Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente.

Caso de estudio: Departamento de Ciencias de la Computación DCC-ESPE

Carrera López, Alberto Francisco y Celi Jiménez, Juan Francisco

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación previo, a la obtención del título de Ingeniero en Sistemas e Informática

Ing. Ron Egas, Mario Bernabé

1 de febrero del 2022

Reporte de similitud de contenidos

Tesis_PKI- Juan Celi-Alberto Carrera version final.pdf

Scanned on: 16:44 February 15, 2022 UTC

Identical Words	221
Words with Minor Changes	11
Paraphrased Words	442
Ommited Words	2565

COPYLEAKS Website | Education | Businesses

MARIO BERNABE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2022.02.22 15:04:17 -05'00'

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Certificación

Certifico que el trabajo de titulación, **"Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente. Caso de estudio: Departamento de Ciencias de la Computación DCC-ESPE",** realizado por los señores **Carrera López, Alberto Francisco** y **Celi Jiménez, Juan Francisco**, ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas "ESPE", razón por la que me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí 1 de febrero del 2022

MARIO BERNABE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2022.02.21 12:08:53 -05'00'

Ing. Ron Egas, Mario Bernabé MSc.

C.C: 1704229747

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Responsabilidad de autoría

Nosotros, **Carrera López, Alberto Francisco** con cédula de ciudadanía N° 1723610737 **y Celi Jiménez, Juan Francisco** con cédula de ciudadanía N° 1717394512 declaramos que el contenido, ideas y criterios del trabajo de titulación: **"Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente. Caso de estudio: Departamento de Ciencias de la Computación DCC-ESPE",** 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 1 de febrero del 2022

Carrera López, Alberto Francisco

C.C: 1723610737

Celi Jiménez, Juan Francisco

C.C: 17171394512

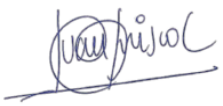
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Autorización de publicación

Nosotros, **Carrera López, Alberto Francisco** con cédula de ciudadanía N° 1723610737 **y Celi Jiménez, Juan Francisco** con cédula de ciudadanía N° 1717394512, autorizamos a la Universidad de las Fuerzas Armadas "ESPE" publicar el trabajo de titulación: **"Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente. Caso de estudio: Departamento de Ciencias de la Computación DCC-ESPE"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí 1 de febrero del 2022



Carrera López, Alberto Francisco

C.C: 1723610737

Celi Jiménez, Juan Francisco

C.C: 17171394512

Dedicatoria

Con mucha honra dedico este trabajo a mi madre, pues sin ella no lo habría logrado. Su paciencia y fe hacia mí, me han motivado para no rendirme ante ninguna situación y su apoyo incondicional ha estado en cada paso que he dado en este largo camino llamado vida.

Alberto Francisco Carrera López

Dedico este logro a mis hijos que sirva de ejemplo para que siempre cumplan sus metas, a mi esposa, padres, hermanos y familia por su apoyo incondicional.

Juan Francisco Celi Jiménez

Agradecimientos

Agradezco a Dios por haberme dado la inteligencia y la capacidad para cumplir mis metas.

A mi familia pues todos con su aliento y apoyo han sido de vital importancia para conseguir este objetivo.

A mis profesores, compañeros y amigos de universidad porque el compartir aulas y conocimientos ha hecho que crezca tanto personal como profesionalmente.

Alberto Francisco Carrera López

Agradezco a Dios y a la virgencita del Cisne por la salud y la vida que me conceden, un especial y enorme agradecimiento a mis dos hijos Francisco Gustavo y Francisco Gael por ustedes lo hice gracias por su cariño, alegría y confianza.

A mis padres, hermanos y familiares muchas gracias por ser ese apoyo incondicional en cada paso que doy.

Finalmente, a mis profesores un agradecimiento eterno porque han entregado generosamente sus conocimientos y enseñanzas que sin duda son un aporte fundamental en mi vida.

Juan Francisco Celi Jiménez

Índice de contenido

Índice de tablas

Índice de figuras

Resumen

El cuestionamiento de las seguridades existentes en la transferencia y comunicación de datos es actualmente uno de los temas más relevantes en el ámbito tecnológico, el uso diario del internet es inevitable e indispensable como revisar el correo electrónico, realizar transacciones bancarias y visitar las redes sociales.

En el desarrollo de este proyecto se han analizado los sistemas criptográficos simétricos y asimétricos, los primeros también conocidos como de clave privada, son utilizados con una sola clave que cifra y descifra los mensajes. La principal seguridad se centra en la clave que debe ser robusta.

La criptografía asimétrica o de clave pública utiliza un par de claves, una pública y una privada con las que se cifran en la emisión y se descifra en la recepción los mensajes. Una de las principales ventajas de este tipo de criptografía es que no se comparte la clave privada que es otorgada por la entidad de certificación.

Una infraestructura de clave pública (PKI) es una combinación de hardware, software, políticas y normas de funcionamiento para la entrega de certificados digitales que identifican a un usuario, con la que se obtiene una comunicación segura, además proporciona: no repudio, confidencialidad, integridad y autenticidad en el proceso de comunicación. Con estos certificados se puede firmar documentos e incluso cifrar los datos para ser enviados.

PALABRAS CLAVE:

- **CRIPTOGRAFÍA SIMÉTRICA**
- **CRIPTOGRAFÍA ASIMÉTRICA**
- **ALGORITMOS**

Abstract

The questioning of the existing securities in the transfer and communication of data is currently one of the most relevant issues in the technological field, the daily use of the Internet is inevitable and essential, such as checking email, performing bank transactions and visiting social networks.

In the development of this project, the symmetric and asymmetric cryptographic systems have been analyzed, the former also known as private key, they are used with a single key that encrypts and decrypts messages. The main security is focused on the key, so it must be robust.

Asymmetric or public key cryptography uses a pair of keys, one public and one private, with which messages are encrypted when they are sent and decrypted when they are received. One of the main advantages of this type of cryptography is that the private key that is granted by the certification authority is not shared.

A public key infrastructure (PKI) is a combination of hardware, software, policies and operating standards for the delivery of digital certificates that identify a user, with which secure communication is obtained, it also provides non-repudiation, confidentiality, integrity and authenticity in the communication process. With these certificates you can sign documents and even encrypt the data to be sent.

KEYWORDS:

- **SYMMETRIC CRYPTOGRAPHY**
- **ASYMMETRIC CRYPTOGRAPHY**
- **ALGORITHMS**

Capítulo I

Introducción

Antecedentes

Las redes de comunicación como Internet han abierto posibilidades para el intercambio de información (Marrero Travieso, 2003), conforme pasa el tiempo, esta opción ha sido cada vez más utilizada a nivel mundial en varios ámbitos. Debido a este incremento, los riesgos inherentes de tecnologías y sistemas de información que no poseen controles de seguridad son cada vez mayores, considerando que las amenazas existentes son globales.

En Ecuador es notable el incremento del uso de internet (Arcotel, 2020), para el año de 2020 contaba con 2.241.836 de cuentas de internet fijo y 9.765.161 cuentas de internet móvil, que representa un gran intercambio de información, por lo que el estado en el año de 2018 puso en marcha el “Plan Nacional de Gobierno Electrónico” con la finalidad de “ser un país en cual los ciudadanos sean actores activos en las decisiones del Estado al tener facilidades de acceso a los servicios, información y participación por medios electrónicos” (MINTEL, 2018).

El entorno de educación superior no es ajeno al intercambio de información, tampoco lo es al constante avance de tecnología y por ende a sus riesgos asociados, el presente proyecto se enfocará en la Universidad de las Fuerzas Armadas ESPE que está integrada por estudiantes, personal docente e investigador, y personal administrativo, quienes son los principales beneficiarios de los servicios de tecnología que la Universidad provee. Actualmente en la Universidad se maneja un gran volumen de información de miles de estudiantes, quienes además hacen uso de sus plataformas y medios digitales para enviar documentación.

Identificación del problema

El continuo avance tecnológico ha hecho que la Universidad se adapte a los cambios en tecnología y automatice varios de sus procesos fundamentales para su adecuado funcionamiento, sin embargo, ciertos procesos aún no se encuentran automatizados completamente, aún se utiliza la firma a manuscrita para legalizar la documentación que se tramita en su interior y más aún, no existe un sustento de que los documentos sean de autoría de una persona en concreto. La investigación se centrará en el Departamento de Ciencias de la Computación de la Universidad.

Es preciso mencionar que la incertidumbre o desconocimiento acerca del origen, la autoría e integridad de un documento tienen como consecuencia la desconfianza en el uso de estos instrumentos e incluso provocan retraso, pérdida y paralización en los procesos institucionales, así mismo un documento, ya sea digital o digitalizado, que es enviado por medios electrónicos puede ser editado, alterado o reemplazado por otro, sin que exista una certeza de su origen y trámite (Sanhueza, 2018).

Sin embargo, existen herramientas que solventan la problemática abordada, pero algunas tienen costos asociados a su adquisición y uso. Debido a la pandemia y los recortes de asignaciones presupuestarias, la Universidad no se encuentra en capacidad de asignar un fondo para la implementación de una solución en la que implique egreso de recursos económicos.

Justificación

Los aspectos más relevantes para justificar el proyecto hacen referencia a las causas y efectos de la problemática y son los siguientes:

Dado que para la realización de la mayoría de los documentos se utilizan máquinas electrónicas tales como un ordenador, lo más adecuado sería que la

herramienta para firmar los documentos se encuentre bajo el mismo medio, agilitando así cualquier tipo de proceso en el cual se requiera la firma de una persona.

Una firma digital asegura la autoría e integridad de los documentos realizados digitalmente, además tiene igual validez que los documentos firmados en papel (Gómez, y otros, 2006), por lo que es de gran valor agregar legalidad e integridad al entorno virtual de la universidad en cuanto a envío de documentos digitalmente se refiere.

Con el PKI se logra establecer identidades digitales que permitir la ejecución de operaciones criptográficas como el cifrado, las firmas digitales y la no repudiación de las transacciones electrónicas con garantías, garantizando la confidencialidad, la autenticidad, la integridad y la no repudiación en la entrega de mensajes seguros cuando se transmiten (Carvajal, 2007), lo que genera principalmente confianza y seguridad en los docentes y servidores públicos que reciben esta información.

Objetivos

Objetivo general

Implementar una PKI utilizando software libre para garantizar la integridad de los documentos firmados digitalmente, basado en el marco legal ecuatoriano.

Objetivos específicos

- Realizar una revisión sistemática de literatura de estudios, investigaciones y proyectos relacionados a criptografía y firmas digitales con el propósito de comprender su uso e implementación.
- Determinar las políticas y procedimientos para el funcionamiento de la Infraestructura de Llave Pública (PKI) en el DCCO.
- Desarrollar la aplicación web para automatizar el ciclo de vida de los certificados digitales de los estudiantes del DCCO.

- Evaluar la aplicación web para garantizar la integridad y autenticación del origen de los documentos firmados digitalmente por los estudiantes del DCCO.

Alcance

El presente proyecto propone que la Universidad de las Fuerzas Armadas ESPE cuente con una herramienta que facilite a su personal docente y estudiantes, la firma de documentos sin la necesidad de imprimirlos, que asegure su integridad, autenticación de origen y no repudio agregando así valor legal al entorno virtual de la institución, y que además su uso y/o adquisición no represente ningún valor monetario.

Los documentos serán firmados digitalmente con un algoritmo de firma digital que está compuesto de una función hash y un algoritmo criptográfico, ambos basados en estándares internacionales y serán definidos durante el transcurso de la investigación, la firma a su vez generara un código QR que proporcionara información del firmante.

Como solución se plantea una Infraestructura de Llave Pública usando software libre y cuya arquitectura estará compuesta de:

La autoridad de certificación que será la entidad de confianza encargada de gestionar el ciclo de vida los certificados digitales, que a su vez permitirán garantizar la identidad de una persona con las siguientes fases: solicitud, emisión, renovación, revocación y suspensión; así mismo se definirán políticas correspondientes a las fases del ciclo de vida de la siguiente manera:

- Solicitud para cuando un estudiante requiera crear un certificado digital.
- Emisión, cuando el certificado pase la fase de solicitud y esté listo para ser entregado al solicitante.

- Renovación cuando el certificado haya cumplido con su periodo de validez establecido y se requiera recobrar validez, dicho periodo será establecido durante el transcurso de la investigación.
- Revocación cuando un certificado pierde validez por incumplimientos por parte del estudiante tales como faltas al reglamento de la universidad, de igual manera esto se definirá durante el transcurso de la investigación
- Suspensión de un certificado será cuando por eventos no previstos tales como el fallecimiento del estudiante este dejará de ser válido.

La autoridad de registro encargada de controlar la generación de certificados, para la presente investigación se trabajará junto con el caso de estudio para verificar la información de los estudiantes pertenecientes a las carreras del departamento.

Las autoridades de los repositorios en los que se almacenan los certificados emitidos, así como los que han sido revocados por las políticas establecidas y, por tanto, ya no son válidos.

Para utilizar los certificados digitales en una aplicación web, se realizará el análisis y se definirá durante el trascurso del proyecto políticas y procedimientos para el funcionamiento de la PKI.

Para complementar de manera más amplia el alcance del proyecto propuesto, se plantea a continuación preguntas de investigación por cada objetivo específico planteado, se toma como base como mínimo dos preguntas, que es un número apropiado para el desarrollo de la investigación.

Tabla 1

Objetivos y preguntas

Objetivo específico	Pregunta de investigación

i. Realizar una revisión sistemática de literatura de estudios, investigaciones y proyectos de criptografía y firmas digitales con el propósito de comprender su uso e implementación.	a. ¿Qué soluciones proponen los estudios para asegurar la integridad y autenticación de origen de documentos enviados a través de medios electrónicos? b. ¿Qué tipos de algoritmos criptográficos son utilizados e implementados?
ii. Determinar las políticas y procedimientos para el funcionamiento de la Infraestructura de Llave Pública (PKI) en el DCCO.	a. ¿Cómo se establece políticas y procedimientos para el funcionamiento de una PKI? b. ¿En base de qué aspectos se deben establecer políticas y procedimientos para el funcionamiento de una PKI?
iii. Desarrollar la aplicación web para automatizar el ciclo de vida de los certificados digitales de los estudiantes del DCCO.	a. ¿Cómo se desarrolla una solución de firma digital? b. ¿Qué herramientas se debería tomar como base en un desarrollo de una solución criptográfica?
iv. Evaluar la aplicación web desarrollada para garantizar integridad y autenticación en los mensajes de datos.	a. ¿Cómo se evalúa una solución en base de criptografía aplicada y firmas digitales? b. ¿Qué se debe tener en cuenta para evaluar una solución en base de criptografía aplicada y firmas digitales?

Nota. Elaboración propia

Hipótesis

De acuerdo con la metodología de investigación se formuló la siguiente hipótesis de trabajo:

La implementación de una PKI brinda una solución que disminuye la incertidumbre acerca de la autoría e integridad de los documentos enviados por los estudiantes a través de medios virtuales en el Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE.

El planteamiento de la hipótesis establece la evaluación del rendimiento de la implementación de la solución.

Metodología

Para el desarrollo del proyecto, se considera la metodología de Design Science Research centrada en el desarrollo y el rendimiento de artefactos con la intención de mejorar su rendimiento funcional (Vaishnavi & Kuechler, 2008).

A continuación, se hace una breve introducción de las fases que la componen y se muestra su alineamiento con los objetivos específicos planteados en la sección sexta de la investigación.

Metodología Design Science Research

Se aplica a categorías de artefactos que incluyen algoritmos, interfaces humanos/computadora, metodologías de diseño y lenguajes. Su aplicación es más notable en las disciplinas de Ingeniería e Informática (Vaishnavi & Kuechler, 2008).

Según (Offermann, Levina, Schönherr, & Bub, 2009), la metodología se compone de tres fases principales:

- Identificación del problema

- Diseño de la solución
- Evaluación

Dentro de la primera fase se debe identificar el problema y obtener juicios de expertos por lo que se alinea con el primer objetivo específico, así mismo se debe realizar una revisión de literatura por lo que también se alinea con el primer objetivo específico.

En la segunda fase, se debe diseñar la solución a la problemática identificada, para lo que esta fase estaría alineada tanto con el segundo como con el tercer objetivo específico.

Finalmente, para la tercera fase que es la evaluación se alinea con el cuarto objetivo específico que habla de evaluar la solución.

Capitulo II

Estado del arte

En el desarrollo de la investigación es necesario conocer algunos conceptos relacionados con la seguridad de la información, criptografía, PKI y sus componentes, poniendo énfasis en la fundamentación teórica con la que se desarrolla el proyecto.

Se ha elegido el análisis de los sistemas criptográficos que se utilizan actualmente para la seguridad de la información, en vista del constante incremento de documentos digitales y menor emisión de documentos impresos en papel, por lo que es necesario incrementar las seguridades de los archivos electrónicos para garantizar la fiabilidad y confianza en los mismos (Villalba, 2014).

La existencia de la criptografía de clave pública permite otorgar seguridad para la comunicación entre dos o más usuarios conociendo la clave pública entre ellos, existen varios asuntos que necesitan ser resueltos: ¿Cómo generar una comunicación con alguien que no hemos contactado antes?, ¿Cómo generar, emitir, administrar, almacenar, renovar y revocar las claves públicas y certificados? Para dar solución a estas interrogantes se creó la Infraestructura de Clave Pública (PKI).

Si se desea contar con un certificado digital, es necesario que el proceso lo realice una entidad de certificación y para su implementación se necesita una herramienta o software especializado. Por lo general el costo para la implementación de una entidad de certificación es muy elevado debido a que es especializado y ajustable a los requerimientos de cada institución. Por esta razón se evalúan varias herramientas de software libre que pueden dar soluciones de certificación con bajos costos.

Fundamentación teórica

Seguridad de la información

El crecimiento y auge de las redes de comunicaciones, la creación de nuevos servicios asociados con la transferencia de datos a nivel mundial mediante el internet, así como el gran número de transacciones que diariamente se realizan, conlleva un enorme aumento en los ataques informáticos que se producen diariamente utilizando modalidades avanzadas y hostiles a las que se encuentra expuesto cualquier dispositivo que se encuentre conectado al internet (Mieres, 2009).

Todas las personas y organizaciones están comprometidas a ataques informáticos que comúnmente pretenden robar información e identidades, en servidores con datos de clientes e información personal, incluso datos sensibles de organizaciones militares o médicas (Abril, 2013). Es de cuestionar si los encargados de las tecnologías de la información en cada organización cumplen y hacen cumplir todas las metodologías y políticas necesarias para mitigar y minimizar el riesgo de los ataques informáticos.

La seguridad de la información es una disciplina que garantiza la implementación de un entorno que cuente con todas las protecciones ante vulnerabilidades, debilidades y ataques para la información y los datos de las personas y organizaciones (Ormaza A. , 2016).

Cuando nos referimos a seguridad de la información la definimos bajo el concepto de preservar la disponibilidad, integridad y confidencialidad de los datos utilizando diferentes técnicas, planes, acciones y soluciones de protección (Figueroa, 2017). De este modo aparecen para su estudio los pilares fundamentales de la seguridad de la información.

Pilares de la seguridad de la información

En la actualidad se considera a la información como uno de los activos más importantes y de valor importante dentro de las organizaciones productivas y de las personas en general, considerando que el dominio de los datos representa una gran ventaja competitiva de acuerdo al uso en el ámbito de negocio o personal (Zuñiga, 2015).

Se considera a la integridad, disponibilidad y confidencialidad como los pilares fundamentales de la seguridad de la información sobre los que se sustenta la confianza de las personas y organizaciones.

Integridad

Se refiere básicamente a que los datos o la información que contiene un documento no sean modificados sin los permisos necesarios. Este aspecto se refiere a que una persona sin autorización agregue o quite datos e información de forma intencional o accidental.

Disponibilidad

Los datos y la información deben estar accesibles, utilizables, continuos y disponibles para usuarios autorizados en el momento que lo requieran.

Confidencialidad

Uno de los aspectos más importantes en la seguridad de la información, la confidencialidad debe asegurar que los datos únicamente sean accesibles y utilizados por personas autorizadas.

Estado de los datos

Al tratarse del activo más importante que posee una empresa, institución o persona en general los cuidados con los datos no se escatiman, es un derecho fundamental de las personas el cuidado y protección de sus datos, dependiendo de

los estados en que se encuentren se tienen diferentes métodos de protección y características de su funcionamiento (García A. , 2007).

En reposo

El término en reposo para los datos es cuando la información puede estar almacenada en un medio lógico o físico como memorias externas, discos duros o ficheros y que esta información no esta ha sido usada, accedida ni procesada.

Esta información en reposo únicamente es segura cuando está encriptada y su clave no se ubica en el mismo lugar de almacenamiento, además, que sea lo suficientemente fuerte para evitar ataques de fuerza bruta o diccionario.

En tránsito

Los datos o la información que se mueven por un canal de comunicación público o privado sea este de mensajería, correo electrónico, aplicaciones web o cualquier forma de paquete que viaje en la red.

Actualmente la mayor cantidad de datos se encuentran en tránsito por cualquier medio sobre todo en las redes sociales, la mejor forma de prevenir y evitar ataques es la restricción de acceso a lugares de dudosa procedencia además del cifrado de datos cuando se envía y recibe.

En proceso

Muy comúnmente llamados datos en uso, es decir que se encuentran ya en las tablas de una base de datos siendo analizados.

Cuando los datos o la información están en tratamiento generalmente existe de por medio un usuario interesado en datos sensibles que logra romper las defensas y obtiene acceso a la información. Para dar protección a estos datos la mejor forma es hacerlo con anterioridad, con acciones preventivas que eviten

entregar la información como herramientas de control de acceso, gestión de identidad y generación de claves seguras.

Contramedidas

Son las técnicas y tácticas para proteger un sistema ante amenazas y vulnerabilidades. Las contramedidas tienen como objetivo principal evitar la explotación de las vulnerabilidades de un sistema y de este modo evitar la entrega de información relevante que comprometa su accionar.

Tecnologías.

La industria debe tomar cartas en el asunto y adaptarse a los requerimientos de seguridad de las organizaciones en el ámbito tecnológico, con equipos modernos que minimicen los riesgos de ataques y generen tranquilidad en los usuarios (Téllez, 2018). La tecnología de la información domina más de un área en las organizaciones y es un punto clave en el factor económico, el mal almacenamiento, la pérdida de datos o la divulgación de la información pueden traer graves consecuencias. Entre algunas de las más importantes tecnologías en seguridad de la información están las siguientes:

Criptografía: los algoritmos criptográficos de clave pública se utilizan para generar llaves tanto públicas como privadas, de este modo realizar transferencias de información segura.

Protocolos de enrutamiento: son los responsables de mantener una ruta conocida para el intercambio de información, además de proporcionar las reglas de comunicación entre los routers.

Clasificación de los datos: existe gran cantidad de información a nuestro alrededor, una de las formas para generar mayor seguridad es clasificándola de acuerdo con su importancia y de este modo otorgar jerarquización en el acceso, dependiendo del rango en el que se la ubique.

Sistemas operativos seguros: los sistemas operativos deben tener controles y claves de acceso, mantener siempre actualizados los sistemas de antivirus y de seguridad, así como administrar los puertos y entradas que no se requieran disponer.

Conexiones de red: todos los dispositivos deben tener una conexión segura con los protocolos HTTPS y SFTP. Es recomendable mantener únicamente habilitados los puertos y servidos que se requieren.

Formación y capacitación.

En el ámbito del manejo del talento humano la capacitación es un proceso prioritario en la seguridad de la información, se trata de mejorar, actualizar y ampliar las habilidades y actitudes de las personas y sus conocimientos en el campo de seguridades. El proceso de capacitación ayuda al cumplimiento de los objetivos de la organización generando una cultura en valores que aporta al crecimiento de las personas, ayuda al desarrollo de sus tareas, evita vulnerabilidades y reduce el gasto de la organización (Rendón, 2020).

Uno de los puntos a tomarse en cuenta dentro de las normas y políticas de seguridad, es la implementación de procesos de capacitación al personal tanto por las funciones que desempeñan como la relación con los datos que manejan, de este modo, se adquiere el conocimiento necesario para tomar las medidas adecuadas ante cualquier eventualidad. Un plan de capacitación para que se considere efectivo debe cumplir algunas condiciones:

- Los planes de capacitación deben definir un alcance en concordancia con las responsabilidades y tareas de los empleados.
- Tener un lineamiento con los objetivos y metas de la organización.
- Contar con el presupuesto necesario para capacitaciones.

- Ubicar adecuadamente al personal para que de este modo se pueda poner en práctica y se optimice los conocimientos.

Políticas y procedimientos.

