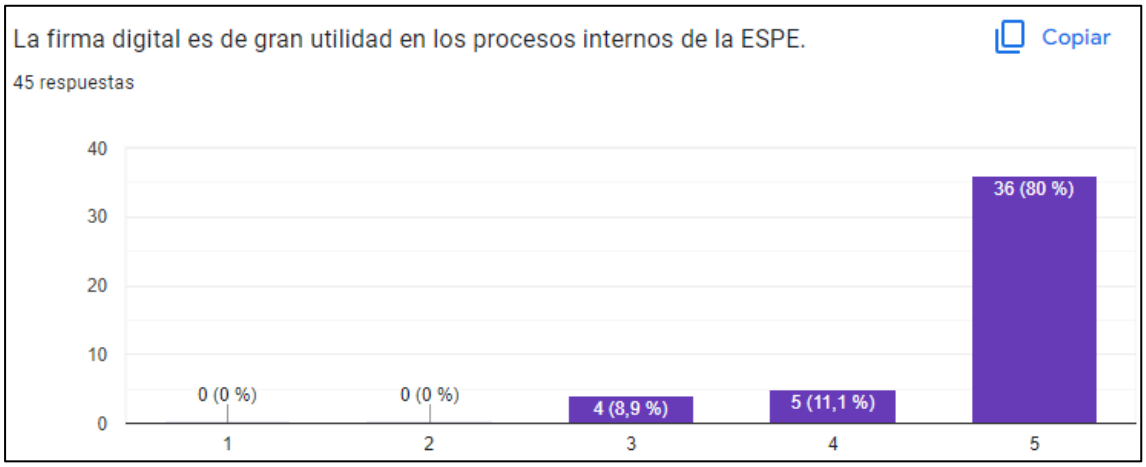
El 60% de los usuarios del sistema PKI ESPE consideran que en absoluto, no se necesitaría el soporte de un técnico para poder utilizar la firma digital, el 24.4% de los usuarios consideran que necesitan algo de soporte de un técnico, un 11.1% de los usuarios consideran que podrían llegar a necesitar soporte de un técnico para el uso de la firma digital y el 4.4% de los usuarios consideran que necesitan parcial o totalmente el soporte de un técnico para el uso de su firma digital. Con esto se llega a demostrar que el uso de la herramienta PKI ESPE es fácil y cuentan con la información necesaria para la generación de su certificado digital y utilizarlo, sin la intervención de una persona que guíe o dé soporte en el proceso. Existe un bajo porcentaje de usuarios que requieren soporte para el uso de la firma digital, por lo que es necesario capacitar a todos los usuarios previo al uso de la firma electrónica.

Pregunta 5

La firma digital es de gran utilidad en los procesos internos de la ESPE.

Figura 72

Resultados de la pregunta 5 de la evaluación



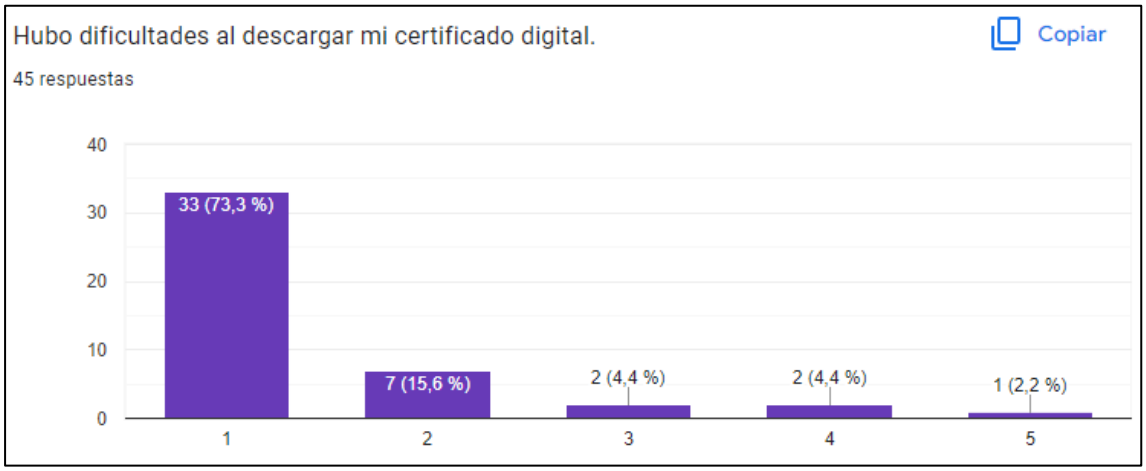
El 80% de los usuarios del sistema PKI ESPE consideran que la firma digital es de gran utilidad en los procesos internos de la ESPE, el 11.1% de los usuarios consideran útil la firma digital y un 8.9% de los usuarios consideran irrelevante el uso de la firma digital en los procesos internos de la ESPE. Con esto se determina que la implementación de la firma digital es de gran valía para la Universidad de las Fuerzas Armadas ESPE y que debe extenderse su uso para todos los trámites legales. Existe un porcentaje de usuarios que no contemplan la utilidad de la firma digital completamente por lo que se ve la necesidad de implementar medidas de socialización de las ventajas de la firma digital y extender su uso por parte de los miembros de la Universidad.