Son protocolos, normas y procedimientos a seguir en los que se dan a conocer los lineamientos para proteger la seguridad de la información y los datos, definir funciones y responsabilidades dentro del entorno de la organización, con el objetivo de obtener un correcto funcionamiento (Antillano, 2007). Según (Altamirano, 2017). Las políticas de seguridad son parte fundamental, con gran impacto dentro de la organización, los objetivos y responsabilidades no estarían correctamente delimitados sin una política de seguridad. Para obtener resultados efectivos en las políticas de seguridad debe existir una combinación entre la cultura organizacional, las herramientas y el monitoreo permanente además de la participación y predisposición de los usuarios directos, sin dejar de lado el apoyo técnico y económico (Dussan, 2006).

PKI

Conceptos generales

Criptografía

La transmisión de datos de forma segura se ha convertido en uno de los principales retos en el ámbito digital, es necesario asegurar la información de las personas y organizaciones, en la antiguamente esta seguridad se la proporcionaba de forma física ya sea guardias personales, cajas fuertes o políticas administrativas para el tratamiento de la información (Paredes, 2006). Con la llegada de las computadoras, así como el auge del internet que ha generado servicios automáticos de uso, almacenamiento y transferencias de datos la seguridad, es primordial para cualquier persona o institución garantizar la confidencialidad, integridad y accesibilidad pilares fundamentales de la seguridad de la información mediante sistemas de criptografía.

Criptografía proviene etimológicamente del griego Kriptos = ocultar y Graphos = escritura, que tiene como resultado ocultar la escritura mediante varias técnicas para que un mensaje no sea legible de forma clara.

La criptografía es una rama de las matemáticas que hace uso de diversas técnicas y métodos, con el objetivo de ocultar y proteger un mensaje, utilizando algoritmos y una o varias claves que únicamente las personas que las sepan o posean podrán descifrar o tener acceso al mensaje (Velasco, 2006).

La religión, la industria y la milicia son algunos de los ámbitos que generaron el nacimiento de la criptografía desde siglos atrás, los egipcios ya utilizaban técnicas de ocultamiento de la escritura entre ellos los sacerdotes con los jeroglíficos otro claro ejemplo en el uso de la criptografía es la escítala espartana usada en la guerra de Atenas y Esparta que no era más que una vara en la que enrollaban un tira de lana o cuero en la que se escribía el mensaje (Fernández, 2004).

León Batista Alberti considerado por muchos el padre de la criptografía, en el siglo XV, desarrolló una máquina que poseía dos discos concéntricos que giraban de forma independiente con lo que se generaban alfabetos de transposición diferentes. Los métodos de Richelieu y Rossignol fueron utilizados por Napoleón cuando en sus documentos estratégicos militares enviaba números en vez de letras o grupos de letras para evitar que sus mensajes fueran descubiertos.

En las guerras del siglo XX la criptografía tuvo su máximo auge y fue empleada en el ámbito militar, las fuerzas alemanas crean la máquina **enigma** que enviaba mensajes de manera oculta, mediante el giro preciso de tres cilindros que generaban una letra del mensaje. Mucho tiempo transcurrió hasta cuando los mandos aliados tomaron la decisión de constituir un grupo de expertos entre los cuales se encontraba Alan Turing, para generar otra máquina que lograra descifrar estos mensajes. Es así como nace la máquina Colossus (Paredes, 2006). Existe una

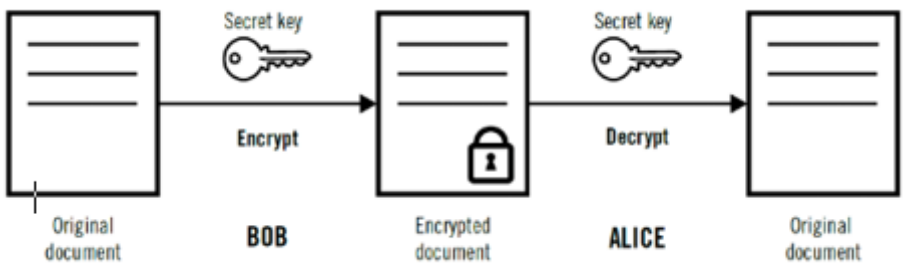
gran variedad de ejemplos en la historia de la criptografía. En la actualidad, el internet hace uso de varios algoritmos criptográficos que incluso a la vista del usuario es imperceptible, generalmente esto ocurre cuando tratamos de hacer compras en línea, verificamos nuestra cuenta bancaria o incluso visitamos nuestro sistema de mensajería (Velasco, 2006).

Criptografía Simétrica o de clave secreta

Este tipo de criptografía es la más conocida y utilizada por su simplicidad, desde la antigüedad por egipcios y romanos y en la actualidad en cifrado de datos y correo electrónico, su principal característica es el uso de una sola clave para cifrar y descifrar documentos (Carvajal, 2007). Se han generado inconvenientes porque el transmisor debe enviar su clave al receptor y al ser única en su transmisión puede ser interceptada y con ello quedan al descubierto los datos. Uno de los primeros proyectos realizados por el gobierno de los estados unidos fue el sistema DES con un tamaño de 56 bits corto y fácil de descifrar. Posteriormente en 1998 se creó el sistema criptográfico 3DES mejorando su nivel de seguridad y aumentando su tamaño a 192 bits. Finalmente, en el año 2001 se crea AES con un tamaño de 128 bits, mucho más rápido que sus antecesores y con mayor seguridad, es utilizado hasta la actualidad.

Figura 1

Criptografía de clave primaria



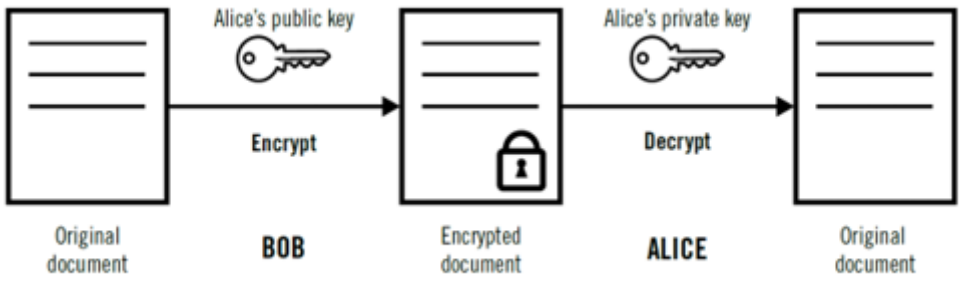
Criptografía Asimétrica o de clave pública

La criptografía asimétrica es mucho más moderna, actualmente se la utiliza comúnmente en el comercio electrónico. Consiste en generar dos pares de claves una pública y una privada tanto para el emisor como para el receptor las claves públicas serán intercambiadas y utilizadas para cifrar los mensajes, mientras que las claves privadas permanecen con los usuarios de forma segura con la que pueden descifrar los datos. Este tipo de cifrado es mucho más seguro, y principalmente cumplen con el requerimiento de no repudio y aceptación (García F. Y., 2018).

Dentro de la criptografía asimétrica tenemos al algoritmo RSA, que factoriza un número resultante de multiplicar dos números primos. Otro método muy conocido es el de Diffie-Hellman que se basa en calcular logaritmos discretos para un cuerpo infinito que luego de diferentes operaciones y aplicaciones matemáticas genera las claves compartidas.

Figura 2

Criptografía de clave pública



Función Hash

También conocida como función resumen, proporciona una porción o resumen de un mensaje, esta función permite obtener de un conjunto de bits con longitud arbitraria un conjunto de bits con una longitud preestablecida generalmente 128,256 o 512 bits (Arrieta, 2017). Este código es único para cada entrada y es

usado comúnmente para garantizar que un documento no haya sido retocado. Tiene como característica que no es irreversible es decir no puede generar el documento original con el código de salida. Entre los algoritmos más conocidos están MD5 y SHA I, SHA 2 y SHA 3

MD5

Su creador Ron Rivest en el año de 1991 lanza el algoritmo Message Digest Algorithm 5 el mismo que genera un código de 128 bit de tamaño, por motivos de debilidades en su estructura aparece SHA I (Delgado, 2006).

SHA I

Para 1993 aparece Secure Hash Algorithm con técnicas similares a la de MD5 pero con mayores seguridades generando un código de 264 bits, es usado para la distribución de firmas y certificados digitales.

SHA 2 y SHA 3

Son versiones más modernas que SHA 1, creadas por las debilidades descubiertas en sus versiones anteriores.

DSA

Utilizado y aprobado generalmente para firma digital Digital Signature Algorithm utiliza una clave pública no muy recomendable para la transmisión confidencial.

Firma digital

Una firma digital nace de un procedimiento criptográfico con el objetivo de instaurar una dependencia única entre el firmante y la firma, dando fe del archivo realizado y la aceptación de los compromisos que este contenga similar a una firma manuscrita (Ormaza D. , 2017). En la actualidad facilita la transferencia de

información segura por medios electrónicos, las firmas digitales deben estar preparadas y ser susceptibles a verificaciones por una tercera parte que permita detectar anomalías en las firmas o firmantes.

Con la firma digital se concede al receptor la capacidad de autenticación y verificación y de los orígenes de la información, así como también que en el transcurso no haya sido modificada.

Mediante la firma digital es posible realizar cuatro operaciones básicas: generar, extender, archivar y verificar. Cuando se crea un dato y se lo asocia a un documento de tal forma que este dato sea único y se vincule al documento. Cuando se aplica sellos de tiempo a un documento con el fin de garantizar que la firma digital se mantenga vigente en el tiempo se refiere a archivar. Revisar que el documento no ha sido alterando desde el momento de su firma y autenticar la identificación del firmante es el momento de verificar la firma digital, finalmente archivar es el mantenimiento de los documentos. La firma digital se mantiene activa por muchos años, con esto acredita la autoría de acciones y manifestación de voluntad existentes en los documentos.

Certificado Digital

Es un documento que demuestra e identifica los atributos del poseedor, los certificados digitales actúan como una credencial electrónica y tienen la función principal de restringir, verificar y proporcionar acceso a la web evitando suplantaciones de identidad, las entidades que validan los certificados digitales son las Autoridades de Certificación (CA) quienes garantizan que los certificados tengan validez ante terceras personas (Talens, 2012). Se utiliza un sistema de cifrado de datos con clave pública y privada para encriptación y des encriptación de la información correspondiente a los certificados digitales.

Normas de certificación

Estándar X 509

El estándar X 509 pertenece a la ITU (International Communication Union) y contiene formatos, normativas y estándares para certificados e infraestructuras de clave pública, se publicó en el año 1988 con la primera versión X 500, posteriormente en 1993 se publica la versión 2 que se establece como únicos datos del certificado del emisor y el usuario final, existe una versión 3 con su principal característica de generar soporte tecnológico de mallas y bridges (Pérez, 2018).

Las especificaciones para la implementación de listas de certificados de PKI también están incluidas en el estándar X509.

Dentro de los elementos del estándar X509 se encuentran:

- Versión

En este apartado se coloca la versión del estándar X 509 en el cual se creó 1,2 y 3.

- Número de serie de la certificación.

Es el número único perteneciente a cada certificado y es otorgado por la autoridad certificadora al momento de su creación.

- Identificador del algoritmo de firma.

Este es el apartado que presenta el nombre o tipo de algoritmo que se utilizó en la firma del certificado digital.

- Datos del emisor.

Aquí se detalla la autoridad certificadora que ha emitido y firmado los certificados.

- Tiempo de validez.

En este apartado se puntualiza la duración valida del certificado, se detalla una fecha de inicio y una fecha de caducidad hasta la cual el certificado tiene validez.

- Nombre del usuario.

En este campo se coloca la identificación del usuario que debe ser único para la autoridad de certificación.

- Información de la clave pública del usuario.

Se detalla la información de la clave pública, los parámetros y algoritmos asociados con el usuario del certificado.

- Identificador único del emisor.

Este apartado es opcional y permite tener una identificación del emisor de un certificado digital, hace una reutilización de nombres.

- Identificador único del sujeto.

Se puede colocar de forma opcional y utilizarse para la identificación única del dueño del certificado digital.

- Extensiones.

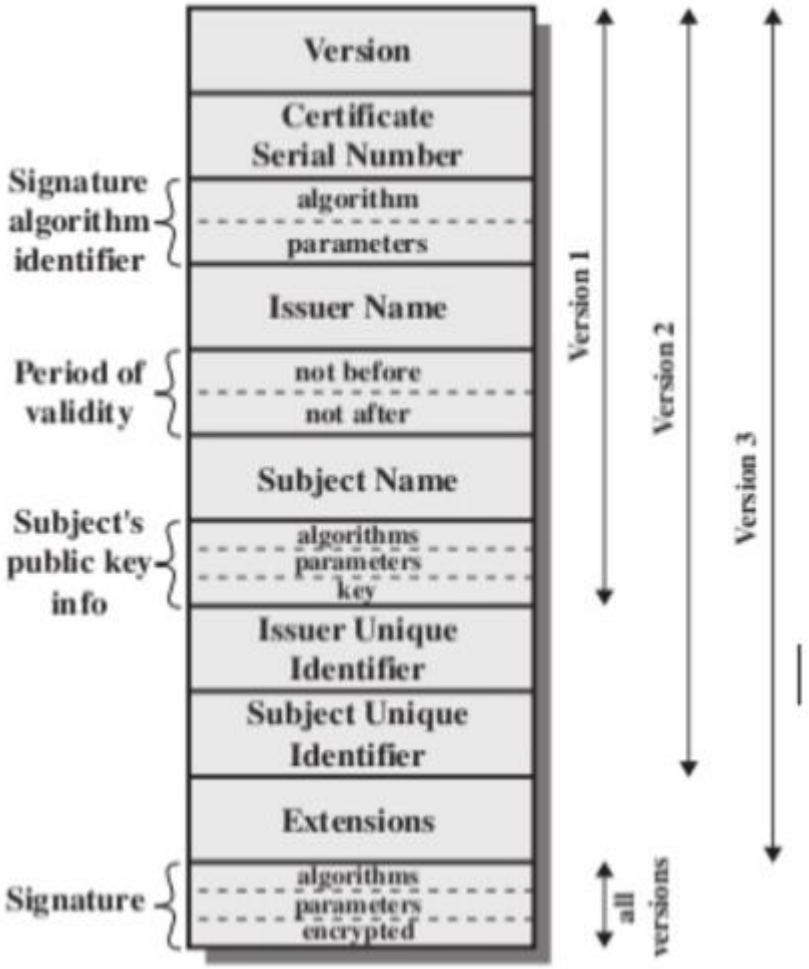
Se encuentran especificaciones opcionales que corresponden a la utilización y tratamiento del certificado.

- Firma digital del certificado.

  Se detalla la firma real gestionada con la clave privada y su respectivo algoritmo específico de la entidad que la emitió.

Figura 3

Firma Digital



PKI (Public Key Infrastructure)

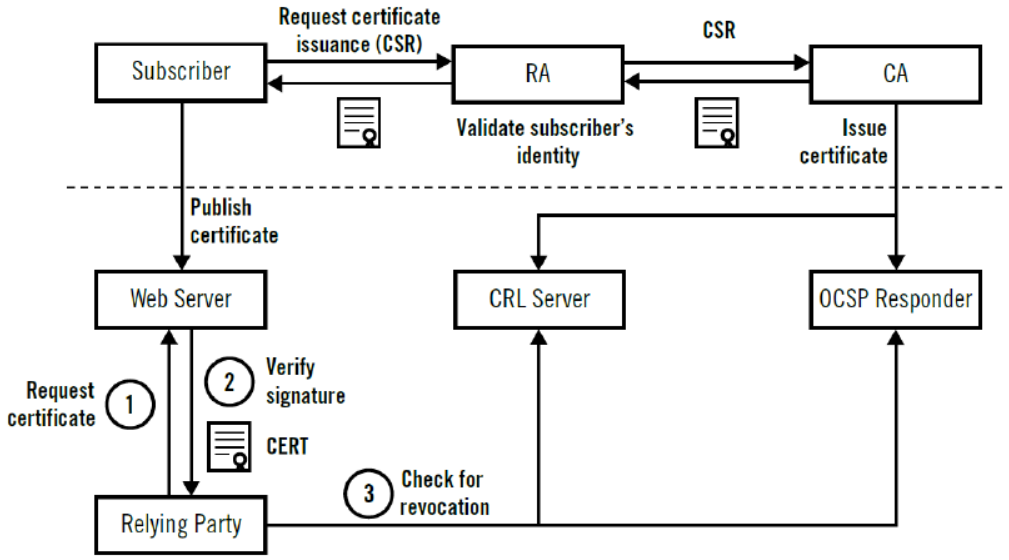
El tema principal en este proyecto de investigación es abordar más a detalle la PKI (Public Key Infrastructure) Infraestructura de clave pública por sus siglas en inglés, sus aplicaciones, utilidades e implementación para la solución de problemas de seguridad de la información.

Una PKI es una combinación de software, hardware, así como también procedimientos y políticas que soportan criptografía de clave pública para la creación, administración, almacenamiento, distribución y revocación de certificados (Castro, 2015). Brinda un gran soporte a la utilización del cifrado de claves públicas y

permite autenticar a los usuarios que intervienen en una comunicación. Uno de los objetivos principales de una PKI es garantizar el no repudio y para ello se debe preservar la integridad de los datos y la identidad de la persona. (Urquijo, 2012)

Figura 4

Arquitectura PKI



Componentes de la PKI

Buscar y conseguir una comunicación segura entre varias entidades es el arte y la ciencia que realiza la criptografía, si no existe ningún inconveniente solventa los pilares básicos en la seguridad de la información las cuales son confidencialidad, autenticidad e integridad (Longueira, 2019).

La PKI trabaja en conjunto con reglas, normas y estándares para generar mayor confianza y seguridad en la transmisión de datos entre entidades y usuarios. Las PKI no están sujetas a ninguna tecnología en concreto, ya que proporcionan un marco de trabajo de acuerdo con las necesidades de cada circunstancia en la que se aplique. Su aplicación primordial es legitimar la seguridad y el intercambio de información sensible usando certificados digitales y claves criptográficas.

Entre los procedimientos más importantes que ejecutan las PKI están:

- Registro de usuarios
- Emisión de certificados
- Revocar certificados
- Recopilar certificados
- Gestionar el ciclo de vida de las claves

Para el cumplimiento de estas tareas las PKI cuentan con los siguientes elementos:

Usuario.

Los usuarios son los poseedores de las llaves tanto públicas como privadas que con la ayuda de herramientas tecnológicas validan firmas digitales, cifran documentos y proporcionan seguridad a sus datos.

Autoridad de Certificación (CA, Certification Authority).

Conocida como la parte de confianza que tiene la responsabilidad de dar fe y seguridad, así como legitimar la relación entre la clave pública y la identidad del usuario. Tiene que estar en capacidad de realizar la emisión, revocación y actualización de certificados.

Autoridad de Registro (RA, Registration Authority).

Son las encargadas de dar trámite a las peticiones o revocaciones de certificados. Responsable del enlace y concordancia entre el certificado o clave pública y el propietario, la CA puede realizar directamente esta comprobación. Cuando las personas entregan toda la documentación requerida a la RA esta la analiza y remite la aprobación a la CA que emite un certificado.

Repositorios.

Es la organización que proporciona almacenamiento sobre la estructura PKI principalmente de certificados y listas de revocación cada vez que el CA lo emite o lo revoca. A estos listados se los puede conocer como CRL (Certificate Revocation List).

Autoridad de Validación (VA, Validation Authority).

Genera un reporte del estado de los certificados cada vez que se realice alguna modificación por parte de la CA, validando cada uno de los certificados.

Características de una PKI

Las principales características con las que debe contar una infraestructura de clave pública para la transferencia electrónica segura son confidencialidad, no repudio, autenticación e integridad.

No repudio: es un terminado usado comúnmente en seguridad informática para indicar el falso rechazo de una persona en la participación de una comunicación electrónica o en el intercambio de información y datos. Se utiliza generalmente en la firma de documentos electrónicos con lo cual es imposible que cualquiera de las partes involucradas niegue o repudie su participación (Hernádez, 2008).

Integridad: cuando los datos permanecen completos, correctos y sin alteraciones o adulteraciones se dice que existe integridad en la información, los datos no pueden haber sido modificados o cambiados durante la transmisión, para su comprobación las PKI utilizan funciones hash con las que pueden comprobar su integridad.

Autenticación: la autenticación es permitir y verificar el acceso a determinada comunicación electrónica únicamente al personal autorizado, por medio

de su identificación o credenciales de identidad que en estos casos son comúnmente un usuario y una contraseña asignada.

Confidencialidad: garantiza que la información personal que se requiere transmitir entre un emisor y un receptor no sea vista, interferida o divulgada por un tercero. Para esto las PKI utilizan encriptación en los datos que se transmiten, de esta forma aseguran que la información no sea obtenida por usuarios no autorizados.

Funcionamiento básico

El alumno “A” quiere realizar una comunicación digital segura con el alumno “B”, el objetivo de esta comunicación es que no sea intervenida y que los datos no sean cambiados en el transcurso de la comunicación, así como también tener constancia de que la información fue realizada por las personas que intervinieron en el enlace en el caso de que una de las partes la negara. En la figura 5 se muestra como se realiza el proceso de una PKI.

1. El alumno “A” ingresa a la infraestructura PKI para generar sus claves pública y privada, posteriormente se realiza el trámite para solicitar un certificado digital esto va dirigido a la autoridad de registro. El mismo trámite realiza el alumno “B”.
2. La aceptación o negación de las solicitudes está bajo responsabilidad de la autoridad de registro, en el caso de ser aprobado se dirige el pedido a la autoridad de certificación para que realice el trámite de firma de contrato de aceptación de políticas y verificación de la identidad del alumno, este trámite puede ser realizado también por la misma autoridad de registro.

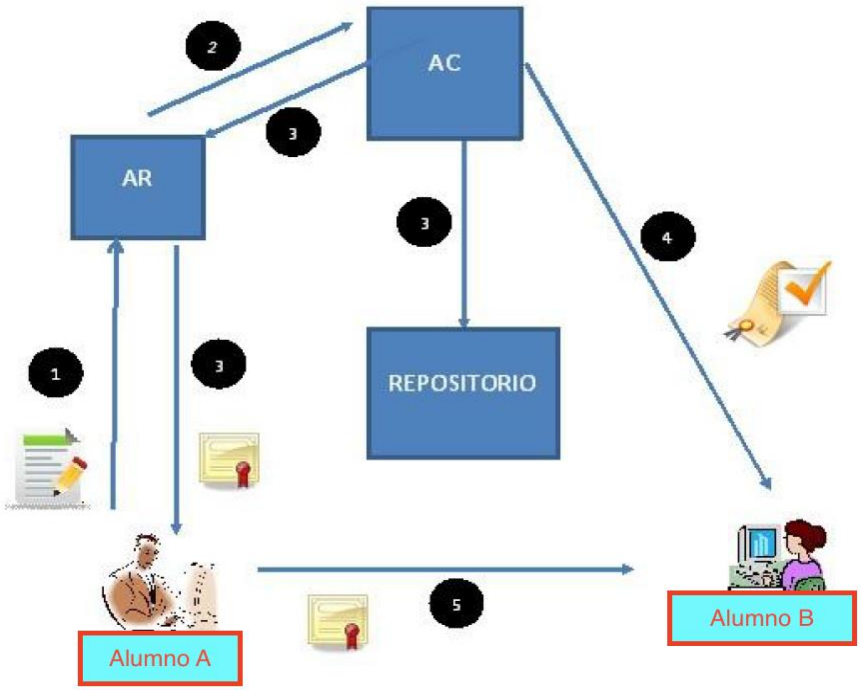
3. Los alumnos reciben una notificación por parte de la autoridad de registro sobre su trámite, además, queda almacenado en un repositorio por un tiempo determinado por las políticas de la entidad de certificación.

4. Para la comunicación es necesario saber las claves públicas de ambos, que se encuentran almacenados en repositorios que son accesibles o por pedido a las autoridades de certificación.

5. Para finalizar, cuando los alumnos A y B tengan las claves públicas de ambos, podrán realizar una comunicación segura y confiable.

Figura 5

Funcionamiento PKI



Modelo de gestión de la PKI

Un modelo se puede definir como una representación cualitativa o cuantitativa de un proceso con el que se observan los efectos de los factores importantes para cumplir con el propósito propuesto (Velásquez, 2003). Se obtienen resultados de análisis experimentales, se establece límites en su accionar, con pruebas para obtener como resultado una comprensión más clara de las características de la situación.

La gestión por su parte es la acción de realizar diligencias encaminadas al logro o administración de un negocio, en algunos casos la gestión ayuda al proceso en la toma de decisiones aplicando conocimiento de las ciencias empresariales y económicas (Córdoba, 2012).

Se puede definir un modelo de gestión como el marco de referencia para administrar una organización. En el caso de una PKI se gestiona todo el proceso que engloba la emisión de certificados de forma segura.

Metodologías para implantar una PKI.

ITIL

(Information Technology Infrastructure Library) debido a sus siglas en inglés que traducido al español es “Biblioteca de infraestructuras de tecnologías de la información”, se lo reconoce mundialmente por las mejores prácticas de gestión para los servicios de tecnología de la información (ITSM). ITIL ayuda también al mejoramiento continuo y desempeño de las organizaciones (Bravo, 2020).

A finales de 1980 aparece su primera versión que contempla alrededor de 38 libros en los cuales aborda temáticas sobre nivel de servicio, gestión de incidentes, plan de contingencia y gestión de cambios.

Para el año 2000 nace la versión 2 de ITIL que reduce sustancialmente la cantidad de libros de manera lógica, la mayor novedad es que formaliza el estándar BS 15000: 2000, además del código de buenas prácticas DISC PD 005.

Para el año 2007 se publica una versión 3 de ITIL con cambios mayores, proporciona una visión mayor del ciclo de vida completo de los servicios y detalla ampliamente los componentes de apoyo indispensables para la prestación de servicios.

Luego de una actualización del modelo con mejoras menores en el año 2011, pasa a su versión actual: ITIL v4 donde se enfoca en el valor y el ciclo de vida del servicio, no solo como procesos si no como una estructura de ciclo de vida, llamada sistema de valor de servicio.

El modelo de ITIL v4 se enfoca en el valor del servicio y posee información acerca de:

Entender conceptos principales de la gestión de servicios de TI.

Dimensiones del servicio y principios guías de ITIL.

Los componentes del sistema de valor de servicio y conceptos claves de la mejora continua.

Prácticas de ITIL y su contribución a las actividades de la cadena de valor.

ITIL v4 tiene cuatro dimensiones para la gestión de servicios, incluye personas y organizaciones dentro de la empresa como: proveedores, socios, clientes, tecnologías utilizadas. Para su mejor entendimiento considera cuatro dimensiones. El éxito del servicio depende de la correcta interpretación y tratamiento de sus dimensiones que son:

Información y tecnología.

Organizaciones y personas.

Proveedores y asociados.

Procesos y flujos de valor.

ITIL v4 contempla 7 principios para una mejora continua dentro de las organizaciones:

Centrarse en el valor.

Se debe tener claro que la organización debe generar valor para los clientes y las partes interesadas. Es necesario tomar en cuenta la experiencia del usuario del servicio y como éste les beneficia.

Empiece donde está.

Para avanzar con mayor rapidez optimizar el contenido y generar apoyo de sus colaboradores, es recomendable realizar los cambios a partir del punto en donde nos encontramos y no volver a hacer todo desde cero ya que esto puede tener efectos negativos.

Progrese iterativamente con comentarios.

Realizar divisiones del trabajo permite saber dónde nos encontramos y de este modo ir cumpliendo las metas específicas que lleguen a contribuir con el objetivo general. Realizar retroalimentaciones es indispensable para saber que las tareas realizadas están siendo bien enfocadas y apropiadas.

Colaborar y promover la visibilidad.

Colocar a las personas en los roles indicados beneficia al cumplimiento de los objetivos de la organización sumado a la cultura de colaboración que se debe promover, esto agrega mucho más valor a todas las partes involucradas, la forma

correcta es emitir información clara que sea entendida por todos los miembros de la organización.

Piense y trabaje de manera integral.

Una organización funciona como un todo y las decisiones que se tomen tendrán repercusión en el resto de las áreas. Se debe pensar con cabeza fría antes de tomar acciones que generen inconvenientes en alguna área y eviten que la organización cree valor.

Mantenlo simple y práctico.

Los procesos deben ser lo más simple posibles siempre que se pueda, existen procesos complejos que pueden reducir su cantidad de actividades, transformándose en tareas más básicas que crean valor en las personas involucradas.

ITIL 4 Sistema de valor de servicio

Más comúnmente conocido como SVS (Sistema de Valor de Servicio) se considera una parte muy importante dentro de ITIL v4 ya que ayuda a la generación conjunta de valores. Se describe que los componentes y actividades se interrelacionan y trabajan en conjunto para dar valor a las organizaciones y todas las partes interesadas.

La parte principal del SVS es la cadena de valor del servicio, que no es más que la combinación de seis actividades clave que deben trabajar en conjunto para dar valor a los usuarios finales mediante la entrega del servicio adecuado, todas las actividades reciben insumos de fuentes externas y están interconectadas entre sí, a continuación, se detallan las actividades de la cadena de valor: planificar para mejorar, comprometerse, diseño y transición, obtener o construir y entrega y soporte.

Prácticas

En ITIL v4 las prácticas de gestión son un conjunto de recursos organizacionales que se enfocan en realizar u obtener un objetivo. Una de las diferencias entre ITIL v3 y la v4 es justamente que en la versión más actual describe prácticas en lugar de procesos, estas prácticas en general contribuyen al dominio de la gestión empresarial con 14 prácticas, la gestión de servicios con 17 prácticas y las soluciones tecnológicas con 3 prácticas.

ITIL (Ciclo de vida)

Estrategia de servicio de ITIL

Cuando una organización de TI pretende ofrecer un servicio, lo primero que debe abordar es la estrategia de servicio, para comprender y estudiar las necesidades y los objetivos de los clientes en lo referente a TI. De esta manera puede crear un servicio que cumpla con las expectativas del usuario y la organización.

Cuando las actividades de la organización de TI y los objetivos de la organización y las necesidades del cliente están en consonancia, el proceso y su resultado será de mayor valor y la organización de TI podrá ser una fuerza habilitadora al interior de la organización.

La estrategia de servicio está conformada por los procesos que se indican a continuación:

ITSM:

- Gestión de estrategia
- Administración financiera
- Gestión de cartera de servicios

- Gestión de la demanda

Para garantizar que una organización provea los servicios de TI a los precios más cómodos, es necesario tener un proceso de gestión financiera que considere los factores del mercado y el cliente, este estudio siempre va en busca de un equilibrio entre calidad, demanda y precio cumpliendo con todos los requisitos que la organización lo disponga y requiera.

La cartera de servicios se refiere a la oferta de servicios que dispone una organización, que debe cumplirse de manera satisfactoria para los clientes, esta cartera contiene todos los servicios de TI, los que no se han ofrecido aún y los que han sido retirados de la oferta y ya no posee la organización de TI.

Diseño de servicios de ITIL

Los servicios que presta la organización, los factores tecnológicos mas todos los elementos que llevan a cabo el diseño de servicio deben centrarse en cumplir con los objetivos de ITIL. Al incluir la evaluación de procesos dentro del diseño del servicio se obtiene como resultado mejoras en la coordinación dentro de la organización, como por ejemplo cuando se enlazan los entornos comerciales, técnicos y financieros generando óptimos resultados.

Cuando se habla de procesos de servicios debe considerarse:

1. Coordinación de diseño.
2. Servicio de gestión de catálogos
3. Gestión de nivel de servicio
4. Gestión de seguridad
5. Administración de suministros
6. Administración de disponibilidad

7. Gestión de la capacidad
8. Gestión de la continuidad del servicio de TI

Una de las responsabilidades más importantes de los diseñadores de servicios es la gestión del catálogo de servicios, que se encuentra generalmente como un portal en la web donde se presentan todos los servicios y la información de cada uno de ellos como: solicitudes de servicio, servicios disponibles, pasos a seguir, asesoría en línea, personal de agentes disponibles, precios y ayuda en general para cada servicio.

Transición del servicio ITIL

Cuando se termina el diseño y comienza la operación del servicio entran en acción los procesos de transición de servicios. En este momento los nuevos servicios pasan de su etapa de diseño a su etapa de ejecución o implementación real. ITIL cuenta con siete procesos de transición que tienen como objetivo orientar a los nuevos servicios de TI para que cumplan con las exigencias estratégicas previstas, además de que cumplan con su vida útil de manera eficiente.

Los procesos de la fase de transición de servicios de ITSM son:

1. Plan de apoyo y transición.
2. Gerencia del cambio
3. Ayuda activa y manejo de configuración
4. Gerencia y lanzamiento de despliegue
5. Sistema de prueba y validación
6. Análisis de cambio
7. Gestión del Conocimiento

El ciclo de vida de Deming está presente en varios estándares de calidad y se refleja en todo el proceso de ITIL, más aún en la transición del servicio, la actividad más importante es la evaluación del servicio para garantizar que la oferta de servicios se cumpla adecuadamente cuando se ponga en marcha, dentro de estas pruebas están la de validación, prueba de servicio y validación de cambios.

Del proceso de organización de TI se encarga la gestión del conocimiento, que cubre varios campos como el de recopilación de información y datos importantes, para evitar la redundancia en la adquisición de conocimiento. Permite a la organización obtener estrategias claras para tomar decisiones en el ámbito de gestión.

Operación del servicio ITIL

La fase más crucial del ciclo de vida del gestión de servicios de TI es la operación del servicio de TI, que en síntesis es manejar los procesos ITIL y las mejores prácticas que ayuden a la organización a generar los niveles de satisfacción adecuados para los clientes o usuarios finales. Este es el punto más relevante porque sin una óptima operación de este servicio, ninguna otra etapa del ciclo de vida serviría, considerando que en la operación interviene como actor principal el valor real que se le da al cliente.

Dentro de la operación del servicio de TI se tiene:

1. Gestión de Acceso
2. Gestión de eventos
3. Petición de cumplimiento
4. Administración de problemas

5. Manejo de Incidentes

Las operaciones de servicio de TI tienen cuatro funciones que son:

1. Mesa de servicio
2. Dirección técnica
3. Manejo de aplicaciones
4. Administración de operaciones de TI

ITIL posee un servicios entorno a asistencia técnica que es la pieza fundamental debido a que realiza operaciones de contacto directo con los problemas que se relacionan con los procesos de ITSM, así como también tiene un canal de comunicación con las necesidades del personal de TI, usuarios finales y clientes.

Aspectos como el control de incidentes, asesorías técnicas, recepción de solicitudes, cambios de interfaz, ayuda en la configuración, mejora del servicio entre muchas otras más, son atendidos por personal calificado y profesional que entrega su conocimiento y apoyo para el logro de los objetivos de la organización.

ITIL Mejora continua del servicio

Cuando se llega a la fase final del ciclo de vida, se habla de una mejora continua de la gestión de servicios basada en ITIL, en esta parte los dueños de los procesos resuelven incertidumbres tales como ¿Qué hacer para dar un mejora a la eficiencia en los servicios de TI de una organización?, o, ¿Qué hacer cuando las tareas no se ejecutan de acuerdo con lo planificado? Hay que destacar que la mejora continua es un proceso en el que se analizan datos e información de hechos y acciones ocurridas, para mejorar y obtener lecciones aprendidas.

Son de gran ayuda para la mejora continua los procesos para medir la calidad del servicio, los informes del servicio y el cálculo del rendimiento de la inversión, y

finalmente existen siete pasos que ayudan a implementar metodologías mejoradas de gestión de servicio que son:

1. Establecer el plan de mejora.
2. Determinar lo que se pretende medir.
3. Recolección de datos
4. Procesamiento de los datos
5. Análisis de datos e información.
6. Exponer y hacer uso de la información.
7. Ejecutar mejoras

El servicio y su mejora continua dependen mucho de varios procesos. Entre ellos la gestión del conocimiento, que se encarga de la recopilación, estudio y análisis de datos que permitan tomar las mejores decisiones con el fin de mejorar e innovar un cambio organizacional.

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.

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.

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.
- 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.

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.

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.

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. 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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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:

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.

Los certificados y firmas electrónicas que sean publicados por entidades certificadoras no acreditadas serán denominados certificados de firma electrónica no acreditados, con lo cual queda a responsabilidad del usuario probar su validez ante las autoridades competentes de ser necesario.

Las entidades de certificación no acreditadas cuentas con menos privilegios que las entidades acreditadas, uno de ellos es que el sector público no puede acceder a los servicios de certificación de entidades no acreditadas conforme a lo establecido en el artículo 7 de la resolución 584.

Herramientas de software libre para crear una PKI

PGP

Pretty Good Privacy por sus siglas en inglés quiere decir privacidad bastante buena, su creador es Phill Zimmermman. Es una herramienta creada para encriptar correos electrónicos, discos duros, documentos, datos entre varias aplicaciones más, una de las características más importantes es que se adapta y es compatible entre varias plataformas, es por ello que el usuario tiene protección en su correo electrónico, archivos y datos mediante cifrado con lo cual solo su destinatario podrá descifrar el contenido (Travieso, 2003).

PGP está creada para utilizarse tanto para usuarios comunes, así como también a grandes niveles en empresas y corporaciones manteniendo su estándar de calidad en seguridad por lo que se convirtió en un software de los más usados en el mundo (Cedillo, 2006).

Es de fácil de accionar; específicamente se generan dos llaves la pública y privada. La privada es aquella que mantiene el usuario en secreto y con la cual se des encripta los datos, la pública es aquella que se transmite a los demás y su utilidad permite que otros usuarios puedan enviarle un mensaje cifrado.

Además, en la firma de documentos digitalmente se utiliza la llave privada para sellar el documento y generar autenticidad en el mismo, posteriormente cuando el documento llega a su destino PGP comprueba los datos y la firma con la llave publica que posee el remitente, de existir algún cambio tanto en los datos como en la firma se emite un mensaje de que la persona o el documento no son los correctos (Lee, 2013).

PGP está disponible en su página web https://www.openpgp.org/ para su descarga con sus versiones más recomendadas para cada sistema operativo.

OPENCA

Es un proyecto de código abierto que nace en el año 1998 para implementar autoridades de certificación robusta utilizando otras aplicaciones open source como OpenLDAP, Apache, OpendSSL. Este software posee una interfaz web mediante el servidor Apache, que le concede funciones de una PKI y genera operaciones de la autoridad de certificación como: solicitud de certificados, revocación y búsqueda de certificados. Esta aplicación permite también la verificación y comprobación del estado de los certificados (Boiero, 2014).

EJBCA

Conocida por sus siglas en inglés Enterprise Java Bean Certificate Authority (EJBCA), es una herramienta basada en código abierto para la implementación de autoridades de certificación de clave pública de acuerdo con estándares X.509 e IETF.PKIX. Posee gran flexibilidad en sus componentes y mucha facilidad para que se acoplen con sus arquitecturas de certificación, posee una interfaz web service así como el servicio XML Key Management Specification.

Es una herramienta muy robusta que soporta múltiples niveles de usuarios AC y diferentes módulos Hardware Security Module (HSM). Esta herramienta puede ser instalada bajo cualquier servidor de aplicaciones J2EE como Glassfish, Weblogic, Oracle containers siendo la más óptima y sencilla JBoss bajo GPL (Solinas, 2013).

XCA

Una aplicación muy conocida y de fácil uso, la cual tiene como objetivo principal la creación y administración de certificados bajo normas X.509 así como también genera claves privadas DSA, RSA y smart card y todo lo necesario para la implementación de una CA. Permite la importación de los archivos y claves en

diversos tipos de formatos como DER o PEM, a partir de la versión 2.0 de XCA utiliza una base de datos SQL para el almacenamiento de elementos criptográficos.

Capítulo III

Administración General

Análisis del contexto

La Universidad de las Fuerzas Armadas “ESPE” es una de las instituciones de educación superior más reconocidas del país, con más de 99 años de experiencia en la formación de profesionales para la sociedad. La “ESPE” actualmente está compuesta por un campus matriz en Sangolquí, con sedes de Latacunga y Santo Domingo de los Tsáchilas y el Instituto de Idiomas en la ciudad de Quito. La Universidad de las Fuerzas Armadas “ESPE” cuenta con más de 13000 estudiantes entre civiles y militares además se encuentra dentro ranking de las 250 mejores universidades de América Latina y la cuarta mejor universidad en el Ecuador según Ranking mundial de universidades QS (Universidad de las Fuerzas Armadas "ESPE", 2014).

Dentro de la misión de la “ESPE” se considera la formación de profesionales con excelencia, cultivando valores éticos y morales, con un gran conocimiento científico y pensamiento crítico para atender las necesidades de la sociedad y de las Fuerzas Armadas. Los valores que se inculcan son la honestidad, el respeto, la disciplina, la identidad, la responsabilidad social y el civismo.

Análisis de la demanda

Los usuarios y beneficiarios directos de este proyecto son alrededor de 13000 estudiantes de la universidad de las Fuerzas Armadas “ESPE”, que se encuentren cursando sus estudios entre primero y noveno semestre, quienes podrán contar con una herramienta para firmar y enviar documentación de forma segura, como beneficiarios indirectos se encuentran los docentes y personal administrativo de la comunidad universitaria ya que se fortalece la confianza en la recepción de información y las seguridades informáticas.

El requerimiento principal de los estudiantes es contar con una forma segura de validar un documento generado por ellos y tener un respaldo que certifique que esta información no ha sido modificada hasta llegar a su destinatario. Con la firma electrónica generamos los principios de identidad, confidencialidad, no repudio e integridad para que sea utilizada por los alumnos de la universidad en sus actividades diarias.

Servicio requerido

Los avances tecnológicos hacen que se vayan disminuyendo las transacciones en papel y aumentando las seguridades en los dispositivos tecnológicos, mucho más en el ámbito académico. El servicio que se requiere es la generación y uso de certificados electrónicos, para firmar documentos de los alumnos de la Universidad de las Fuerzas Armadas “ESPE”, mediante la creación de una PKI con la herramienta de software libre EJBCA que proporcione certificados digitales.

Las principales características de los certificados digitales que se les proporciona a los estudiantes son:

- Que garantice el no repudio.
- Permita firmar documentos electrónicamente.
- Permita ahorrar tiempo y dinero en trámites administrativos mediante el internet.
- Garantice legalmente la identidad del alumno.

El presente proyecto propone que la Universidad de las Fuerzas Armadas ESPE cuente con una herramienta que facilite a los estudiantes, la firma de documentos sin la necesidad de imprimirlos, que asegure su integridad, autenticación de origen y no repudio agregando así valor legal al entorno virtual de la

institución, y que además su uso y/o adquisición no represente ningún valor monetario.

Los documentos serán firmados digitalmente con un algoritmo de firma digital compuesto de una función hash y un algoritmo criptográfico, ambos basados en estándares internacionales que serán definidos durante el transcurso de la investigación, la firma a su vez generará un código QR que proporcionará información del firmante.

Gestión de servicio

Diseño de políticas aplicadas al servicio

Políticas de certificación

Las políticas de certificación son las reglas, roles obligaciones y responsabilidades a las que están sometidos los usuarios ante la Autoridad de certificación desde la solicitud, administración y uso de los certificados.

Solicitud de certificado

Para ser solicitante y posteriormente acceder a la certificación digital el alumno deberá contar con los siguientes requisitos:

- Identificador único de estudiante otorgado por la Universidad de las Fuerzas Armadas ESPE, nombres completos y correo electrónico institucional.
- Llenar la solicitud que se encuentra en la aplicación web, con los datos mencionados.

Emisión de certificado

Cuando un estudiante desee un certificado digital se acoge al siguiente procedimiento:

- El alumno accede a la aplicación web y procede a registrar y subir en formato digital la información requerida.
- El responsable del registro verificará que la información este completa y sea adecuada, de no ser así se le solicita al alumno corregir o completar la información, de estar correcta y completa se le notificará vía correo electrónico para continuar con la identificación y emisión del certificado.
- El alumno debe presentarse portando su documento de identidad cédula o pasaporte ante la autoridad de registro de manera virtual.
- Una vez identificado el alumno la AR confrontará el documento de identificación y en caso de conformidad se procede a la emisión del certificado.

Aceptación del certificado

Al momento de la entrega y firma del contrato se acepta el certificado por parte del subscriptor.

El acto de aceptación deberá realizarse de forma obligatoria ante el encargado de la entidad suscriptora o la unidad de registro.

El alumno posee 48 horas para verificar que la información del certificado sea la adecuada a partir de su entrega.

En caso de que exista inconsistencia entre los datos del certificado y el de la entidad suscriptora deberá comunicarlo de forma inmediata para su anulación y a la emisión de un certificado correcto.

Transcurrido el período sin comunicación se entiende la aprobación del certificado y su contenido.

El alumno acepta el certificado y asume el contenido con las obligaciones que ello conlleva.

Revocación de certificado

La revocación de certificados para los estudiantes ocurre en una de las siguientes circunstancias:

- Solicitud del subscriptor de manera voluntaria.
- Pérdida de clave.
- Inutilización por daños en el soporte del certificado.
- Uso incorrecto e indebido del certificado.
- Deceso del suscriptor.
- Inexactitud de la información proporcionados por el estudiante.
- Error de emisión del certificado.
- Cuando las claves privadas del usuario están siendo comprometidas.
- Por el incumplimiento de la AR, o el suscriptor de las obligaciones establecidas.
- Por incumplimiento de la AR o el suscriptor de obligaciones determinadas.
- Por la salida o abandono de la universidad.

Suspensión de certificado

La suspensión de certificados electrónicos se ejecuta cuando:

- Pérdida de las claves o que las mismas estén comprometidas.
- Por pedido expreso del alumno.

El certificado suspendido será publicado en la lista de certificados revocados y permanecerá ahí hasta su cambio de estado, de no realizarse su activación permanecerá ahí indefinidamente.

Renovación de certificado

Cuando un certificado está a punto de caducar y el estudiante quiere seguir utilizando el mismo con las mismas características, se utiliza este procedimiento; en este caso, la entidad generará nuevas claves.

El tiempo vigente de los certificados es por el lapso de 4 años, posterior a ello se podrá realizar el trámite para su renovación cumpliendo con los siguientes requisitos:

- El alumno deberá realizar una solicitud en la cual consten sus datos personales actualizados y en la misma se detalle el requiriendo de la renovación.
- El alumno accede a la aplicación web, y debe llenar la información completa en el formulario de renovación de certificado, verificando que no exista errores en la información requerida, en caso de que esta no sea correcta se le solicitará al alumno realice una nueva solicitud, si la información es la correcta recibirá un correo electrónico para que se acerque con su documento de identidad hasta admisión y registro.
- El alumno deberá realizar la solicitud con anticipación de 30 días de concluida la vigencia de su certificado.
- No debe haber conocimiento de mal uso de certificado o de incurrir en causas de revocación o suspensión.
- La solicitud de renovación se refiere al mismo tipo emitido anteriormente y con la misma información.

- En la renovación el alumno puede cambiar sus datos excepto el nombre, número de documento de identidad y el tipo de contenedor del certificado de firma electrónica.

Política de Seguridad Lógica de la PKI

La infraestructura PKI mantiene todas las medidas de seguridad garantizando:

- Todos los accesos tanto físicos como lógicos a los sistemas y datos de la infraestructura y se encuentra restringido a personal autorizado
- El manejo, emisión y operación responsable de las claves y certificados.
- La administración del sistema de control de la infraestructura PKI que es accedido previo sistema de autenticación y desarrollado con todas las medidas de seguridad.
- La supervisión continua del correcto funcionamiento del hardware y software

Política de Seguridad Física de la PKI

La infraestructura de clave pública se encuentra ubicada en el departamento de ciencias de la computación con las debidas medidas de seguridad.

La entidad de registro se encuentra en una oficina adecuada específicamente para generar el servicio de manera adecuada, permanente y seguro. En los departamentos donde se encuentra la infraestructura PKI existe video vigilancia, monitoreo las 24 horas.

Todas las oficinas también cuentan con guardianía permanente y puertas con acceso biométrico.

Posee un generador eléctrico en caso de suspensión temporal del servicio de luz, garantizando el funcionamiento normal de los equipos.

Existe extintores de incendios en todos los pisos donde se encuentra la infraestructura PKI además detectores de humo y alarmas que dan alerta temprana al cuerpo de bomberos.

La información recolectada se guarda en servidores con respaldos seguros evitando mantener la información en un solo lugar.

Políticas de roles de certificación.

Existen roles establecidos para la operación y administración de la infraestructura PKI y que se detallan a continuación:

Administrador del sistema.

Es la persona encargada de instalar, operar y mantener el software y las bases de datos, además registra la entrada segura a la aplicación.

Operador del sistema.

Es responsable del funcionamiento del sistema, no tiene autorización para realizar la operación de restaurar de datos ni backups manuales, esta es potestad del administrador. Puede también generar manualmente las CLR y consultas de las CLR ya emitidas.

Operador de certificados

Es el responsable de la etapa de vida de los certificados emisión, renovación, revocación, suspensión y reactivación de estos.

Auditor

Es la persona autorizada de consultar los log o archivos para mantener los registros de auditoria del sistema.