Pregunta 6

Hubo dificultades al descargar mi certificado digital.

Figura 73

Resultados de la pregunta 6 de la evaluación



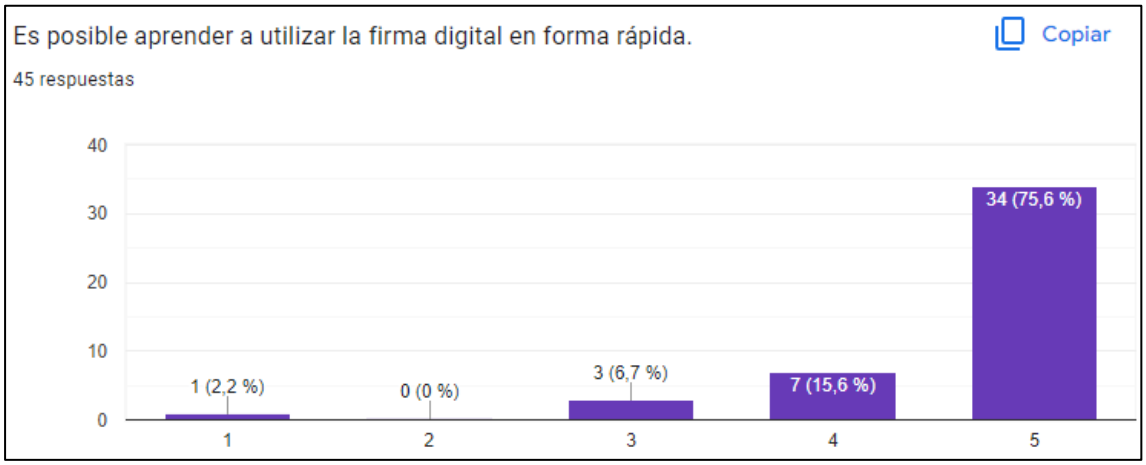
El 73.3% de los usuarios del sistema PKI ESPE no presentaron dificultades al descargar su certificado digital, el 15.6% de los usuarios tuvieron dificultades mínimas para descargar el certificado digital, el 4.4% de los usuarios tuvieron algunas dificultades, otro 4.4% de los usuarios tuvieron muchas dificultades para descargar el certificado digital y un 2.2% de los usuarios consideran que existen demasiadas dificultades para descargar el certificado digital. Se llega a mostrar que la herramienta cuenta con la disponibilidad y la respuesta a los requerimientos de forma adecuada, además de la correcta interpretación y seguimiento de las instrucciones brindadas a los usuarios. Existe usuarios que encuentran dificultades y pese a ser un porcentaje mínimo, es necesario verificar la claridad de las instrucciones y añadir de forma detallada pasos adicionales que aumenten la legibilidad e interpretación de las mismas.

Pregunta 7

Es posible aprender a utilizar la firma digital en forma rápida.