Capacitación y entrenamiento

Todo el personal relacionado a la infraestructura PKI adicional al conocimiento de las políticas y normas para el funcionamiento de esta certificación, también cuenta con conocimiento en áreas como:

Seguridad de la información.

Seguridad física en caso de desastres naturales y diversas eventualidades se regirán a lo establecido en los planes de contingencia vigentes para los diferentes departamentos de la universidad de las Fuerzas Armadas “ESPE”.

Procedimientos de certificación

El desarrollo de certificación especifica los pasos que el alumno debe realizar para solicitar cualquiera de los servicios de certificación electrónica los cuales se desglosan y se de tallan a continuación.

Solicitud de certificado

Cuando un estudiante desee un certificado electrónico se acoge al siguiente procedimiento:

Llenará la solicitud que se encuentra en la aplicación web y enviarlo con la información requerida.

Emisión de certificado

Cuando un estudiante desee un certificado electrónico se acoge al siguiente procedimiento:

- El alumno accede a la aplicación web y procede a llenar la solicitud, registrar y subir en formato digital la información requerida.
- El encargado del registro verificará que la información este completa y sea adecuada, de no ser así se le solicita al alumno corregir o completar la información, de estar correcta y completa se le notificará vía correo electrónico para continuar con la identificación y emisión del certificado.
- El alumno debe presentarse junto a su documento de identidad cédula o pasaporte ante la autoridad de registro.
- Al ser identificado el alumno la AR comparará el documento de identificación y en caso de conformidad procederá a la emisión del certificado

Revocación de certificado

Se realizará el siguiente proceso para la revocación del certificado:

Se realizará la solicitud correspondiente la misma que se encuentra en la aplicación web sección firma electrónica, exponiendo la causa por la que desea revocar el certificado electrónico. La decisión de anular el certificado será anunciada al alumno por medio de correo electrónico. Todos los certificados revocados estarán disponibles en la CLR la misma que se actualizará cada vez que exista un certificado revocado.

Suspensión de certificado

Se realizará el siguiente proceso para la suspensión del certificado:

Se realizará la solicitud correspondiente la misma que se encuentra en la aplicación web sección firma electrónica, exponiendo la causa por la que desea suspender el certificado electrónico.

Renovación de certificado

El procedimiento para la renovación de un certificado electrónico es el siguiente:

- Completar la solicitud que se encuentra en la aplicación web sección firma electrónica. Enviar la solicitud y todos los documentos habilitantes en formato electrónico. La autoridad de registro será la responsable de verificar la información y la solicitud de renovación. En caso de que esta no sea correcta se le solicitara al alumno su corrección o completamiento, en caso de que la información haya sido completada sin ningún inconveniente se aceptará la solicitud. Se da aviso mediante un correo electrónico para que el alumno se acerque a retirar el certificado electrónico.
- El alumno debe presentarse con su documento de identidad cédula o pasaporte ante la autoridad de registro.
- Identificado el alumno la AR confrontará el documento de identificación y en caso de conformidad procederá a la emisión del certificado.

Gestión Técnica

Diseño de la capacidad de Servicio

La aplicación web podrá gestionar todo el ciclo de vida de un certificado digital y será capaz de soportar todas las políticas y procedimientos definidos en la sección de Gestión de Servicios. Asimismo, deberá contar con la capacidad de definir roles basados en las políticas y procedimientos definidos en la sección de Gestión de Servicios, los cuales son:

- Autoridad de Certificación
- Autoridad de Registro
- Auditor

- Entidad Final

La Universidad de las Fuerzas Armadas ESPE mediante la Unidad de Tecnologías de la Información cuenta con diferentes áreas que podrán dar el soporte adecuado para satisfacer los roles requeridos por la aplicación web.

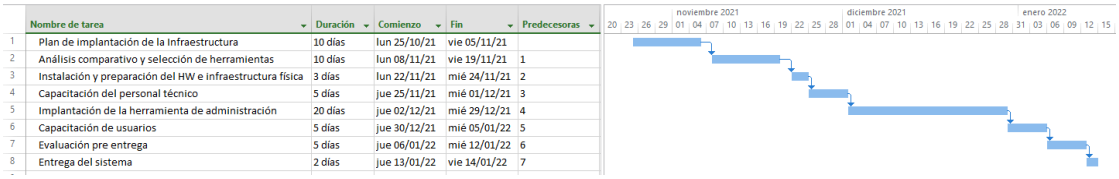
Capítulo IV

Implementación de la infraestructura

Se ha definido las tareas mediante un cronograma que abarca todas las actividades de la fase de entrega y transición del servicio.

Figura 6

cronograma de actividades



	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	Plan de implantación de la Infraestructura	10 días	lun 25/10/21	vie 05/11/21	
2	Análisis comparativo y selección de herramientas	10 días	lun 08/11/21	vie 19/11/21	1
3	Instalación y preparación del HW e infraestructura física	3 días	lun 22/11/21	mié 24/11/21	2
4	Capacitación del personal técnico	5 días	jue 25/11/21	mié 01/12/21	3
5	Implantación de la herramienta de administración	20 días	jue 02/12/21	mié 29/12/21	4
6	Capacitación de usuarios	5 días	jue 30/12/21	mié 05/01/22	5
7	Evaluación pre entrega	5 días	jue 06/01/22	mié 12/01/22	6
8	Entrega del sistema	2 días	jue 13/01/22	vie 14/01/22	7

Desarrollo del plan de implementación

A continuación, se detalla cada una de las tareas.

Tabla 2

Plan de implantación de la Infraestructura

ID	1.1
Actividad	Plan de implantación de la Infraestructura
Duración	10 días
Recursos	2 personas
Descripción	Definir las actividades a realizar y plantear un tiempo adecuado para cada una. Realizar un cronograma de actividades con el tiempo planteado.
Requiere	-

Tabla 3

Análisis comparativo y selección de herramientas

ID	1.2
Actividad	Análisis comparativo y selección de herramientas
Duración	10 días
Recursos	2 personas
Descripción	Analizar las herramientas de PKI basadas en software libre. Seleccionar la herramienta adecuada para su posterior implementación en la ESPE.
Requiere	-

Tabla 4

Instalación y preparación del hardware e infraestructura física

ID	1.3
Actividad	Instalación y preparación del hardware e infraestructura física
Duración	3 días
Recursos	2 personas
Descripción	Solicitar la infraestructura a la UTICs de la Universidad de las Fuerzas Armadas ESPE.
Requiere	-

Tabla 5

Capacitación del personal técnico

ID	1.4
Actividad	Capacitación del personal técnico
Duración	3 días
Recursos	2 personas
Descripción	Capacitar al personal técnico sobre la herramienta a usar tanto a nivel de hardware como software.
Requiere	1.3

Tabla 6

Implantación de la herramienta de administración

ID	1.5
Actividad	Implantación de la herramienta de administración
Duración	20 días
Recursos	2 personas
Descripción	Configuración, despliegue e instalación de la herramienta de PKI seleccionada, la cual gestiona el ciclo de vida de los certificados digitales.
Requiere	1.2, 1.3

Tabla 7

Capacitación de usuarios

ID	1.6
Actividad	Capacitación de usuarios

Duración	5 días
Recursos	2 personas
Descripción	Capacitar a los usuarios finales de la aplicación web para el adecuado uso de la herramienta de administración del periodo de vida de certificados digitales. Crear un manual de usuario donde se especifique paso a paso como usar la herramienta.
Requiere	1.5

Tabla 8

Capacitación de usuarios

ID	1.7
Actividad	Evaluación pre entrega
Duración	5 días
Recursos	2 personas
Descripción	Evaluar la aplicación web mediante pruebas para garantizar su adecuado funcionamiento de la administración del periodo de vida de certificados digitales.
Requiere	1.5

Tabla 9

Entrega del sistema

ID	1.8

Actividad	Entrega del sistema
Duración	2 días
Recursos	2 personas
Descripción	Hacer entrega del aplicativo web que gestiona el ciclo de vida de certificados digitales a la Unidad de tecnologías de la información y Comunicación de la universidad.
Requiere	1.7

Análisis comparativo y selección de la herramienta

El punto más crucial es la identificación adecuada del software o herramienta que gestione certificados, que posea las funcionalidades y características acorde a los requerimientos establecidos, por lo que se han visto varias opciones de herramientas, entre las principales las de código abierto y libre, para que de este modo pueda adaptarse a la normativa requerida (Villalba, 2014).

Para el análisis de estas aplicaciones se utilizan criterios de estandarización RFC 3647 que especifica facilidades de mantenimiento, escalabilidad y soporte. En cuanto a la solución de la implementación de una entidad de certificación digital existe una variedad de aplicaciones en temas de PKI. A continuación se hace un cuadro comparativo de las más relevantes, se valora el software de acuerdo a secciones y subsecciones donde SI significa que Soporta, NO significa que no soporta y FI significa que falta información:

Tabla 10

Análisis y comparación de software PKI

Sección	Subsección	Software		
		XCA	EJBCA	OPENCA
Introducción	Nombre e identificación del proyecto	SI	SI	SI
	Entidades de certificación	SI	SI	SI
	Uso del certificado	SI	SI	SI
Responsabilidades de publicación y repositorio	Identificación de la entidad	NO	SI	SI
	Responsabilidad sobre la publicación de la información	FI	SI	SI
	Tiempo y frecuencia de publicación de la información	FI	SI	SI
	Controles de acceso a los repositorios	NO	SI	SI
Identificación y autenticación	Tipos de nombres asignados	SI	SI	SI
	Validación de identidad inicial	SI	SI	SI
	Identificación y autenticación para solicitud de renovación de claves	NO	SI	SI
	Identificación y autenticación para solicitud de renovación	NO	SI	SI
	Aprobación o rechazo de la solicitud de un certificado	NO	SI	SI
	Tiempo para el procesamiento de una solicitud de certificado	SI	SI	SI
Requisitos operacionales del ciclo de vida del certificado	Acciones de la EC durante la emisión del certificado	NO	SI	SI
	Notificación al suscriptor por parte de la EC respecto de la emisión de un certificado	NO	FI	SI
	Conducta constitutiva de la aceptación de un certificado	NO	FI	SI
	Publicación del certificado	NO	SI	SI
	Modificación de certificado	NO	SI	NO
	Notificar al suscriptor sobre la emisión de un nuevo certificado	NO	FI	FI
	Procedimientos para la solicitud de renovación	NO	SI	SI
	Frecuencia de emisión de CLR	NO	SI	SI
	Disponibilidad en línea de la renovación	NO	SI	SI
	Rasgos operacionales	NO	SI	SI
	Política de recuperación y depósito de claves	NO	SI	SI
	Políticas y prácticas para la encapsulación de claves de sesión	NO	SI	SI
Controles operativos de	Procedimiento de registro de auditoría	NO	SI	SI
	Controles de procedimientos	NO	SI	SI

gestión e instalaciones	Controles de personal	NO	SI	SI
	Frecuencia de procesamiento de registro	NO	SI	SI
Controles técnicos de seguridad	Generación e instalación de par de claves	NO	SI	SI
	Protección de clave privada y criptográfica	NO	SI	SI
	Controles de seguridad del ciclo de vida	NO	SI	NO
Perfiles de certificado CRL y OCSP	Perfil de certificado	SI	SI	SI
	Número de versión	SI	SI	FI
	Extensión de certificado	FI	SI	SI
	Identificadores de objeto de algoritmo	FI	SI	SI
	Forma de nombres	FI	SI	SI
	Restricciones de nombres	FI	SI	SI
	Identificador de objeto de la política de certificado	FI	SI	SI
	Extensión de restricciones de uso de la política	FI	SI	SI
	Sintaxis y semántica de los calificadores de la política	FI	SI	SI
	Perfil de CR	FI	SI	SI
	Número de versión	FI	SI	SI
	CRL y extensiones de entrada CRL	FI	SI	SI
	Perfil OCSP	FI	SI	SI
	Numero de versión	FI	SI	SI
	Extensiones OCSP	FI	SI	SI

Nota. Elaboración propia

Una vez realizado el cuadro comparativo, se puede establecer que tanto las herramientas de EJBCA como de OPENCA son las más completas actualmente, debido a que poseen características similares, por lo que se decide elegir la herramienta de software libre EJBCA por contar con más características a las que da soporte.

Capacitación del personal técnico

Para la capacitación al personal técnico se ha elaborado manuales que contienen los temas de configuración, personalización, despliegue, instalación y configuración de operaciones de la herramienta EJBCA, dichos temas se los puede ubicar en la sección de Implantación de la herramienta de administración.

Instalación y preparación del hardware e infraestructura física

Toda lo concerniente a hardware e infraestructura física son proporcionados por la Universidad de las Fuerzas Armadas ESPE mediante la Unidad de Tecnologías de la Información y Comunicación quien brinda soporte tanto en la etapa de desarrollo y pruebas como en la etapa productiva.

Implantación de la herramienta de administración.

En esta sección se encuentra especificado a detalle el proceso de instalación de la herramienta EJBCA, así también, todos los procesos necesarios para el correcto y adecuado funcionamiento de la PKI.