Figura 74

Resultados de la pregunta 7 de la evaluación



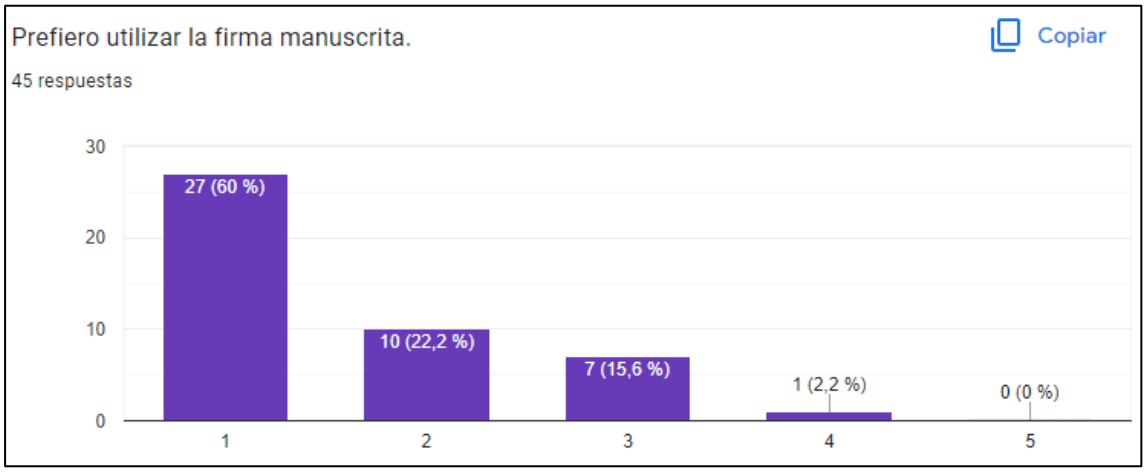
El 75.6% de los usuarios del sistema PKI ESPE consideran que es posible aprender a utilizar la firma digital en forma rápida, el 15.6% de los usuarios consideran que existe alguna ligera dificultad para aprender a usar su firma digital, el 6.7% de usuarios considera que el aprendizaje de la firma digital corresponde a un término medio y únicamente un 2.2% de los usuarios considera imposible aprender a utilizar la firma digital de una forma rápida. Estos resultados nos muestran la facilidad de aprendizaje de la herramienta y su utilidad. Sin embargo es necesario aplicar campañas de capacitación para el adecuado uso de la firma digital y enseñar a los usuarios lo fácil y útil que resulta el manejo de un certificado digital.

Pregunta 8

Prefiero utilizar la firma manuscrita.

Figura 75

Resultados de la pregunta 8 de la evaluación



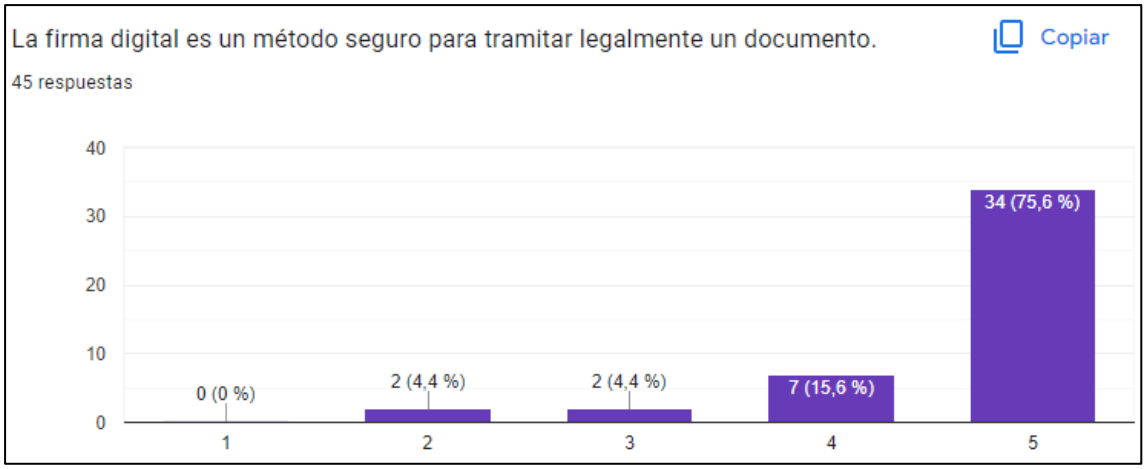
El 60% de los usuarios del sistema PKI ESPE prefieren utilizar la firma digital, un 22.2% no se encuentra convencido del todo sobre la firma digital, el 15.6% de los usuarios considera que no tiene una preferencia por la firma digital o manuscrita y únicamente un 2.2% prefiere en mayor parte la firma manuscrita. Con esto se percibe que la preferencia del servicio está orientada al uso de la firma digital, sin embargo, se puede observar que un bajo porcentaje prefieren la firma manuscrita, por lo que se debería desarrollar un plan de concienciación para el uso de medios digitales y mostrarles a los usuarios las ventajas del uso de un certificado digital, frente al uso de una firma manuscrita.

Pregunta 9

La firma digital es un método seguro para tramitar legalmente un documento.

Figura 76

Resultados de la pregunta 9 de la evaluación



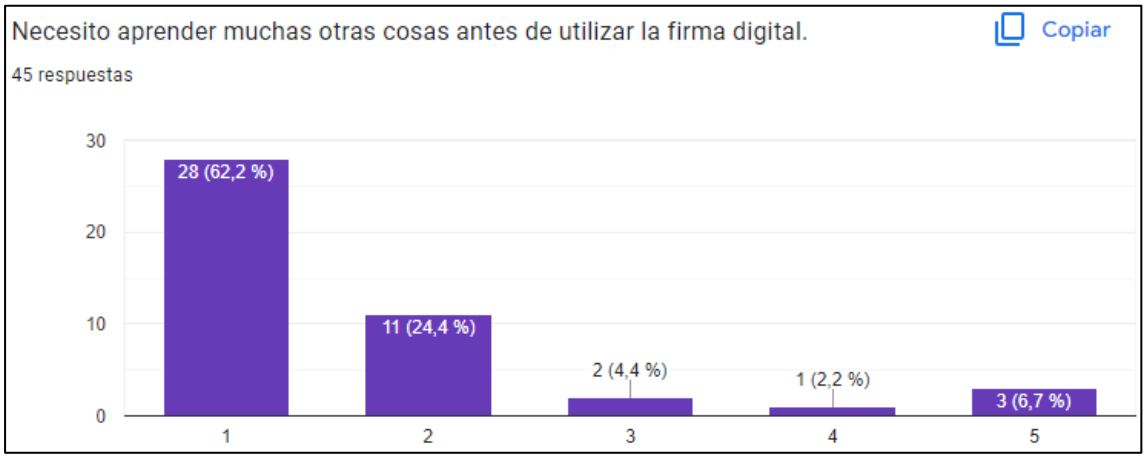
El 75.6% de los usuarios del sistema PKI ESPE consideran que la firma digital es un método completamente seguro para tramitar legalmente un documento, un 15,6% aún tienen ciertas dudas al respecto, un 4,4% de los usuarios consideran que la firma digital no es un método tan seguro y el 4.4% de los usuarios consideran que la firma digital es un método inseguro para tramitar un documento. Estos resultados ponen en evidencia la intención de los usuarios en incrementar el uso de los medios de certificación digital y la seguridad que proveen al momento de su uso. Existen usuarios que no se sienten convencidos, sin embargo, con una correcta campaña de socialización del uso de medios digitales y las ventajas de la firma digital permitirá que mejore la confianza de los usuarios que aún dudan de la seguridad de la misma.

Pregunta 10

Necesito aprender muchas otras cosas antes de utilizar la firma digital.