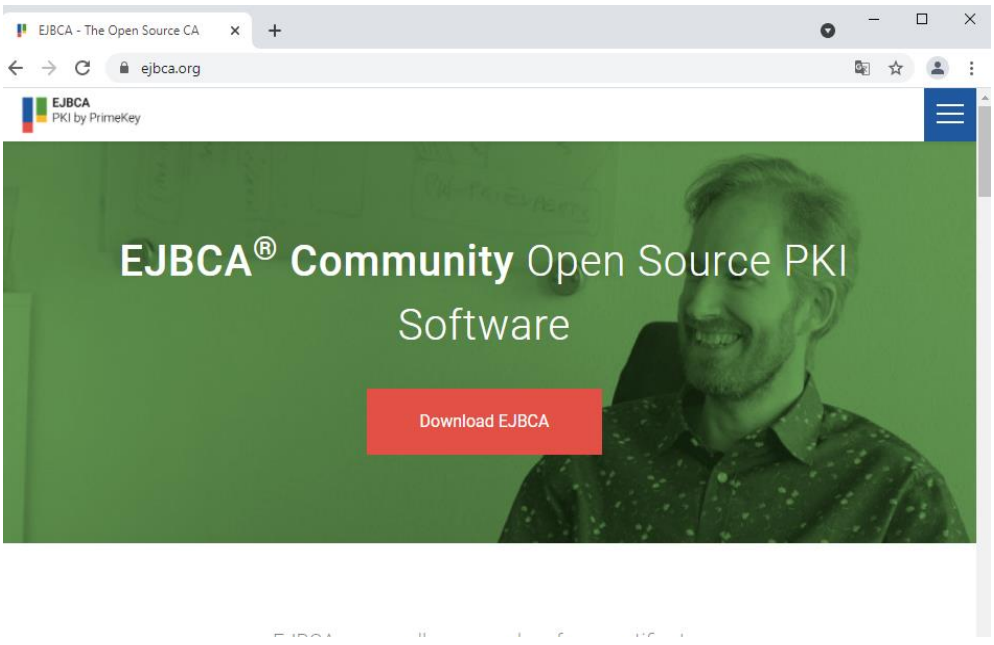
INSTALACIÓN EJBCA

1. Descargar EJBCA

    1.1. Se ingresa al sitio web y presionar en download EJBCA.

Figura 7

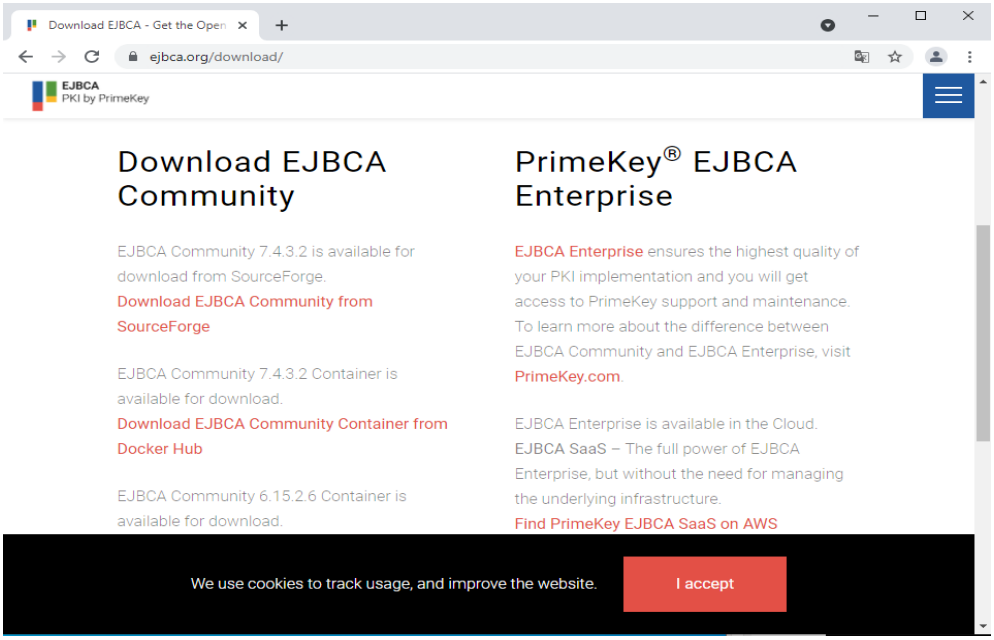
sitio web



1.2. Se escoge versión comunitaria.

Figura 8

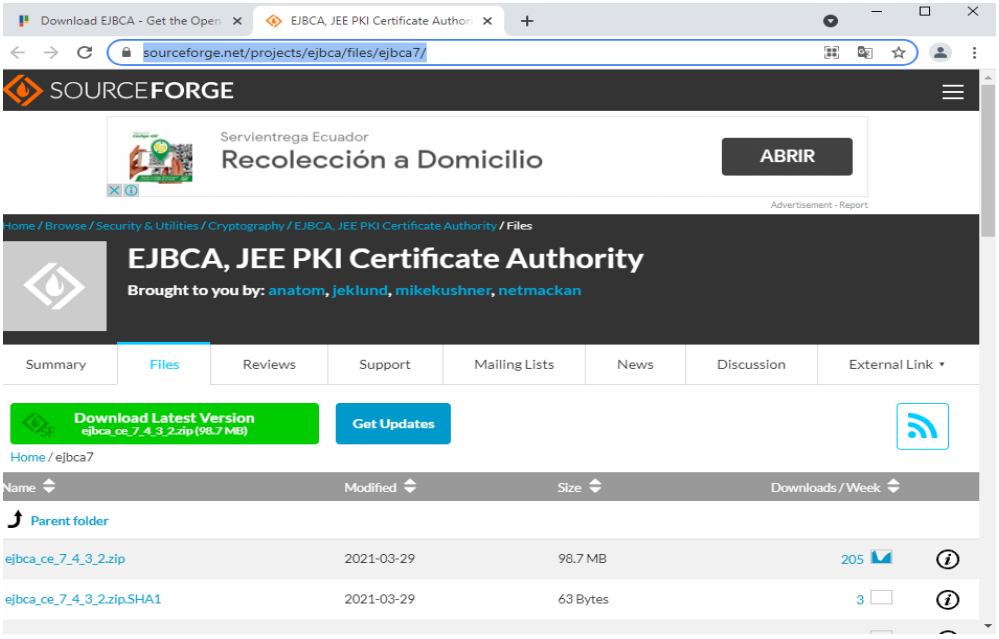
versión



1.3. Automáticamente redirige al enlace de descarga.

Figura 9

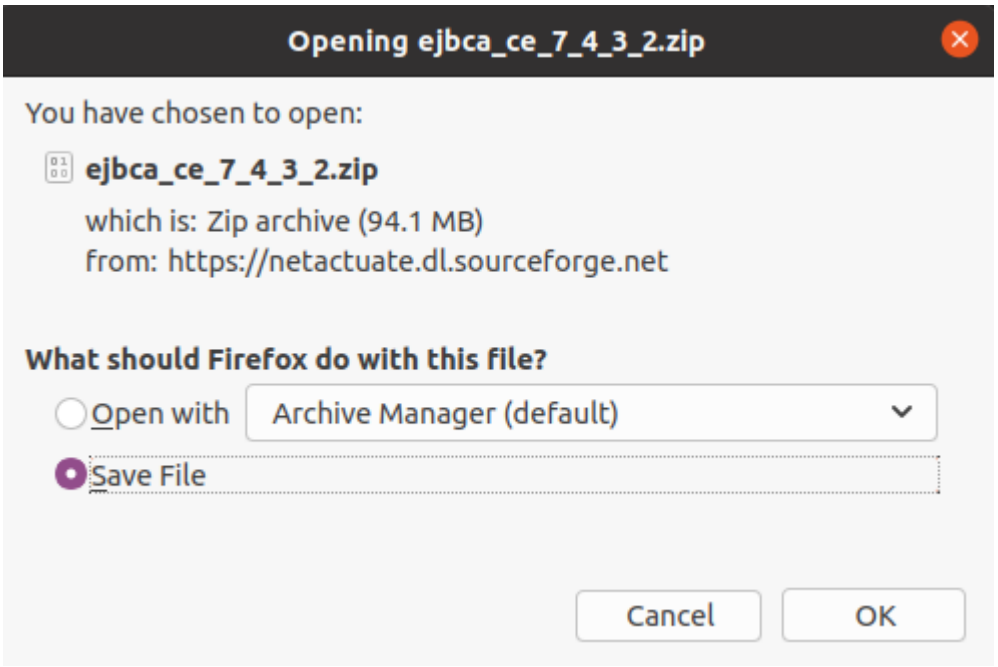
enlace de descarga



1.4. Se guarda la descarga.

Figura 10

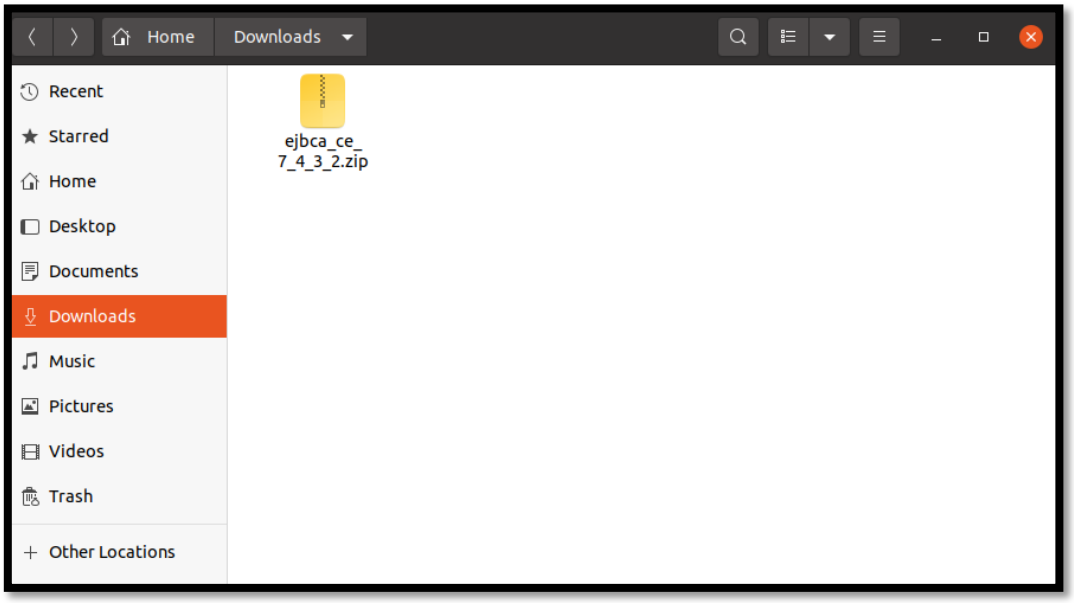
confirmar de descarga



1.5. Por defecto el archivo comprimido que contiene la aplicación de EJBCA se guarda en la carpeta descargas.

Figura 11

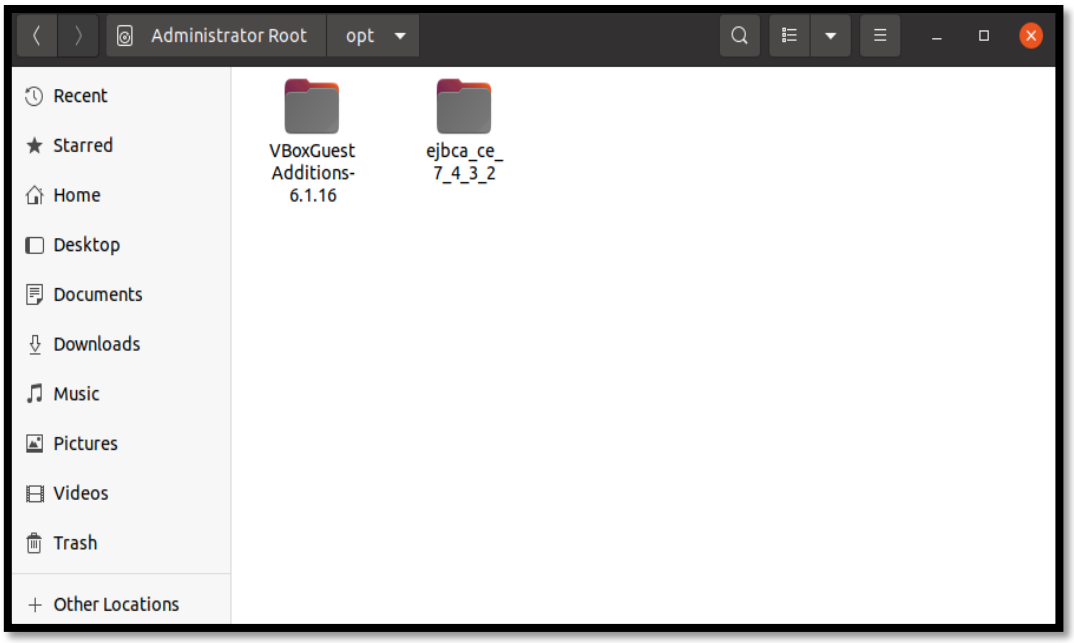
aplicación EJBCA



1.6. Se procede a descomprimir en una carpeta a escoger para este caso en la carpeta /opt.

Figura 12

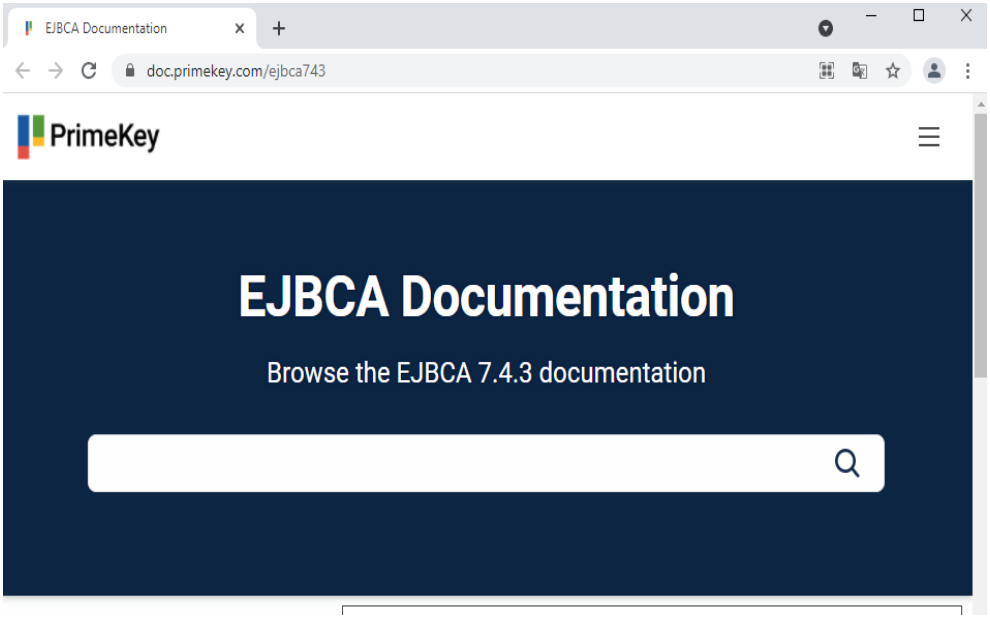
directorio /opt



1.7. Para los siguientes pasos se puede revisar la documentación en **https://doc.primekey.com/ejbca743**.

Figura 13

documentación



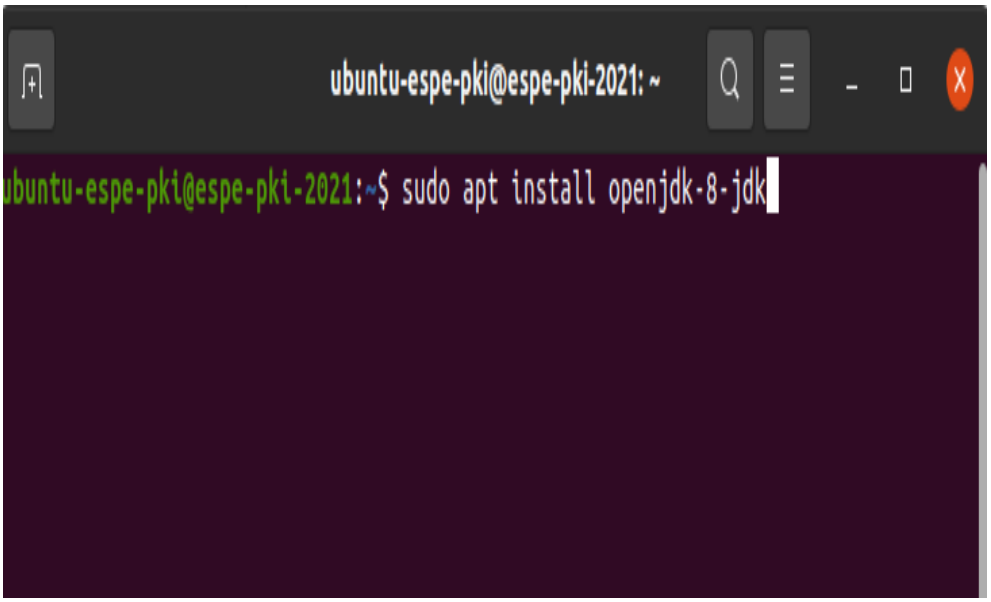
2. Prerrequisitos.

2.1. Instalar java 8.

2.1.1. Se ingresa el comando para instalar java 8.

Figura 14

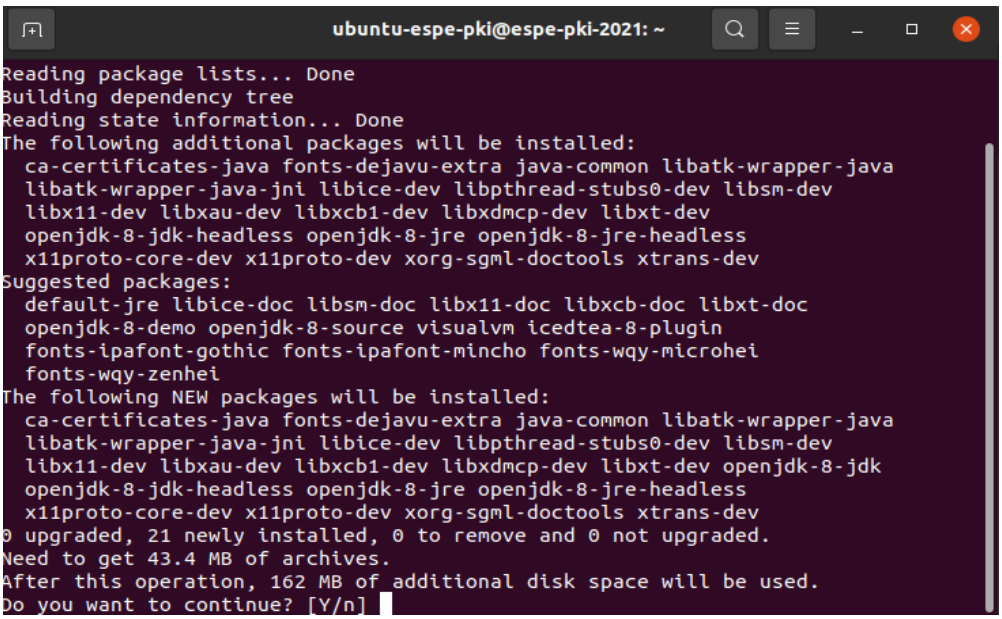
comando de instalación



2.1.2. Se acepta la condición para instalar los paquetes.

Figura 15

condición de instalación



2.1.3. Se verifica que se haya instalado correctamente la versión.

Figura 16

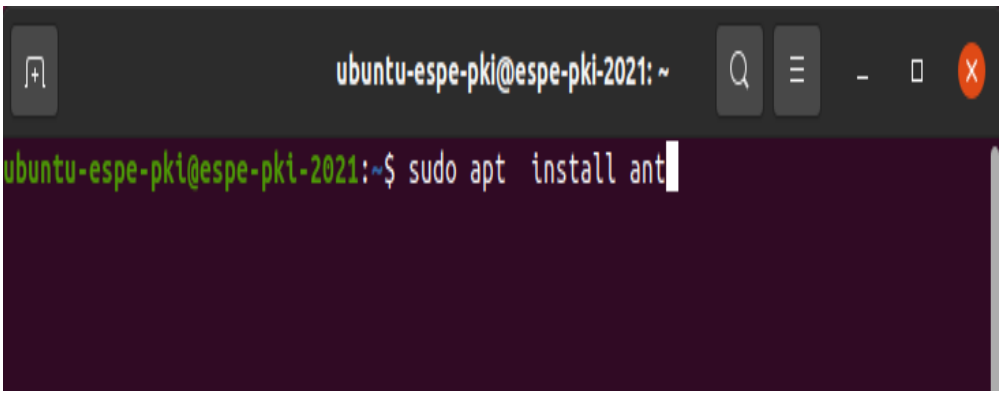
verificación de versión

2.2. Instalar Apache Ant versión 1.8 o posterior

2.2.1. Se ingresa el comando para instalar apache ant.

Figura 17

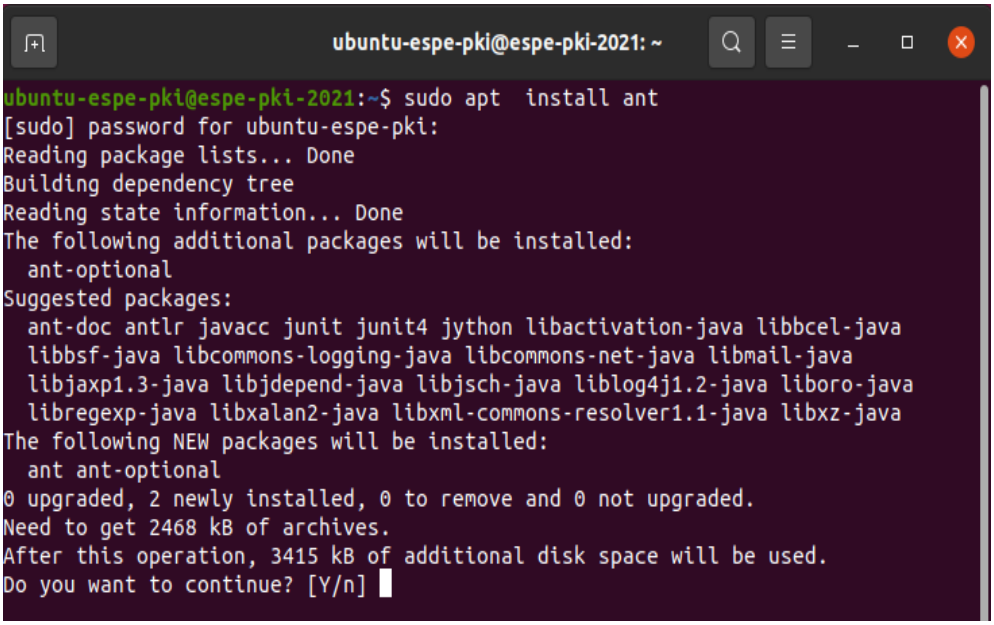
comando para instalar apache



2.2.2. Se acepta la condición para instalar los paquetes.

Figura 18

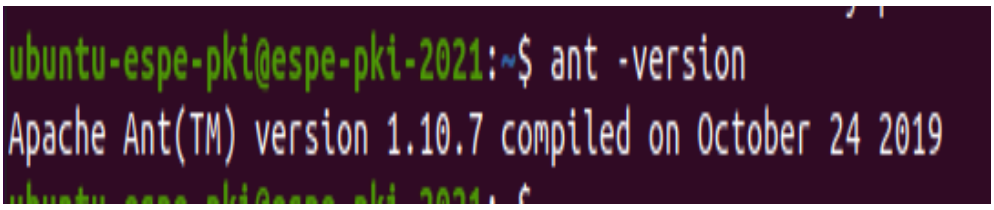
condición de instalación



2.2.3. Se verifica que se haya instalado correctamente la versión.

Figura 19

verificación de versión

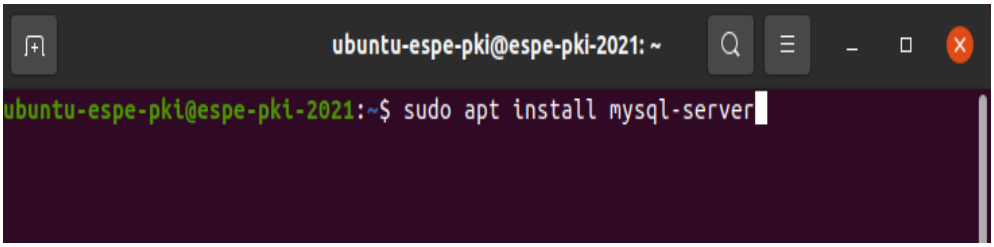


2.3. Instalar el servidor de base de datos, en este caso mysql.

2.3.1. Se ingresa el comando para instalar mysql server.

Figura 20

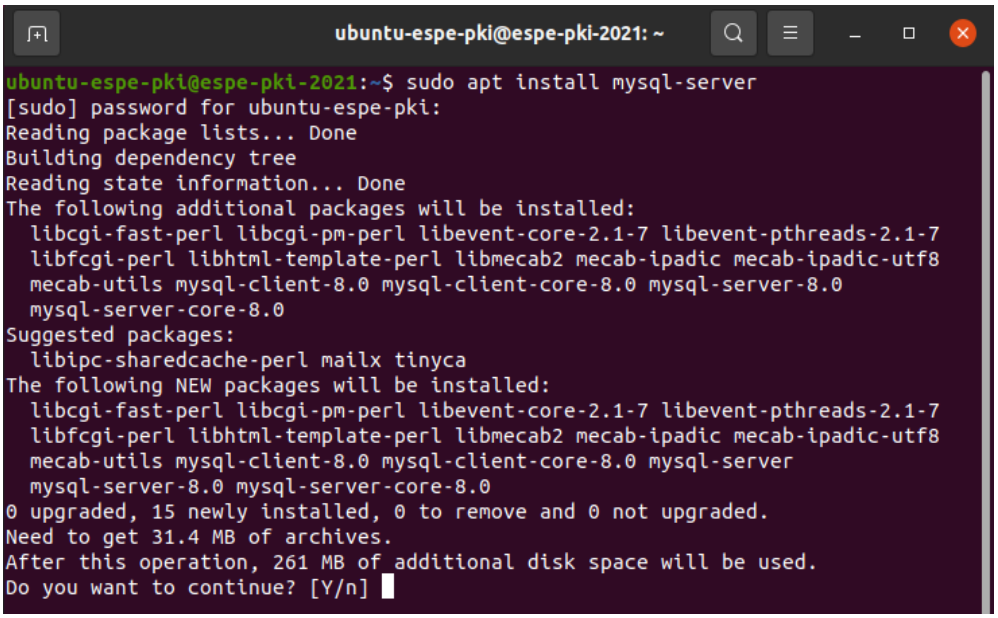
comando mysql



2.3.2. Se acepta la condición para instalar los paquetes.

Figura 21

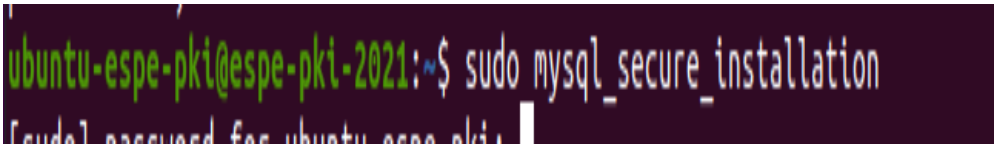
condición para instalar paquetes



2.3.3. Se ejecuta el comando para realizar la configuración de seguridad de mysql.

Figura 22

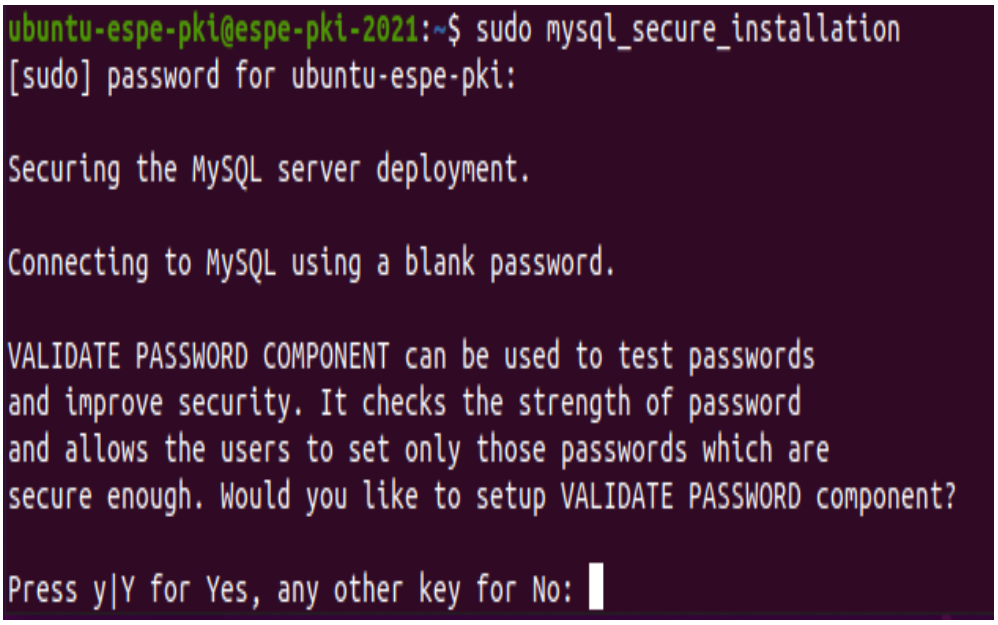
seguridad de mysql



2.3.4. Se acepta la confirmación para validar la contraseña.

Figura 23

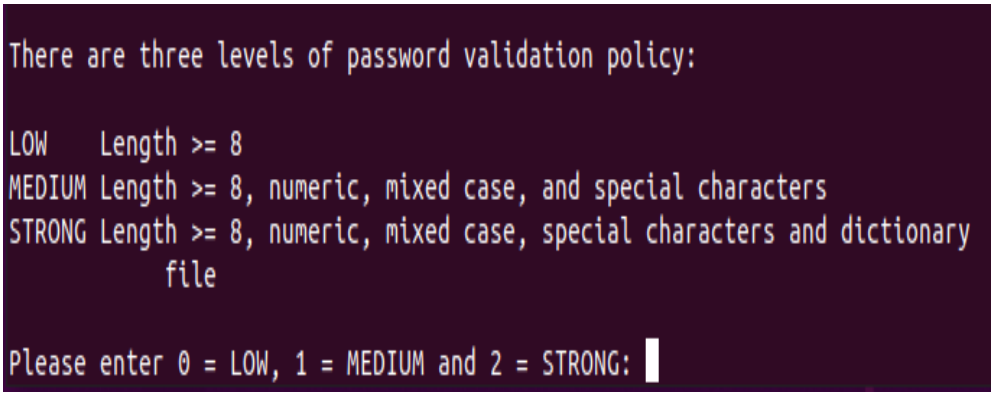
confirmación para validar la contraseña



2.3.5. Se selecciona el nivel de seguridad de la contraseña.

Figura 24

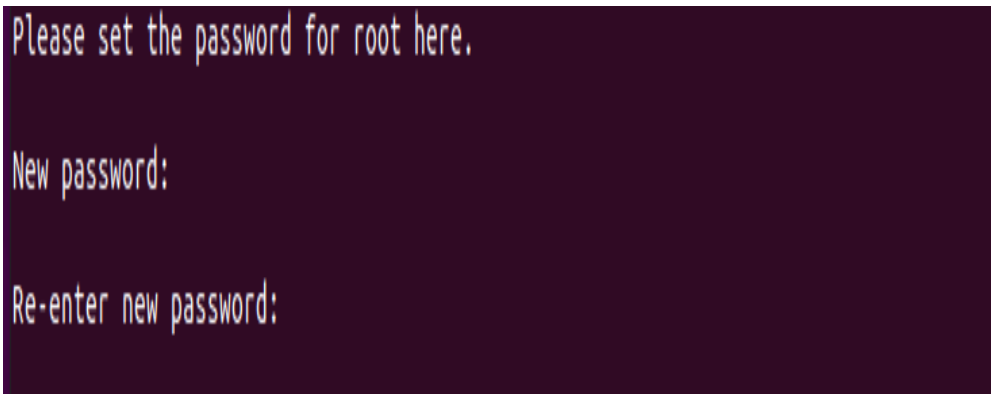
seguridad de la contraseña



2.3.6. Se ingresa la contraseña del usuario root (PassM4r1a*2021).

Figura 25

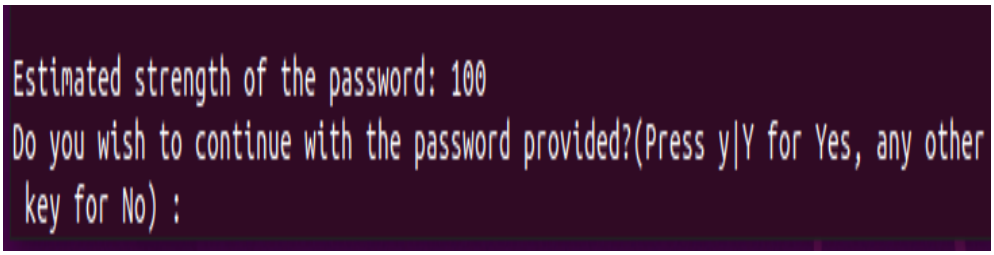
contraseña del usuario root



2.3.7. Se acepta la pregunta de confirmación para continuar.

Figura 26

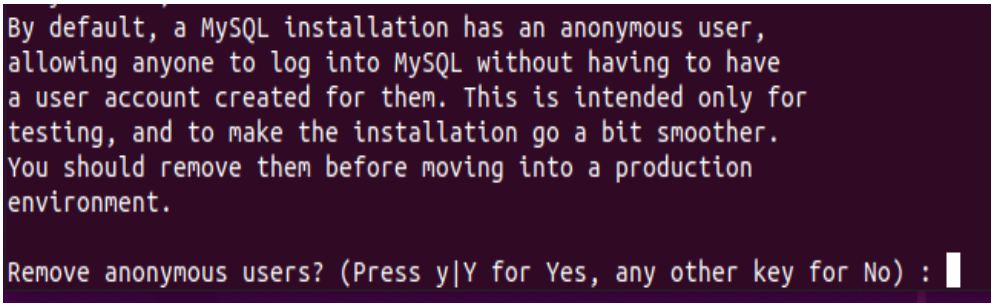
pregunta de confirmación para continuar



2.3.8. Se acepta la pregunta de eliminar el usuario anónimo.

Figura 27

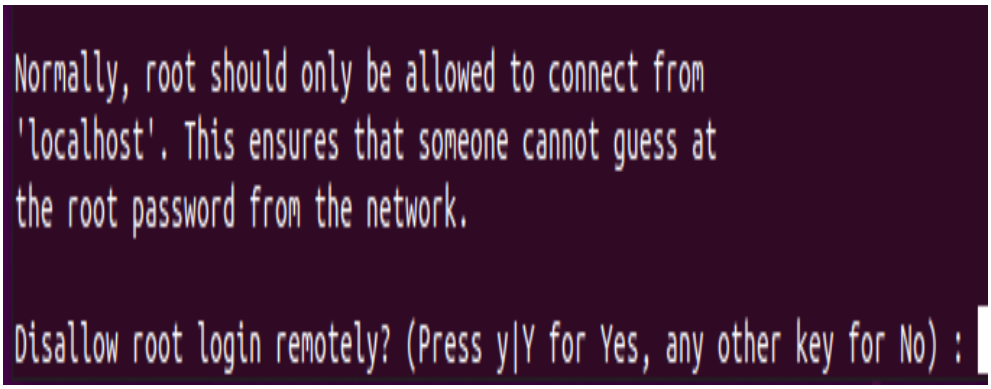
pregunta de eliminar el usuario



2.3.9. Se acepta la pregunta para desactivar el usuario root remotamente.

Figura 28

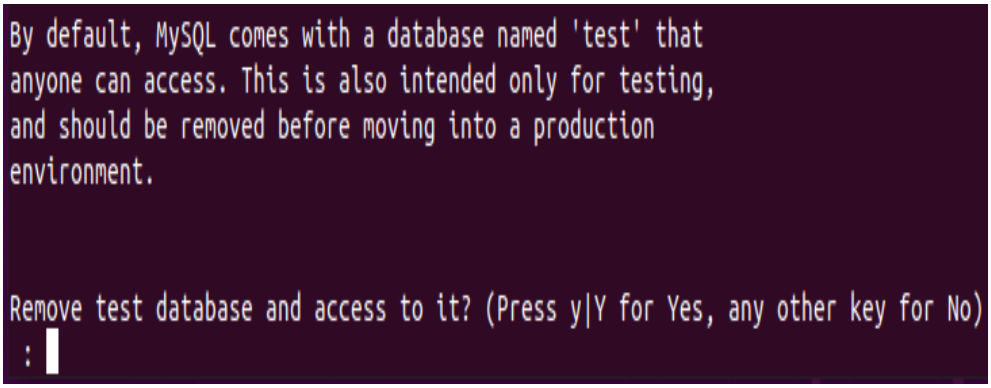
desactivar el usuario root



2.3.10. Se acepta la pregunta para borrar la base de datos de prueba que viene por defecto con la instalación de mysql.

Figura 29

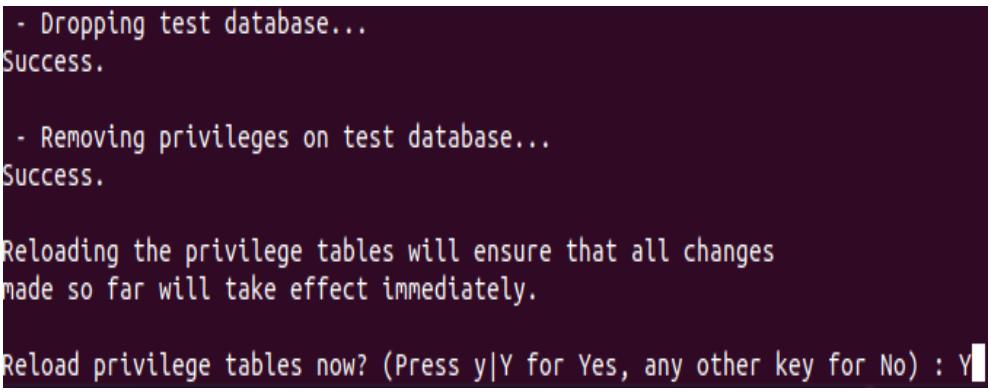
base de datos de prueba



2.3.11. Se acepta la pregunta para recargar privilegios sobre las tablas.

Figura 30

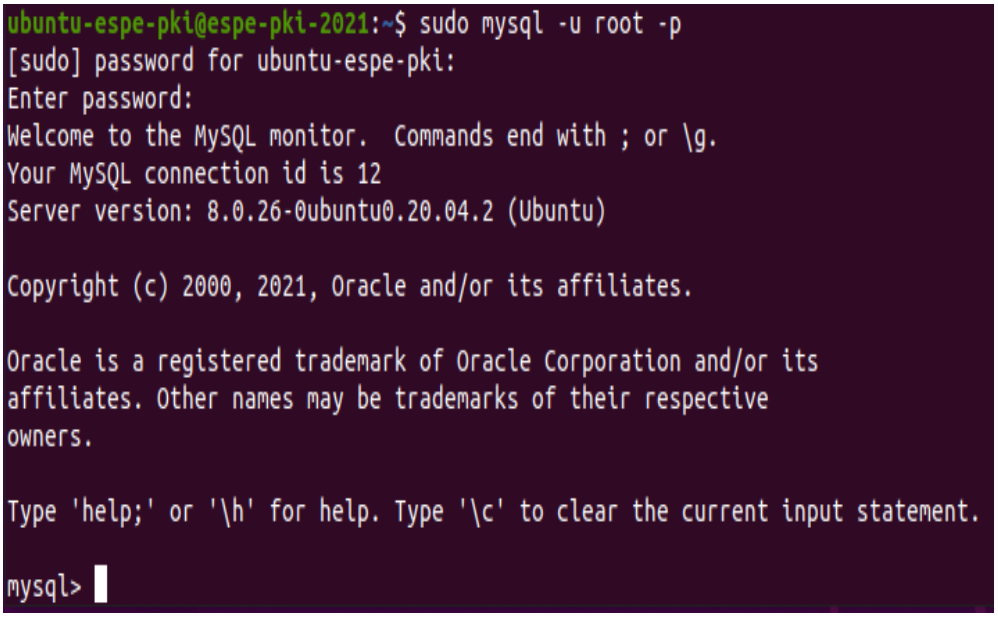
pregunta para recargar privilegios



2.3.12. Se comprueba el acceso del usuario root.

Figura 31

el acceso del usuario root

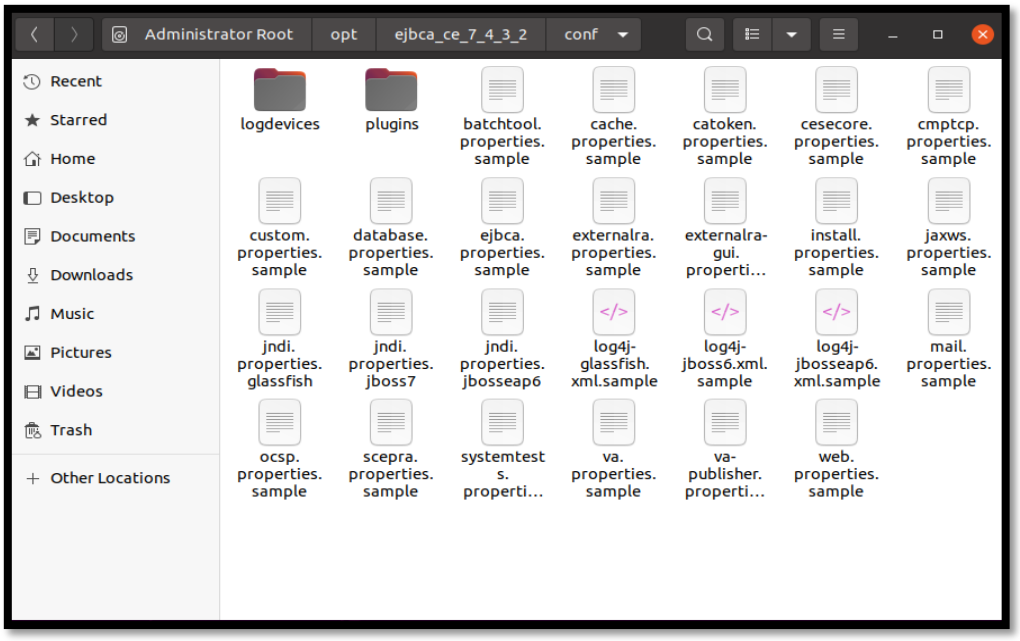


3. Configuración de EJBCA

3.1. Se ingresa al directorio conf de la carpeta donde se encuentra EJBCA.

Figura 32

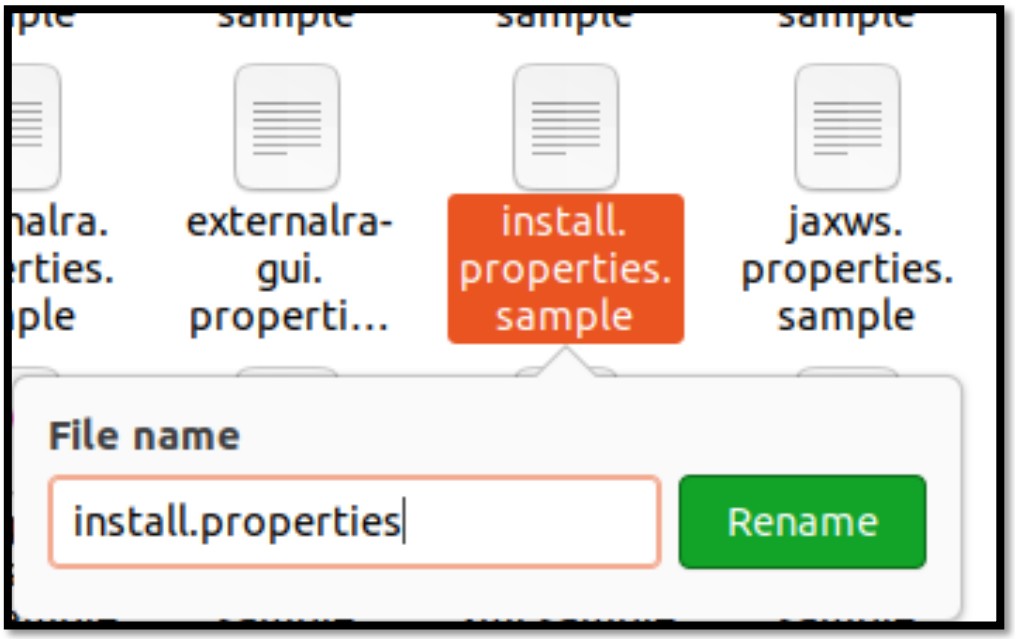
directorio conf



3.2. Se renombra el archivo install.properties.sample a install.properties.

Figura 33

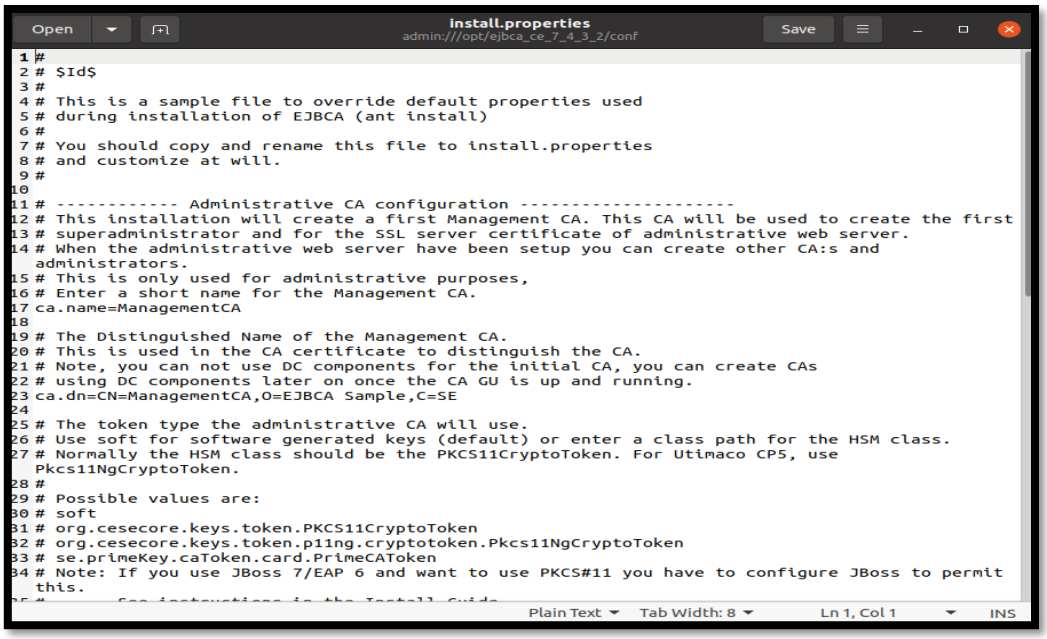
archivo install.properties



3.3. Se abre el archivo para editar el nombre de la CA que viene por defecto.

Figura 34

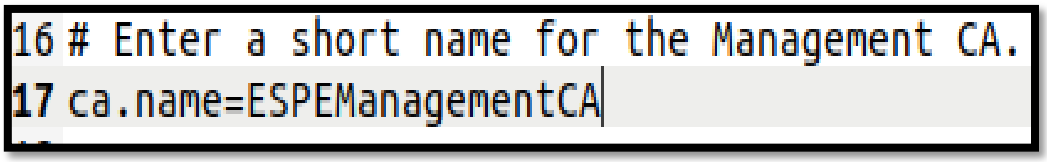
nombre de la CA



3.3.1. Se cambia el nombre de la CA de gestión.

Figura 35

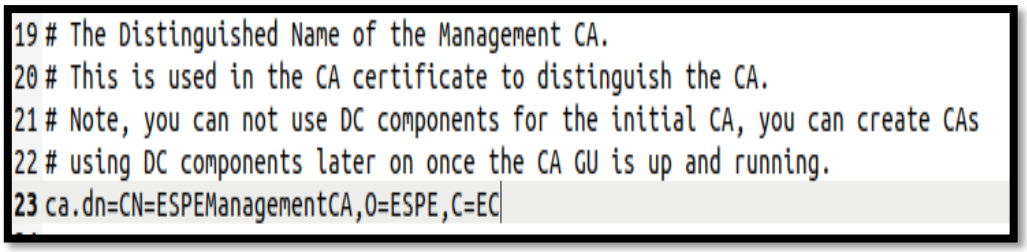
nombre de la CA de gestión



3.3.2. Se cambia el nombre de distinción de la CA de gestión.

Figura 36

distinción de la CA de gestión



3.4. Se renombra el archivo cesecore.properties.sample a cesecore.properties.

Figura 37

archivo cesecore.properties

3.5. Se renombra el archivo ejbca.properties.sample a ejbca.properties.

Figura 38

archivo ejbca.properties

3.6. Se renombra el archivo web.properties.sample a web.properties y se lo abre para su configuración.

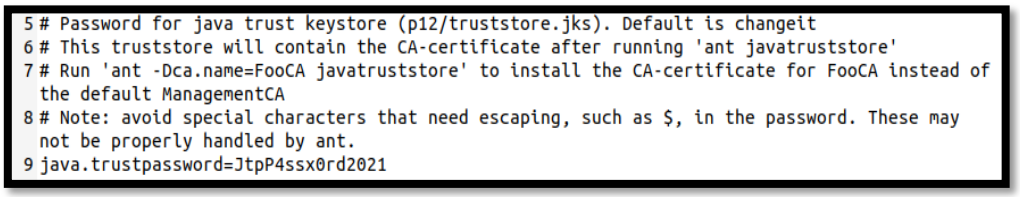
Figura 39

archivo web.properties

3.6.1. Se cambia la contraseña para el almacén de claves de confianza de Java (JtpP4ssx0rd2021).

Figura 40

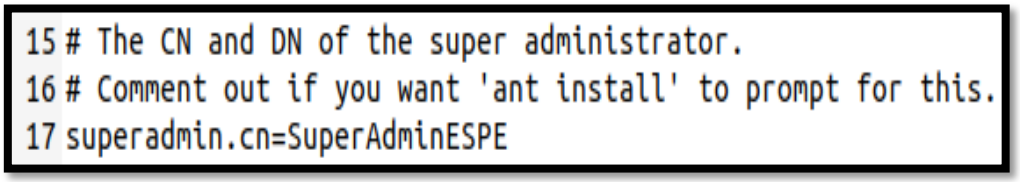
contraseña para el almacén de claves de confianza



3.6.2. Se cambia el nombre del super admin.

Figura 41

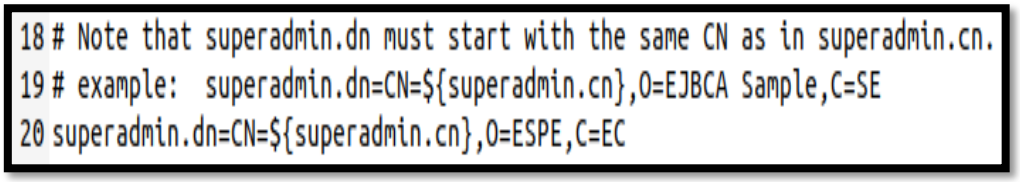
nombre del super admin



3.6.3. Se cambia el nombre de distinción del super admin.

Figura 42

nombre de distinción del super admin



3.6.4. Se cambia la contraseña de super admin (ejbcaSAEP4ssx0rd1922).

Figura 43

contraseña de super admin

```
30 # The password used to protect the generated super administrator P12 keystore (to be imported
   in browser).
31 # Choose a good password here.
32 superadmin.password=ejbcaSAEP4ssx0rd1922
```

3.6.5. Se cambia la contraseña para el almacén de claves del servidor de aplicaciones (serverKSP4ssx0rd2021).

Figura 44

contraseña para el almacén de claves

```
38 # The password used to protect the web server's SSL keystore. Default is serverpwd
39 # Choose a good password here.
40 # If upgrading from EJBCA 3.1, enter here the password found in
41 #   $JBOSS_HOME/server/default/deploy/jbossweb-tomcat55.sar/server.xml
42 #   under the section about 'HTTPS Connector...', the password is in attribute
   'keystorePass=...'.
43 httpsserver.password=serverKSP4ssx0rd2021
```

3.6.6. Se cambia el nombre de host de esta instancia.

Figura 45

nombre de host

```
45 # The CA servers DNS host name, must exist on client using the admin GUI.
46 # Or using IPv6 IP: [::1] or::1
47 httpsserver.hostname=localhost
```

3.6.7. Se cambia el nombre de distinción del sujeto del certificado TLS utilizado por la interfaz de usuario de EJBCA.

Figura 46

nombre de distinción del sujeto

```
49 # The Distinguished Name of the SSL server certificate used by the administrative web GUI.
50 # The CN part should match your host's DNS name to avoid browser warnings.
51 httpsserver.dn=CN=${httpsserver.hostname},O=ESPE,C=EC
```

3.7. Se renombra el archivo database.properties.sample a database.properties y se lo abre para su configuración.

Figura 47

archivo database.properties

3.7.1. Se cambia el nombre de la fuente de datos de la base de datos EJBCA.

Figura 48

nombre de la fuente de datos

```
5 # JNDI name of the DataSource used for EJBCA's database access. The prefix
6 # (e.g. 'java:/', '' or 'jdbc/')is automatically determined for each
7 # application server.
8 # default: EjbcaDS
9 datasource.jndi-name=EspeEjbcaDS
```

3.7.2. Se modifica el nombre de la base de datos que se está utilizando.

Figura 49

nombre de la base de datos

```
16 # The database name selected for deployment, used to copy XDoclet merge files.
17 # All supported databases are defined below, others can easily be added
18 # See the document doc/howto/HOWTO-database.txt for database specifics and tips and tricks.
19 # (Note that the names below are fixed for the database type, it is not the name of your
   database instance.)
20 # Default: h2
21 # For MariaDB, use "mysql"
22 database.name=mysql
```

3.7.3. Se modifica la URL de la base de datos.

Figura 50

URL de la base de datos

```
37 # Database connection URL.
38 # This is the URL used to connect to the database, used to configure a new datasource in JBoss.
39 # Default: jdbc:h2:~/ejbcadb;DB_CLOSE_DELAY=-1
40 database.url=jdbc:mysql://127.0.0.1:3306/ejbca
```

3.7.4. Se modifica el nombre del controlador de la base de datos.

Figura 51

nombre del controlador de la base de datos

```
52 # JDBC driver classname.
53 # The JEE server needs to be configured with the appropriate JDBC driver for the selected
   database
54 # The Default h2 works (as test database) on JBoss 7, on JBoss 5 use org.hsqldb.jdbcDriver
55 # Default: h2
56 database.driver=org.mariadb.jdbc.Driver
57 #database.driver=com.mysql.jdbc.Driver
```

3.7.5. Se cambia el nombre de usuario establecido para la base de datos EJBCA.

Figura 52

usuario EJBCA

```
68 # Database username.
69 # Default: sa (works with H2 on JBoss 7)
70 database.username=ejbca
```

3.7.6. Se cambia la contraseña del usuario establecido para la base de datos EJBCA.

Figura 53

contraseña usuario EJBCA

```
72 # Database password.
73 # Default: sa (works with H2 on JBoss 7)
74 database.password=MYejbcaPassM4r1a*2021
```

4. Configuración de la base de datos.

4.1. Se conecta a la base de datos.

Figura 54

conexión base de datos

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo mysql -u root -p
[sudo] password for ubuntu-espe-pki:
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.26-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

4.2. Se ejecuta la instrucción para hacer la base de datos EJBCA.

```
mysql> CREATE DATABASE ejbca CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
```

4.3. Se crea el usuario para la base de datos con su contraseña (MYejbcaPassM4r1a*2021).

```
mysql> CREATE USER 'ejbca'@'localhost' IDENTIFIED BY 'MYejbcaPassM4r1a*2021';
```

4.4. Se concede los privilegios para el usuario creado.

```
mysql> GRANT ALL PRIVILEGES ON ejbca.* TO 'ejbca'@'localhost';
```

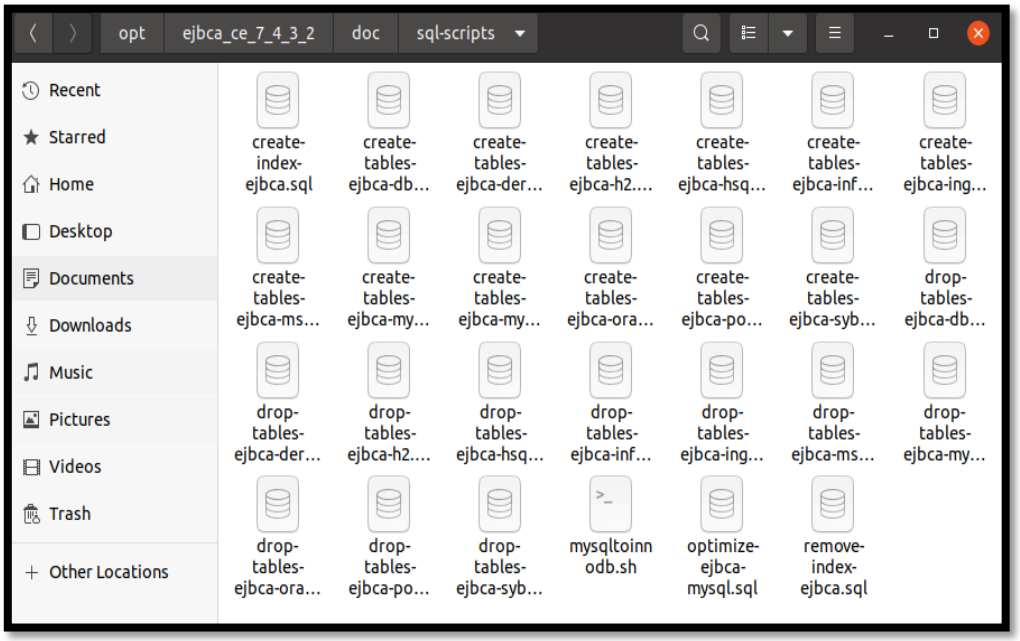
4.5. Se ejecuta el comando para usar la base de datos creada.

```
mysql> use ejbca;
```

4.6. Se ingresa al directorio doc/sql-scripts de la carpeta donde se encuentra EJBCA.

Figura 55

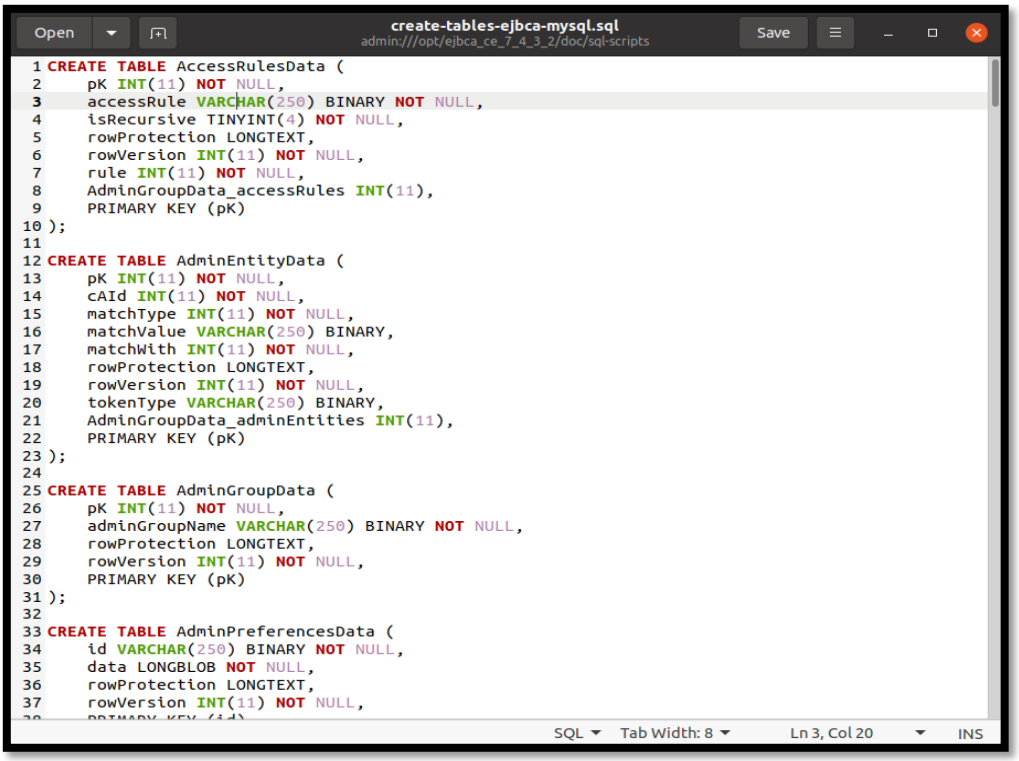
scripts de la carpeta donde se encuentra EJBCA.