Figura 77

Resultados de la pregunta 10 de la evaluación



El 62.2% de los usuarios del sistema PKI ESPE consideran que no es necesario aprender muchas otras cosas antes de utilizar la firma digital, el 24.4% de los usuarios consideran que requieren de algunos otros conocimientos antes de usar la firma digital, el 4.4% de los usuarios consideran que requieren aprender varios conocimientos adicionales antes de usar la firma digital, el 2,2% de los usuarios consideran que de seguro requieren aprender otras cosas previo al uso de la firma digital y un 6.7% consideran que requieren aprender muchas otras cosas antes de utilizar la firma digital. Estos resultados nos muestran la alta usabilidad de la herramienta y la poca capacitación necesaria al momento de firmar un documento digitalmente, esto muestra que, al momento de aumentar la disponibilidad de la herramienta para todos los miembros de la Universidad, será de fácil aprendizaje para los mismos. Por otro lado, existen varios usuarios que consideran no tener un conocimiento suficiente para el uso de la firma digital, por lo que sería recomendable proveer de un contexto general a los usuarios y brindarles todos los conocimientos necesarios en las políticas de uso y en las instrucciones para el usuario.

Informe

Se elaboró un informe de la evaluación en base del formato de ITAF de ISACA, con las observaciones y recomendaciones de los hallazgos encontrados (ver anexo 1).

Dentro del informe se encuentran observaciones y recomendaciones de los hallazgos encontrados que se pueden resumir en las siguientes áreas:

Funcionalidad del servicio

La implementación de la firma digital es de gran valía para la Universidad de las Fuerzas Armadas ESPE y debe extenderse su uso para todos los trámites legales, también se evidencia la intención de los usuarios en incrementar el uso de los medios de certificación digital y la confianza que tienen en la seguridad que proveen al momento de su uso.

Sin embargo, es evidente la necesidad de promover el uso de los certificados digitales, por parte de las autoridades de la Universidad, con ello los usuarios podrán usar la firma digital como un medio adecuado para la certificación de cualquier documento.

Existe un bajo porcentaje de usuarios que no contemplan la utilidad de la firma digital o que no se sienten convencidos de su uso por lo que la Universidad de las Fuerzas Armadas por medio del ESPE CERT debe implementar medidas de socialización del uso de medios digitales y las ventajas de la firma digital logrando que mejore la confianza de los usuarios en la certificación digital y extender su uso por parte de los miembros de la Universidad.

Usabilidad del servicio

La herramienta PKI ESPE cuenta con la disponibilidad y la respuesta a los requerimientos de forma adecuada, además permite la correcta interpretación y seguimiento de las instrucciones brindadas a los usuarios, mostrando no tener complejidad de manera innecesaria y contar con la suficiente información en el manual de usuario para la generación de un certificado.

PKI ESPE es de fácil uso y cuenta con la información necesaria para la generación de un certificado digital y utilizarlo posteriormente sin la intervención de una persona que brinde soporte en el proceso, además se percibe que los usuarios prefieren usar la firma digital por sobre la firma manuscrita.

Por otra parte, existen usuarios que encuentran dificultades en el uso del sistema, otros que requieren soporte para el uso de la firma digital y otros que prefieren el uso de la firma manuscrita, por lo que es recomendable simplificar aún más el proceso de generación

de un certificado digital o deslindar de la generación de estos certificados a los usuarios finales.

También es necesario verificar la claridad de las instrucciones y añadir de forma detallada pasos adicionales que pueden aumentar la legibilidad e interpretación para el uso de la firma digital. Una vez realizadas las correcciones es necesario capacitar a todos los usuarios previo al uso de la firma electrónica, logrando una concienciación para el uso de medios digitales y las ventajas que un certificado digital provee frente al uso de la firma manuscrita.

Facilidad de aprendizaje

El sistema PKI ESPE tiene una acogida adecuada entre los usuarios finales, mostrando la facilidad de aprendizaje de la herramienta y su utilidad, así como la poca capacitación necesaria al momento de firmar un documento digitalmente, la herramienta puede aumentar fácilmente la disponibilidad para todos los miembros de la Universidad, previendo el fácil aprendizaje que supone su uso.

Existen pocos usuarios que consideran no tener un conocimiento suficiente para el uso de la firma digital por lo que se presentan ciertas dificultades al momento de usar la firma electrónica, sería recomendable proveer de un contexto general a los usuarios y brindarles todos los conocimientos necesarios en las políticas de uso y en las instrucciones para el usuario.