4.7. Se abre el archivo create-tables-ejbca-mysql.sql y se copia su contenido.

Figura 56

archivo create-tables

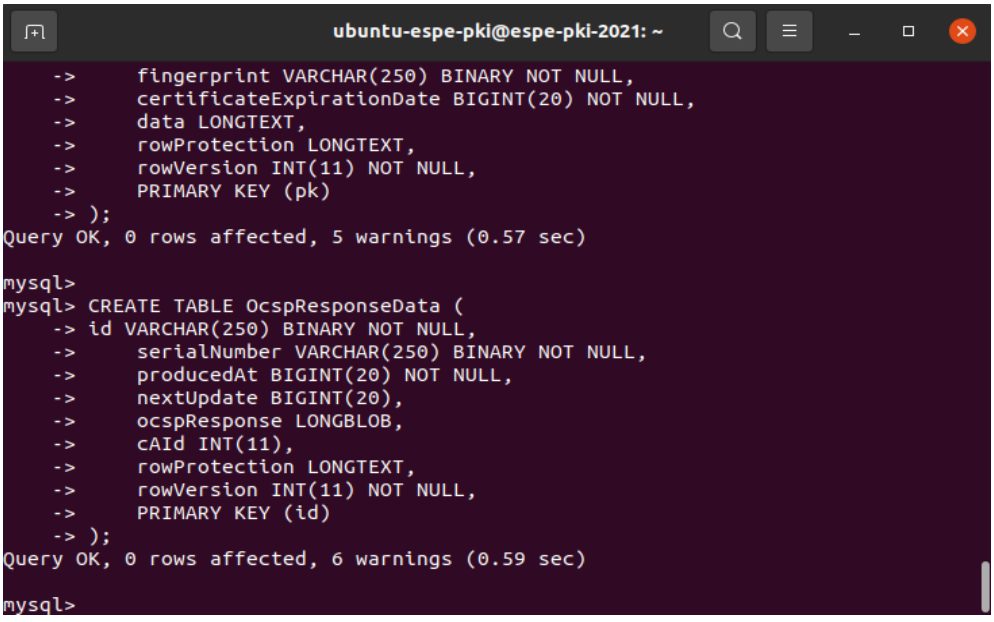



```
CREATE TABLE AccessRulesData (
    pK INT(11) NOT NULL,
    accessRule VARCHAR(250) BINARY NOT NULL,
    isRecursive TINYINT(4) NOT NULL,
    rowProtection LONGTEXT,
    rowVersion INT(11) NOT NULL,
    rule INT(11) NOT NULL,
    AdminGroupData_accessRules INT(11),
    PRIMARY KEY (pK)
);

CREATE TABLE AdminEntityData (
    pK INT(11) NOT NULL,
    cAId INT(11) NOT NULL,
    matchType INT(11) NOT NULL,
    matchValue VARCHAR(250) BINARY,
    matchWith INT(11) NOT NULL,
    rowProtection LONGTEXT,
    rowVersion INT(11) NOT NULL,
    tokenType VARCHAR(250) BINARY,
    AdminGroupData_adminEntities INT(11),
    PRIMARY KEY (pK)
);

CREATE TABLE AdminGroupData (
    pK INT(11) NOT NULL,
    adminGroupName VARCHAR(250) BINARY NOT NULL,
    rowProtection LONGTEXT,
    rowVersion INT(11) NOT NULL,
    PRIMARY KEY (pK)
);

CREATE TABLE AdminPreferencesData (
    id VARCHAR(250) BINARY NOT NULL,
    data LONGBLOB NOT NULL,
    rowProtection LONGTEXT,
    rowVersion INT(11) NOT NULL,
```

4.8. Se pega en la consola el contenido y se deja que se ejecute.

Figura 57

consola el contenido y ejecución

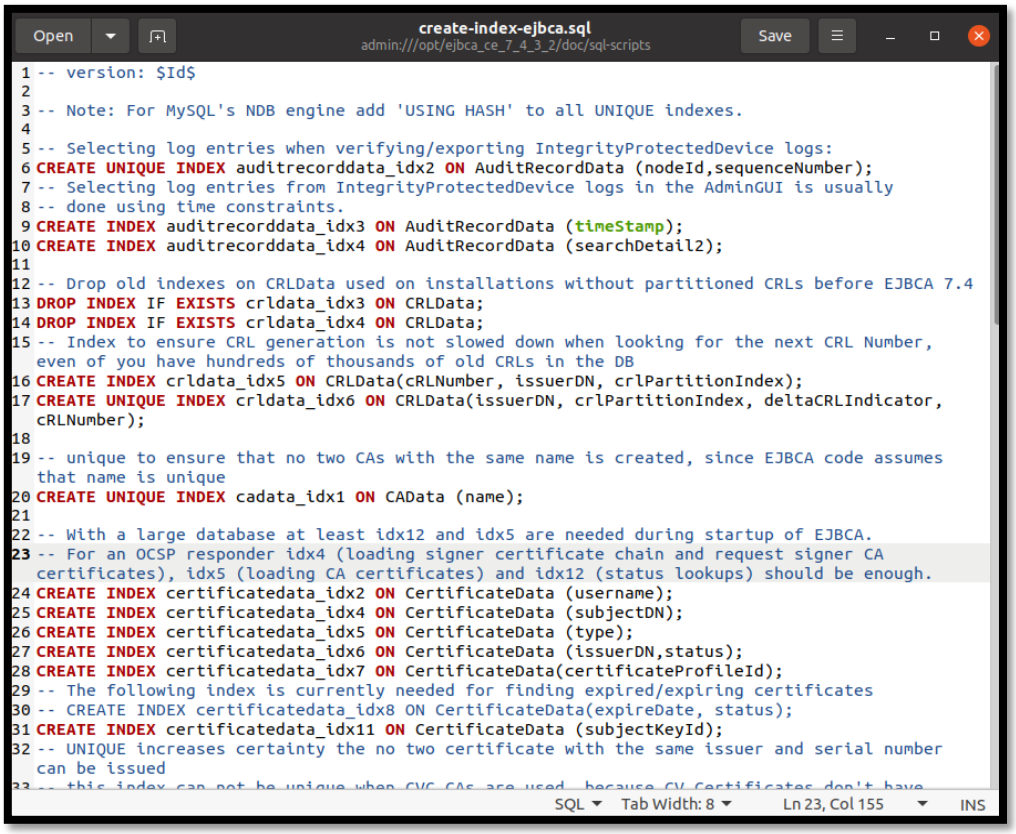



```
    ->     fingerprint VARCHAR(250) BINARY NOT NULL,
    ->     certificateExpirationDate BIGINT(20) NOT NULL,
    ->     data LONGTEXT,
    ->     rowProtection LONGTEXT,
    ->     rowVersion INT(11) NOT NULL,
    ->     PRIMARY KEY (pk)
    -> );
Query OK, 0 rows affected, 5 warnings (0.57 sec)

mysql>
mysql> CREATE TABLE OcspResponseData (
    -> id VARCHAR(250) BINARY NOT NULL,
    ->     serialNumber VARCHAR(250) BINARY NOT NULL,
    ->     producedAt BIGINT(20) NOT NULL,
    ->     nextUpdate BIGINT(20),
    ->     ocspResponse LONGBLOB,
    ->     cAId INT(11),
    ->     rowProtection LONGTEXT,
    ->     rowVersion INT(11) NOT NULL,
    ->     PRIMARY KEY (id)
    -> );
Query OK, 0 rows affected, 6 warnings (0.59 sec)

mysql>
```

4.9. Se abre el archivo create-index-ejbca.sql y se copia su contenido.

Figura 58

archivo create-index-ejbca.sql

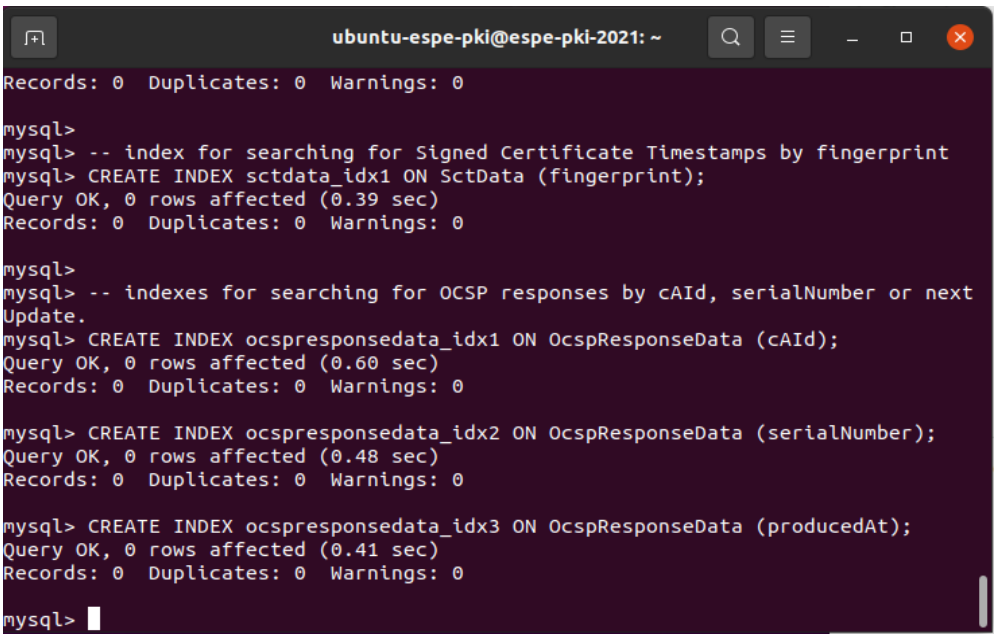



```
1 -- version: $Id$
2
3 -- Note: For MySQL's NDB engine add 'USING HASH' to all UNIQUE indexes.
4
5 -- Selecting log entries when verifying/exporting IntegrityProtectedDevice logs:
6 CREATE UNIQUE INDEX auditrecorddata_idx2 ON AuditRecordData (nodeId,sequenceNumber);
7 -- Selecting log entries from IntegrityProtectedDevice logs in the AdminGUI is usually
8 -- done using time constraints.
9 CREATE INDEX auditrecorddata_idx3 ON AuditRecordData (timeStamp);
10 CREATE INDEX auditrecorddata_idx4 ON AuditRecordData (searchDetail2);
11
12 -- Drop old indexes on CRLData used on installations without partitioned CRLs before EJBCA 7.4
13 DROP INDEX IF EXISTS crldata_idx3 ON CRLData;
14 DROP INDEX IF EXISTS crldata_idx4 ON CRLData;
15 -- Index to ensure CRL generation is not slowed down when looking for the next CRL Number,
   even of you have hundreds of thousands of old CRLs in the DB
16 CREATE INDEX crldata_idx5 ON CRLData(cRLNumber, issuerDN, crlPartitionIndex);
17 CREATE UNIQUE INDEX crldata_idx6 ON CRLData(issuerDN, crlPartitionIndex, deltaCRLIndicator,
   cRLNumber);
18
19 -- unique to ensure that no two CAs with the same name is created, since EJBCA code assumes
   that name is unique
20 CREATE UNIQUE INDEX cadata_idx1 ON CAData (name);
21
22 -- With a large database at least idx12 and idx5 are needed during startup of EJBCA.
23 -- For an OCSP responder idx4 (loading signer certificate chain and request signer CA
   certificates), idx5 (loading CA certificates) and idx12 (status lookups) should be enough.
24 CREATE INDEX certificatedata_idx2 ON CertificateData (username);
25 CREATE INDEX certificatedata_idx4 ON CertificateData (subjectDN);
26 CREATE INDEX certificatedata_idx5 ON CertificateData (type);
27 CREATE INDEX certificatedata_idx6 ON CertificateData (issuerDN,status);
28 CREATE INDEX certificatedata_idx7 ON CertificateData(certificateProfileId);
29 -- The following index is currently needed for finding expired/expiring certificates
30 -- CREATE INDEX certificatedata_idx8 ON CertificateData(expireDate, status);
31 CREATE INDEX certificatedata_idx11 ON CertificateData (subjectKeyId);
32 -- UNIQUE increases certainty the no two certificate with the same issuer and serial number
   can be issued
```

4.10. Se pega en la consola el contenido y se deja que se ejecute.

Figura 59

consola el contenido



5. Instalar y configuración del servidor de aplicaciones.

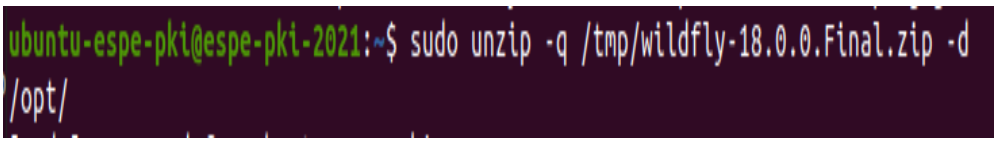
5.1. Descargar y extraer Wildfly 18.0.1

5.1.1. Se ejecuta el comando para descargar wildfly

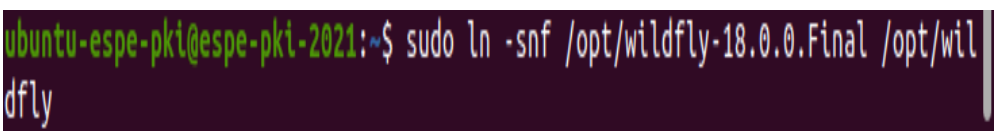
Figura 60

Instalar y configuración del servidor de aplicaciones

5.1.2. Se procede a descomprimir en una carpeta a escoger para este caso en la carpeta opt.



5.1.3. Se crea enlaces entre ficheros



5.2. Eliminar RESTEasy-Crypto

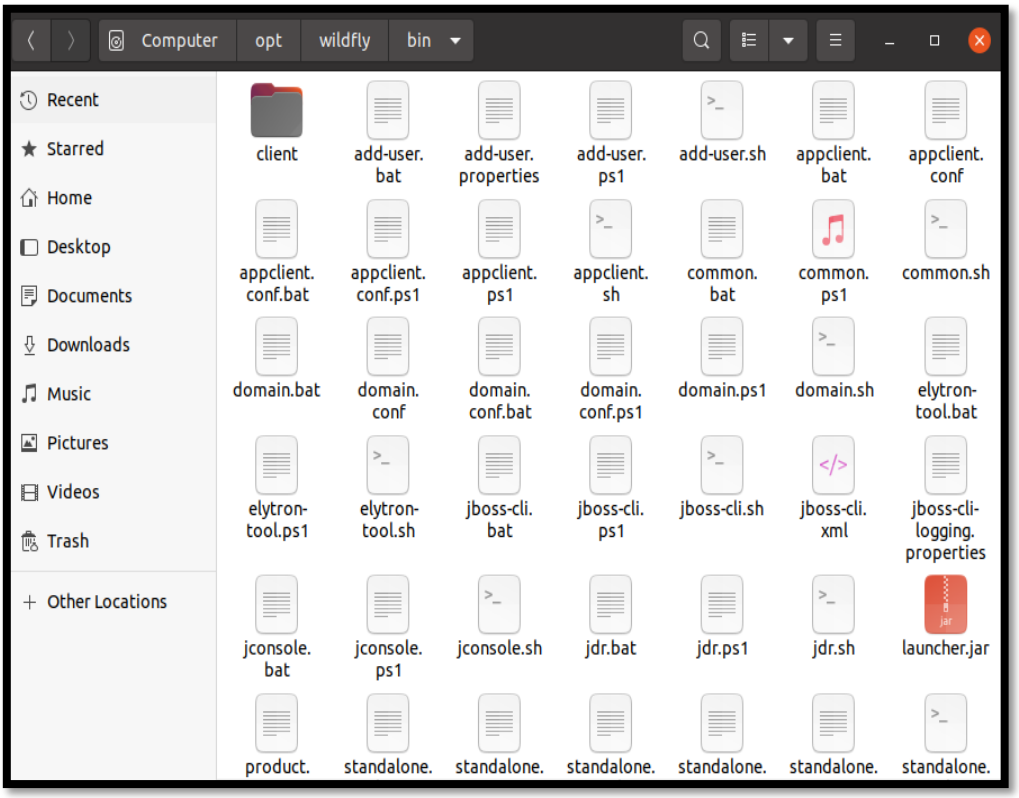
5.2.1. Se ejecuta los comandos:

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo sed -i 's|.*org.jboss.resteasy.resteasy-cr
ypto.*||' /opt/wildfly/modules/system/layers/base/org/jboss/as/jaxrs/main/module
.xml
```

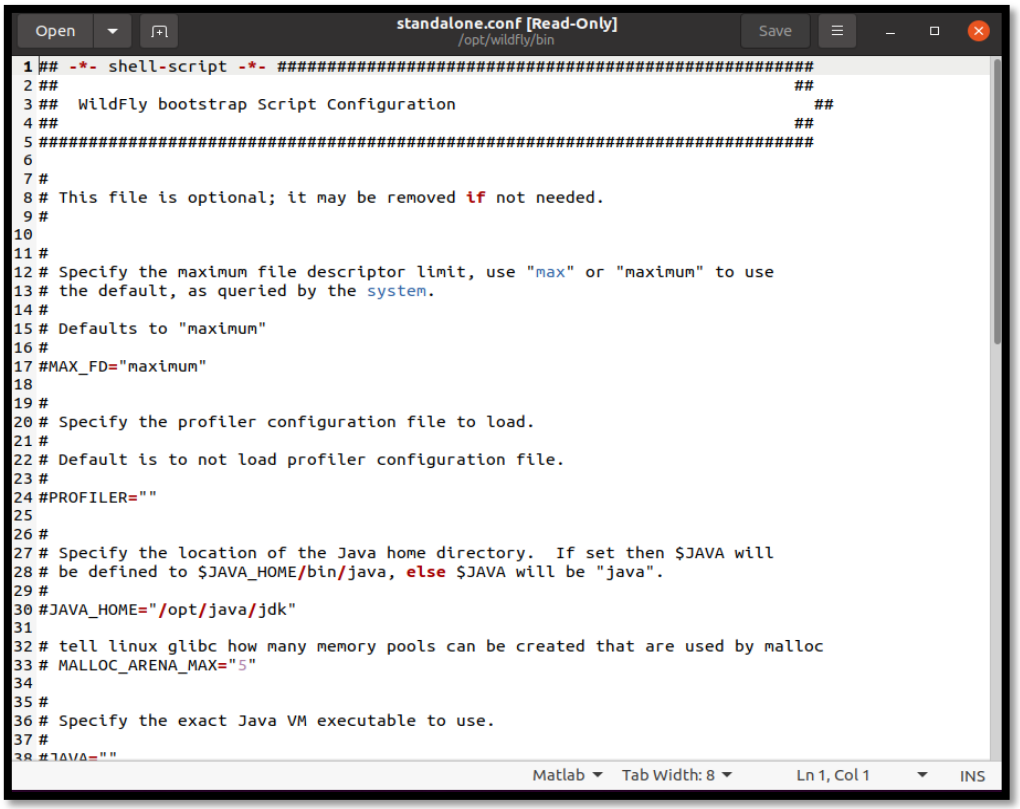
```
ubuntu-espe-pki@espe-pki-2021:~$ sudo rm -rf /opt/wildfly/modules/system/layers/
base/org/jboss/resteasy/resteasy-crypto
```

5.3. Crear una configuración personalizada

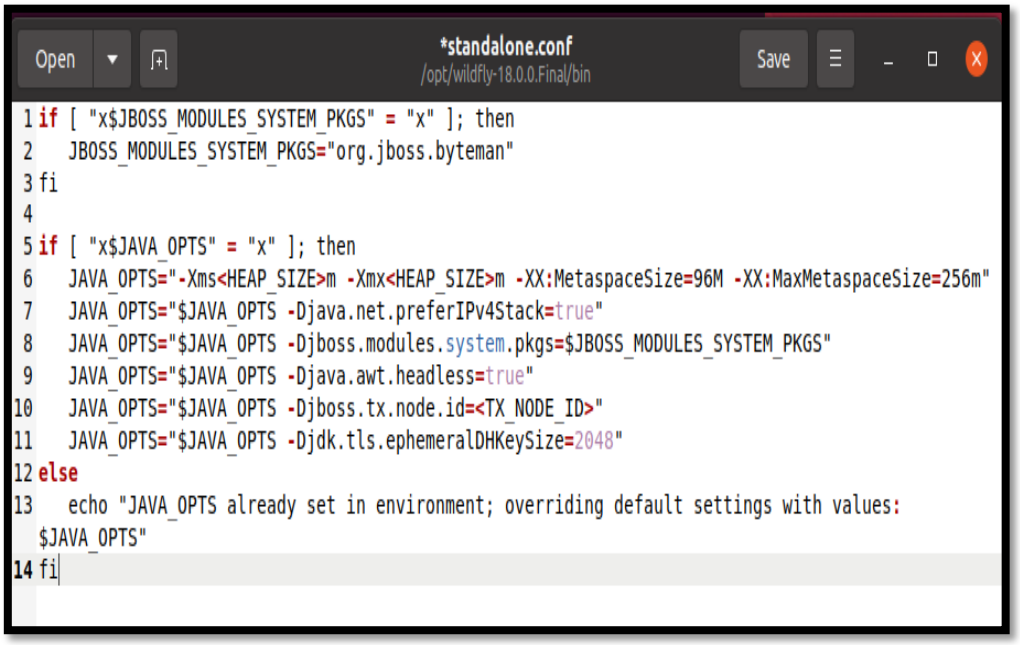
5.3.1. Se ingresa al directorio /bin de la carpeta donde se encuentra el servidor de aplicaciones wildfly



5.3.2. Se abre el archivo standlone.conf y se borra su contenido.



5.3.3. Se pega el contenido que necesita para ejecutar EJBCA



5.4. Se ejecuta el comando para establecer el uso de memoria permitido.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo sed -i -e 's/<HEAP_SIZE>/2048/g' /opt/wild
fly/bin/standalone.conf
```

5.5. Se ejecuta el comando para establecer ID de nodo de transacción.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo sed -i -e "s/<TX_NODE_ID>/$(od -A n -t d -
N 1 /dev/urandom | tr -d ' ')/g" /opt/wildfly/bin/standalone.conf
```

5.6. Se configura WildFly como servicio ejecutando 7 comandos.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo cp /opt/wildfly/docs/contrib/scripts/syste
md/launch.sh /opt/wildfly/bin
ubuntu-espe-pki@espe-pki-2021:~$ sudo cp /opt/wildfly/docs/contrib/scripts/syste
md/wildfly.service /etc/systemd/system
ubuntu-espe-pki@espe-pki-2021:~$ sudo mkdir /etc/wildfly
ubuntu-espe-pki@espe-pki-2021:~$ sudo cp /opt/wildfly/docs/contrib/scripts/syste
md/wildfly.conf /etc/wildfly
ubuntu-espe-pki@espe-pki-2021:~$ sudo systemctl daemon-reload
ubuntu-espe-pki@espe-pki-2021:~$ sudo useradd -M wildfly
ubuntu-espe-pki@espe-pki-2021:~$ sudo chown -R wildfly:wildfly /opt/wildfly-18.0
.0.Final/
```

5.7. Se inicia wildfly como servicio con el comando.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo systemctl start wildfly
```

5.8. Crear una tienda de credenciales Elytron

5.8.1. Se ejecuta los comandos para crear una clave maestra

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo echo '#!/bin/sh' > /usr/bin/wildfly_pass
ubuntu-espe-pki@espe-pki-2021:~$ sudo echo "echo '$(openssl rand -base64 24)'" >
> /usr/bin/wildfly_pass
ubuntu-espe-pki@espe-pki-2021:~$ sudo chown wildfly:wildfly sudo /usr/bin/wildfl
y_pass
ubuntu-espe-pki@espe-pki-2021:~$ sudo chmod 700 sudo /usr/bin/wildfly_pass
```

5.8.2. Se ejecuta el comando para crear la tienda de credenciales, cambiando el nombre de la tienda de credenciales defaultCS por masterCS.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/credential-store=masterCS:add(location=credentials, relative-t
o=jboss.server.config.dir, credential-reference={clear-text="{EXT}/usr/bin/wildf
ly_pass", type="COMMAND"}, create=true)'
{"outcome" => "success"}
```

5.9. Se agrega el driver de base de datos al servidor de aplicaciones

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo wget https://downloads.mariadb.com/Connect
ors/java/latest/mariadb-java-client-2.3.0.jar -O /opt/wildfly/standalone/deploym
ents/mariadb-java-client.jar
```