Se debe aplicar métodos de difusión de las ventajas y correcto uso de una firma digital, pueden aplicarse campañas de capacitación para el adecuado uso de la firma digital y enseñar a los usuarios lo fácil y útil que resulta el manejo de un certificado digital.

Mejora del servicio

Plan de Mejora

Objetivo

Tomar acciones en referencia a las recomendaciones emitidas en el informe de evaluación del funcionamiento del servicio de Firma Electrónica del ESPE-CERT en el

Departamento de Ciencias de la Computación.

Alcance

Implementar mejoras en el servicio de Firma Electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación, a fin de mejorar la funcionalidad y usabilidad del aplicativo PKI ESPE. Con ello se prepara la herramienta para su transición y despliegue para todos los miembros de la Universidad de las Fuerzas Armadas ESPE.

Indicadores de cumplimiento

- Funcionalidad del servicio.
- Usabilidad del servicio.
- Facilidad de aprendizaje.

Recursos

- Humanos

Se cuenta con el docente tutor y los alumnos que se encuentran desarrollando el proyecto de titulación.

- Financieros

No se requiere de recursos financieros en la fase de mejora del servicio.

- Materiales

Servidor en el laboratorio H202, computadoras personales.

- Tecnológicos

Servicios de internet, repositorios e información disponible.

Tareas a realizar

Se ha definido tareas mediante un cronograma que abarca las actividades.

Tabla 6

Tarea y responsables del plan de mejora

Tarea	Responsable	Duración	Comienzo	Fin
Determinación de las acciones de mejora.	Estudiantes	5 días	08 ago	12 ago
Realización de acciones de mejora.	Estudiantes	5 días	13 ago	17 ago
Evaluación del impacto de las acciones de mejora.	Estudiantes	2 días	18 ago	19 ago

Acciones de mejora

Determinación de acciones

- Funcionalidad del servicio

Debido a la evidente necesidad de promover el uso de los certificados digitales, por parte de las autoridades de la Universidad, para que los usuarios puedan usar la firma digital como un medio adecuado para la certificación de cualquier documento, se debe implementar medidas de socialización del uso de medios digitales y las ventajas de la firma digital. Esto debe verse plasmado en las Políticas de Uso de la herramienta, así como en los manuales de usuario.

- Usabilidad del servicio

Se debe simplificar el proceso de generación de un certificado digital o deslindar de la generación de estos certificados a los usuarios finales ya que con ello podría verse mejorada sustancialmente la usabilidad del servicio. Se debe verificar la claridad de las instrucciones existentes en el manual del usuario y añadir de forma detallada pasos adicionales que pueden aumentar la legibilidad e interpretación para el uso de la firma digital. En vista de la necesidad de capacitar a todos los usuarios previo al uso de la firma electrónica, se debe agregar un apartado del contexto y específicamente como se capacitará a los usuarios previo al uso de la firma digital en las Políticas de uso de la

herramienta.

- Facilidad de aprendizaje

Se debe proveer de todos los conocimientos necesarios en las políticas de uso y en las instrucciones para el usuario en referencia al uso de la firma digital y las herramientas que requiere.

Se debe aplicar métodos de difusión de las ventajas, facilidad de uso y utilidad de la firma digital por lo que se debe agregar este apartado en los manuales de uso del sistema.

Realización de acciones de mejora

- Funcionalidad del servicio

Se implementó medidas de socialización del uso de medios digitales y las ventajas de la firma digital, lo cual se plasmó en las Políticas de Uso de la herramienta (ver anexo 2), así como en los manuales de usuario (ver anexo 3).

- Usabilidad del servicio

Se verificó la claridad de las instrucciones existentes en el manual del usuario y se añadió de forma detallada pasos adicionales que aumentaron la legibilidad e interpretación para el uso de la firma digital haciendo énfasis en pasos que podrían estancar al usuario en la obtención de su certificado digital (ver anexo 3).

Se agregó un apartado del contexto y específicamente como se capacitará y entrenará a los usuarios previo al uso de la firma digital en las Políticas de uso de la herramienta (ver anexo 2).

- Facilidad de aprendizaje

Se agrego información adicional en las políticas de uso (ver anexo 2) y en las instrucciones para el usuario (ver anexo 3) en referencia al uso de la firma digital y las herramientas que requiere.

Evaluación del impacto de las acciones de mejora.

Se verificó el cumplimiento de las recomendaciones emitidas en la fase de evaluación del sistema PKI ESPE mediante la verificación de las políticas y manuales de

uso del sistema, donde se pudo evidenciar que se encontraban añadidos los apartados requeridos y modificaciones para un mejor entendimiento por parte de los usuarios.

A fin de valorar el impacto de las acciones de mejora se tomó a dos usuarios que no tienen conocimiento del funcionamiento del sistema, ni el uso de un certificado digital. Al primer usuario se le entregó el manual de usuario anterior (desarrollado en la fase de implementación) y al segundo usuario se le entregó el manual de usuario con las modificaciones realizadas, las agregaciones a fin de mejorar la facilidad de aprendizaje y usabilidad del sistema, así como se le brindó las herramientas necesarias y se obtuvo los siguientes resultados:

Tabla 7

Comparación de usuarios

Actividad	**Usuario 1** **Manual inicial**	**Usuario 2** **Manual modificado**
Lector PDF provisto	No	Si
Tiempo para gestionar un certificado	23 minutos	12 minutos
Tiempo para firmar un documento	8 minutos	4 minutos
Personalización de la firma	No	Si
Visualización de la certificación	No	Si
Asistencia en el proceso	Si	No
Satisfacción del usuario /10	7	10

Luego de la implementación de las recomendaciones emitidas anteriormente, se puede observar una mejoría en el proceso del uso de la aplicación PKI ESPE y proceso de firma de un documento digitalmente mediante la reducción en los tiempos de gestión en los procesos y mejorando la satisfacción del usuario final.

Capítulo V

Conclusiones y Recomendaciones

Conclusiones

El servicio de Firma Electrónica mediante el aplicativo PKI ESPE se implementó en el ESPE CERT del Departamento de las Ciencias de la Computación según ITIL V4, contando con los niveles adecuados de disponibilidad y operación luego de haber realizado una evaluación y aplicado acciones de mejora que permiten prestar este servicio a los estudiantes, docentes y personal administrativo del DCCO y estar en capacidad de extender el servicio a otros departamentos de la Universidad de las Fuerzas Armadas ESPE.

El servicio de Firma Electrónica se encuentra en operación, actualmente disponible para los estudiantes, docentes y personal administrativo del DCCO en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos, el sistema PKI ESPE se encuentra incorporado al catálogo de servicios del ESPE CERT con las políticas e instrucciones necesarias para su correcto funcionamiento.

La evaluación del servicio se realizó orientado a la usabilidad y funcionalidad del servicio, aplicando encuestas a los usuarios finales, permitiendo determinar el cumplimiento de los objetivos del proyecto y la calidad de servicio prestado, llegando a emitir recomendaciones y observaciones para mejorar el servicio.

En base a las observaciones obtenidas en la evaluación del servicio, se realizó el plan de mejoras y se aplicó estas recomendaciones, logrando una mejoría en el proceso del uso de la aplicación PKI ESPE y proceso de firma de un documento digitalmente por parte de los usuarios de la ESPE.

Recomendaciones

El servicio de Firma Electrónica se va a extender a otros departamentos de la Universidad de las Fuerzas Armadas ESPE en el futuro, por lo que se debe realizar un estudio de las leyes que rigen un proyecto de transformación digital, como el de firma electrónica, a fin de conseguir la certificación que establece la Ley de Comercio Electrónico para los entes proveedores de firma electrónica.

En vista de que el servicio de Firma Electrónica se encuentra en operación, se recomienda que la capacitación al personal de operadores de la herramienta, así como a los usuarios de la firma digital sea minucioso y continuo a fin de mantener y mejorar la calidad de servicio. También se debería establecer como medio de legalización y certificación la firma digital emitida por PKI ESPE para el Departamento de Ciencias de la Computación en sesión del consejo de Departamento.

Sería recomendable poner en ejecución una nueva socialización del proyecto y una nueva evaluación de funcionalidad y usabilidad del sistema en un periodo de tiempo en el que los estudiantes requieran un uso más extensivo de la herramienta, como lo es el periodo de matrículas, todo esto con la finalidad de determinar nuevas observaciones o recomendaciones para la mejora de la herramienta.

Se recomienda desarrollar el Plan de Recuperación de Desastres en el CERT ESPE a fin de establecer un proceso de recuperación de datos, hardware y software crítico para el funcionamiento de PKI ESPE en caso de que suceda algún incidente que comprometa la prestación del servicio o los datos de los usuarios.

Referencias

Anghillantte, A., & Romero, L. (2017). Firma Digital. *Ingeniería de Sistemas*. Obtenido de https://rdu.iua.edu.ar/handle/123456789/623

AS_ADAM Adam Datacenter, E. (19 de Septiembre de 2000). *Uanataca. Provider of electronic signature and digital certificates*. Obtenido de Uanataca. Provider of electronic signature and digital certificates: https://web.uanataca.com/ec/

Bon, J. V. (2010).

Carquin, O. (2016).

Carrera, A., & Celi, J. (2022). Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/29387/1/T-ESPE-052319.pdf

Cataldo, A. (2015).

Cordovi, A. (2018). Paquete de Servicios para el Portafirmas Digital de la Universidad de las Ciencias Informáticas. *Trabajos de Diploma*. Obtenido de https://repositorio.uci.cu/jspui/handle/123456789/9925

Ecuador, B. C. (18 de Noviembre de 1997). *Certificación Electrónica*. Obtenido de Banco Central del Ecuador: https://www.eci.bce.ec/

Formentín, M. (2012). La firma electrónica, su recepción legal. Especial referencia a la ausencia legislativa en Cuba. *IUS, 7*(31). Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100007

González, D. B. (2 de 8 de 2021). *Profile*. Obtenido de https://profile.es/blog/que_es_docker/

GOOGLE, U. (30 de Marzo de 2000). *ANF AC*. Obtenido de ANF AC: https://www.anf.es/

Granados, G. (2006).

J, A. (s.f.).

Judicatura, C. d. (6 de Octubre de 2008). *Consejo de la Judicatura*. Obtenido de Consejo de la Judicatura: https://www.funcionjudicial.gob.ec

Microsoft. (23 de 06 de 2022). *Microsoft*. Obtenido de https://docs.microsoft.com/es-es/dotnet/architecture/microservices/container-docker-introduction/docker-defined

Nacional, C. (10 de Abril de 2002). Ley de comercio electrónico, firmas electrónicas y mensaje de datos. *Ley de comercio electrónico, firmas electrónicas y mensaje de datos*. Quito, Pichincha, Ecuador.

Nuñez, E. A. (5 de Mayo de 2014). *Open Webinars*. Obtenido de https://openwebinars.net/blog/docker-que-es-sus-principales-caracteristicas/

Perisse, M. (2008).

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 1-18.

Red Hat. (9 de Enero de 2018). *Red Hat*. Obtenido de https://www.redhat.com/es/topics/containers/what-is-docker

Rubio. (2015).

Sanhueza, M. (2018). Plan de implementación de Firma Digital en la Universidad Nacional de Río Negro. *Licenciatura en Sistemas*. Obtenido de http://hdl.handle.net/20.500.12049/1391

Talens, S. (2008).

Telconet S.A, E. (21 de Diciembre de 2007). *SecurityData*. Obtenido de SecurityData: https://www.securitydata.net.ec/

Tuunanen, T. (2007).

Urrego, V. (2011).

Vermejo, C. (2020). Desarrollo e implementación del Sistema de Firmas Electrónicas y Certificados Digitales del Estado e implantación de la autoridad administrativa competente. *Repositorio ULima*. Obtenido de https://hdl.handle.net/20.500.12724/12017

Zayas, Y. M. (2013). The electronic signature, its legal reception. Special reference to legislative void in Cuba. *Revista del Instituto de Ciencias Jurídicas de Puebla,*

mexico, 104-120.