5.10. Agregar la fuente de datos.

5.10.1. Se ejecuta el comando para agregar un una credencial a la tienda para lo cual se coloca el nombre de la tienda definido en pasos anteriores y la contraseña definida en el archivo database.properties de la carpeta donde se encuentra EJBCA.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/credential-store=masterCS:add-alias(alias=dbPassword, secret-v
alue="MYejbcaPassM4r1a*2021")'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.10.2. Se ejecuta el comando para crear la fuente de datos al servidor de aplicaciones para lo cual se coloca la URL de la base de datos, el driver de base de datos, el nombre usuario establecido para la base de datos y la credencial del paso anterior.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect 'd
ata-source add --name=ejbcads --driver-name="mariadb-java-client.jar" --connecti
on-url="jdbc:mysql://127.0.0.1:3306/ejbca" --jndi-name="java:/EjbcaDS" --use-ccm
=true --driver-class="org.mariadb.jdbc.Driver" --user-name="ejbca" --credential-
reference={store=masterCS, alias=dbPassword} --validate-on-match=true --backgrou
nd-validation=false --prepared-statements-cache-size=50 --share-prepared-stateme
nts=true --min-pool-size=5 --max-pool-size=150 --pool-prefill=true --transaction
-isolation=TRANSACTION_READ_COMMITTED --check-valid-connection-sql="select 1;"'
```

5.10.3. Se recarga el servicio.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
reload'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.11. Se ejecuta los comandos para configurar wildfly remotamente.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=remoting/http-connector=http-remoting-connector:write-attribute(name=c
onnector-ref,value=remoting)'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
socket-binding-group=standard-sockets/socket-binding=remoting:add(port=4447,inte
rface=management)'
{
    "outcome" => "success",
    "response-headers" => {"process-state" => "reload-required"}
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=undertow/server=default-server/http-listener=remoting:add(socket-bindi
ng=remoting,enable-http2=true)'
{
    "outcome" => "success",
    "response-headers" => {"process-state" => "reload-required"}
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
reload'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.12. Configuración de los registros.

5.12.1. Se ejecuta los comandos para configurar los logs principales y su nivel.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=logging/logger=org.ejbca:add(level=INFO)'

{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=logging/logger=org.cesecore:add(level=INFO)'
{"outcome" => "success"}
```

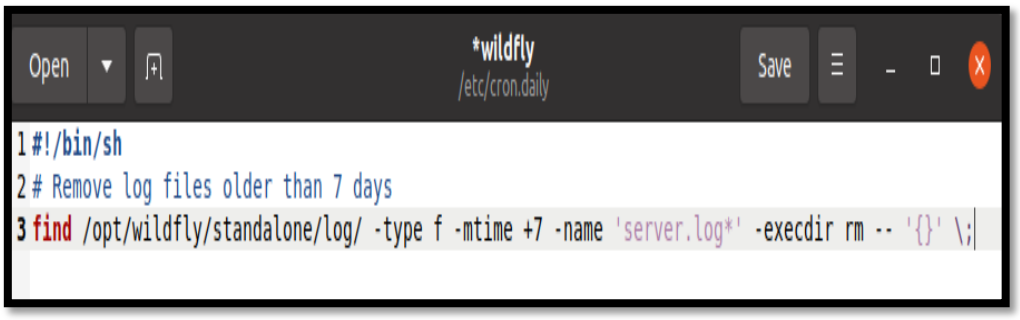
5.12.2. Se ejecuta los comandos para la configuración de logs adicional.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=logging/logger=org.jboss:add(level=WARN)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=logging/logger=org.cesecore.config.ConfigurationHolder:add(level=WARN)
'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=logging/logger=org.hibernate.dialect.H2Dialect:add(level=ERROR)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=logging/logger=org.wildfly:add(level=WARN)'
{"outcome" => "success"}
```

5.12.3. Eliminar archivos de log pasado los 7 días.

5.12.3.1. Se crea un archivo llamado wildfly en el directorio etc/cron.daily.

5.12.3.2. Se coloca el script para la ejecución.



5.12.3.3. Se ejecuta el comando para hacer el archivo ejecutable.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo chmod +x /etc/cron.daily/wildfly
```

5.13. Configuración de escucha HTTP (S) con separación de 3 puertos.

5.13.1. Se ejecuta los comandos para Eliminar la configuración HTTP y TLS existente.

```
ubuntu-espe-pki@espe-pki-2021: ~
buntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
ubsystem=undertow/server=default-server/http-listener=default:remove()'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
buntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
ubsystem=undertow/server=default-server/https-listener=https:remove()'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
buntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
ocket-binding-group=standard-sockets/socket-binding=http:remove()'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
buntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
ocket-binding-group=standard-sockets/socket-binding=https:remove()'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
buntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
eload'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.13.2. Se ejecuta los comandos para agregar nuevas interfaces y sockets.

5.13.3. Se ejecuta los comandos para Configurar TLS para lo cual se debe colocar la contraseña del almacén de claves para keystore.jks, la contraseña del almacén de confianza para truststore.jks que están definidos en el archivo web.properties de la carpeta donde se encuentra EJBCA y el nombre de la tienda de credenciales definida en pasos anteriores.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/credential-store=masterCS:add-alias(alias=httpsKeystorePasswor
d, secret-value="serverKSP4ssx0rd2021")'
{
    "outcome" => "success",
    "result" => undefined
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/credential-store=masterCS:add-alias(alias=httpsTruststorePassw
ord, secret-value="JtpP4ssx0rd2021")'
{
    "outcome" => "success",
    "result" => undefined
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/key-store=httpsKS:add(path="keystore/keystore.jks",relative-to
=jboss.server.config.dir,credential-reference={store=masterCS, alias=httpsKeysto
rePassword},type=JKS)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/key-store=httpsTS:add(path="keystore/truststore.jks",relative-
to=jboss.server.config.dir,credential-reference={store=masterCS, alias=httpsTrus
tstorePassword},type=JKS)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/key-manager=httpsKM:add(key-store=httpsKS,algorithm="SunX509",
credential-reference={store=masterCS, alias=httpsKeystorePassword})'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/trust-manager=httpsTM:add(key-store=httpsTS)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/server-ssl-context=httpspub:add(key-manager=httpsKM,protocols=
["TLSv1.2"],use-cipher-suites-order=false,cipher-suite-filter="TLS_DHE_RSA_WITH_
AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256")'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/server-ssl-context=httpspriv:add(key-manager=httpsKM,protocols
=["TLSv1.2"],use-cipher-suites-order=false,cipher-suite-filter="TLS_DHE_RSA_WITH
_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",trust-manager=httpsTM
,need-client-auth=true)'
{"outcome" => "success"}
```

5.14. Se ejecuta los comandos para agregar los escuchas HTTP(S).

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=undertow/server=default-server/http-listener=http:add(socket-binding="
http", redirect-socket="httpspriv")'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=undertow/server=default-server/https-listener=httpspub:add(socket-bind
ing="httpspub", ssl-context="httpspub", max-parameters=2048)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=undertow/server=default-server/https-listener=httpspriv:add(socket-bin
ding="httpspriv", ssl-context="httpspriv", max-parameters=2048)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
reload'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.15. Se ejecuta los comandos para la configuración del comportamiento del protocolo HTTP(S).

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
system-property=org.apache.catalina.connector.URI_ENCODING:add(value="UTF-8")'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
system-property=org.apache.catalina.connector.USE_BODY_ENCODING_FOR_QUERY_STRING
:add(value=true)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
system-property=org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH:add(valu
e=true)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
system-property=org.apache.tomcat.util.http.Parameters.MAX_COUNT:add(value=2048)
'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
system-property=org.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH:add(
value=true)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=webservices:write-attribute(name=wsdl-host, value=jbossws.undefined.ho
st)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=webservices:write-attribute(name=modify-wsdl-address, value=true)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
reload'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.16. Configuración Opcional.

5.16.1. Se ejecuta los comandos para remover el contenido inicial por defecto de wildfly.

Figura 61

ejecuta los comandos para remover el contenido

5.16.2. Se ejecuta los comandos para redirigir el contenido desconocido a la dirección /ejbca/

5.16.3. Se ejecuta los comandos para eliminar la fuente de datos ExampleDS.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=ee/service=default-bindings:remove()'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect 'd
ata-source remove --name=ExampleDS'
operation-requires-reload: true
process-state:             reload-required
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
reload'
{
    "outcome" => "success",
    "result" => undefined
}
```

5.16.4. Se ejecuta los comandos para agregar soporte para enviar correo electrónico, para lo cual se ingresa las credenciales del cliente de correo electrónico, nombre de host y puerto del servidor de correo electrónico y el nombre de la tienda de credenciales definida en pasos anteriores.

```
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=elytron/credential-store=masterCS:add-alias(alias=smtpPass, secret-val
ue="z6MCXt2UvLnXPBK")'
{
    "outcome" => "success",
    "result" => undefined
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
socket-binding-group=standard-sockets/remote-destination-outbound-socket-binding
=ejbca-mail-smtp:add(port="465", host="smtp.gmail.com")'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=mail/mail-session="java:/EjbcaMail":add(jndi-name=java:/EjbcaMail, fro
m=espe.pki.2021@gmail.com)'
{"outcome" => "success"}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/
subsystem=mail/mail-session="java:/EjbcaMail"/server=smtp:add(outbound-socket-bi
nding-ref=ejbca-mail-smtp, tls=true, username=espe.pki.2021@gmail.com, credentia
l-reference={store=masterCS, alias=smtpPass})'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
ubuntu-espe-pki@espe-pki-2021:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect ':
reload'
{
    "outcome" => "success",
    "result" => undefined
}
```

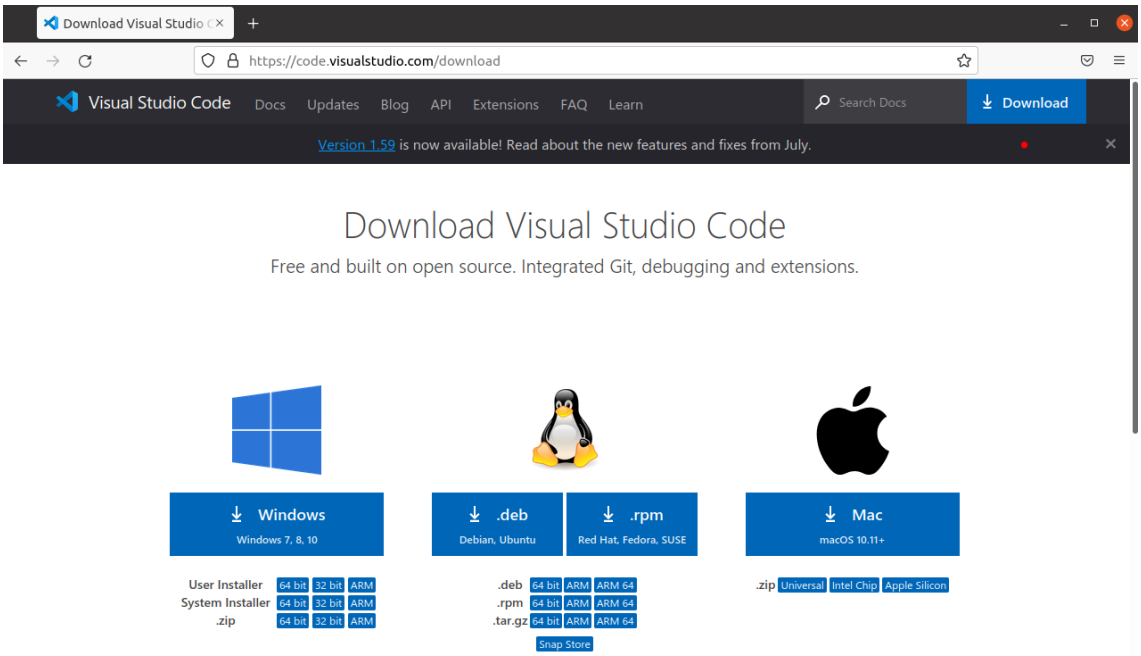
Personalizar JBCA

1. Se descarga e instala un editor de código.

   1.1. Se dirige al sitio web de Visual Studio Code y se descarga la aplicación.

Figura 62

sitio web de Visual Studio Code



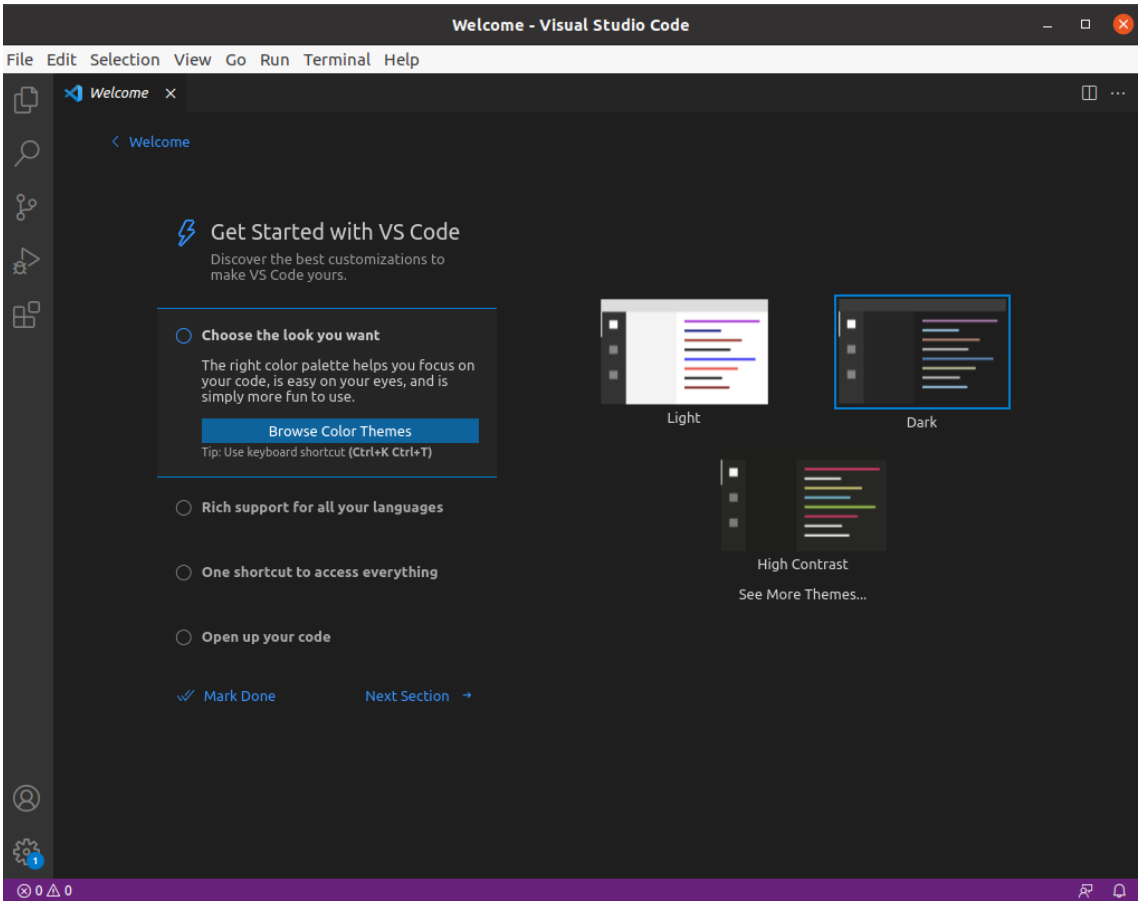
   1.2. Se ejecuta el comando para instalar el editor.

```
ubuntu-espe-pki@espe-pki-2021:~/Downloads$ sudo dpkg -i code_1.59.1-1629375198_a
md64.deb
```

   1.3. Se abre el editor de código.

Figura 63

editor de código

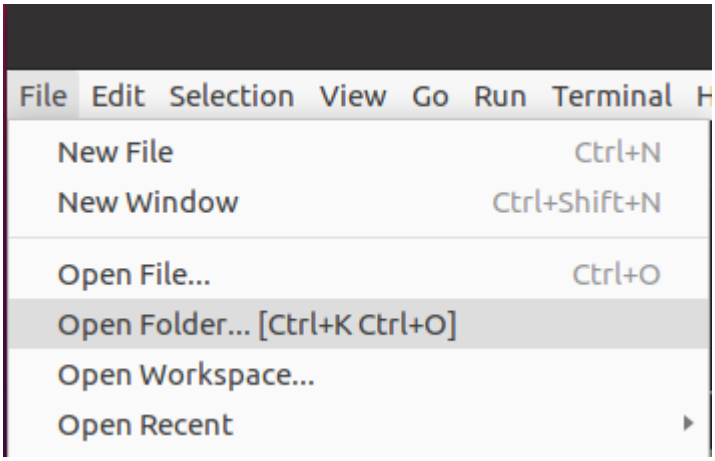


2. Importar el código fuente de EJBCA.

    2.1. Se dirige a la opción de abrir carpeta.

Figura 64

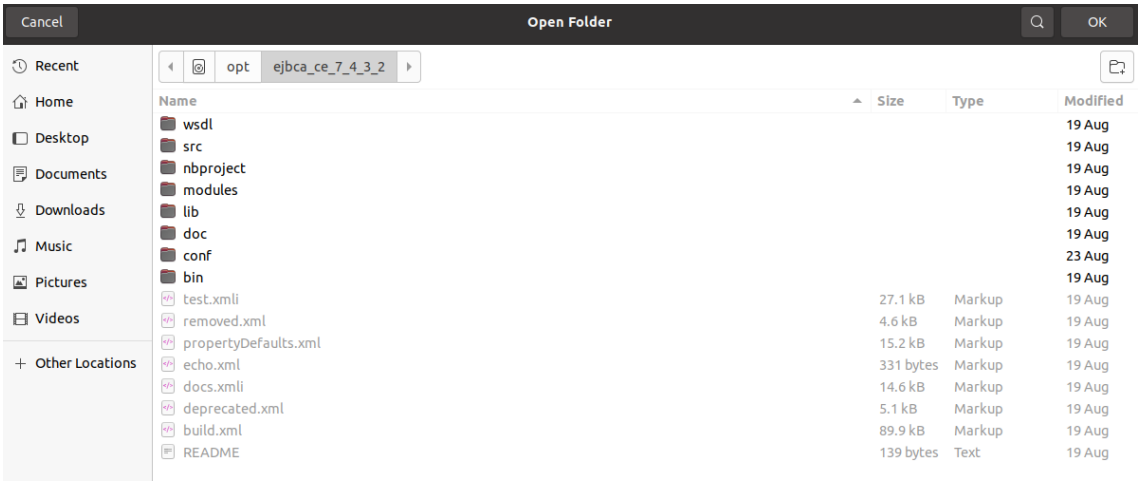
opción de abrir carpeta



2.2. Se abre la ruta carpeta donde se encuentra el proyecto de EJBCA y se pulsa en OK.

Figura 65

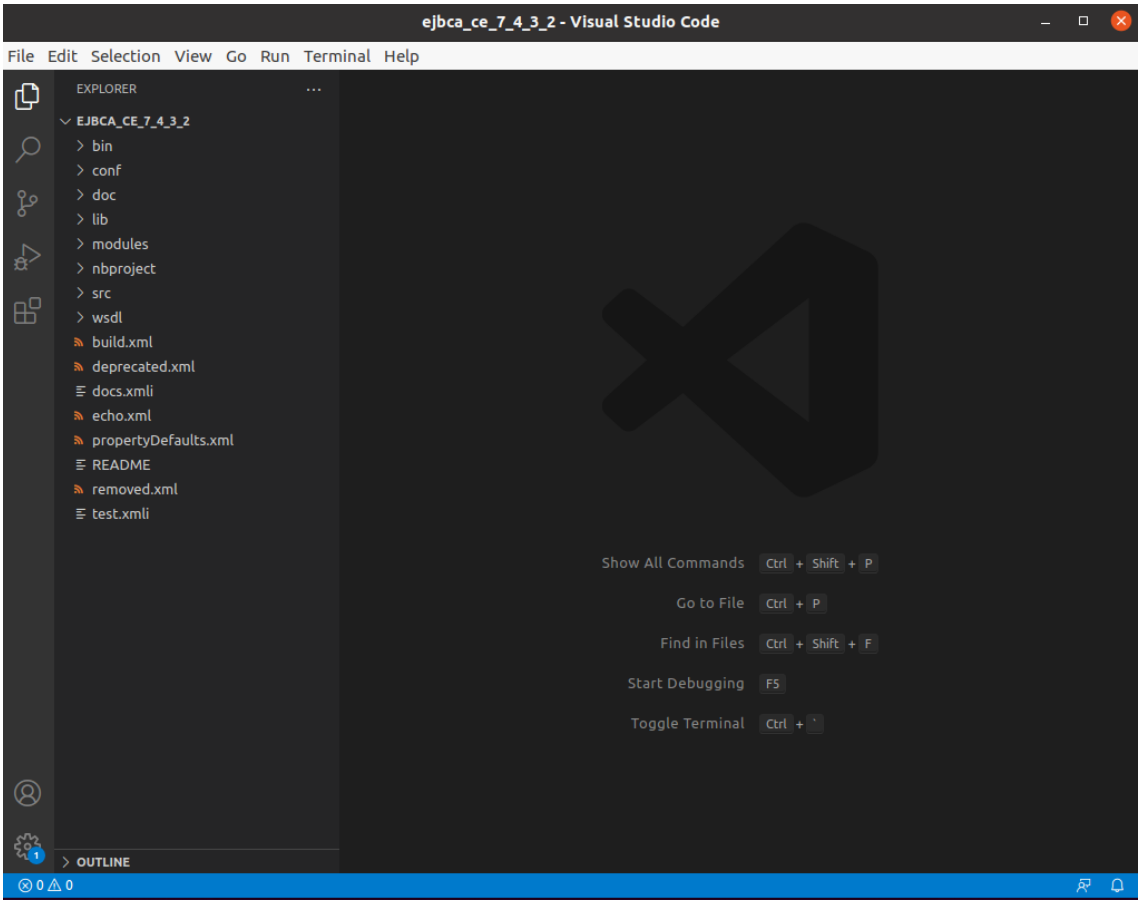
ruta carpeta donde se encuentra el proyecto de EJBCA



2.3. Se verifica que el proyecto se haya abierto correctamente.

Figura 66

verificación



3. Cambiar el idioma a español.

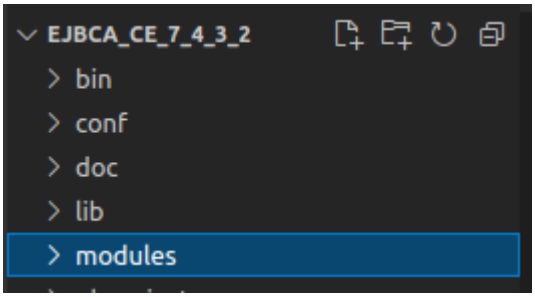
3.1. EJBCA cuenta con tres interfaces principales: la interfaz pública, interfaz de autoridad de registro e interfaz de superadministrador.

3.1.1. Interfaz pública.

3.1.1.1. Se accede a la carpeta de módulos.

Figura 67

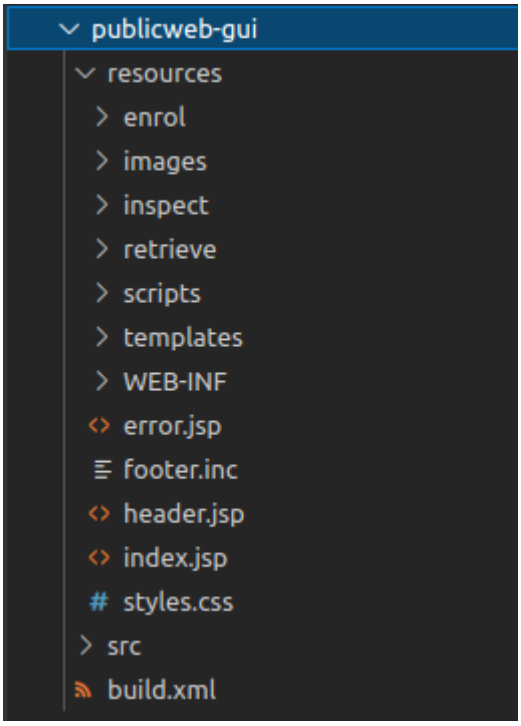
Interfaz pública



3.1.1.2. Dentro de la carpeta modules se accede a la carpeta de interfaz pública.

Figura 68

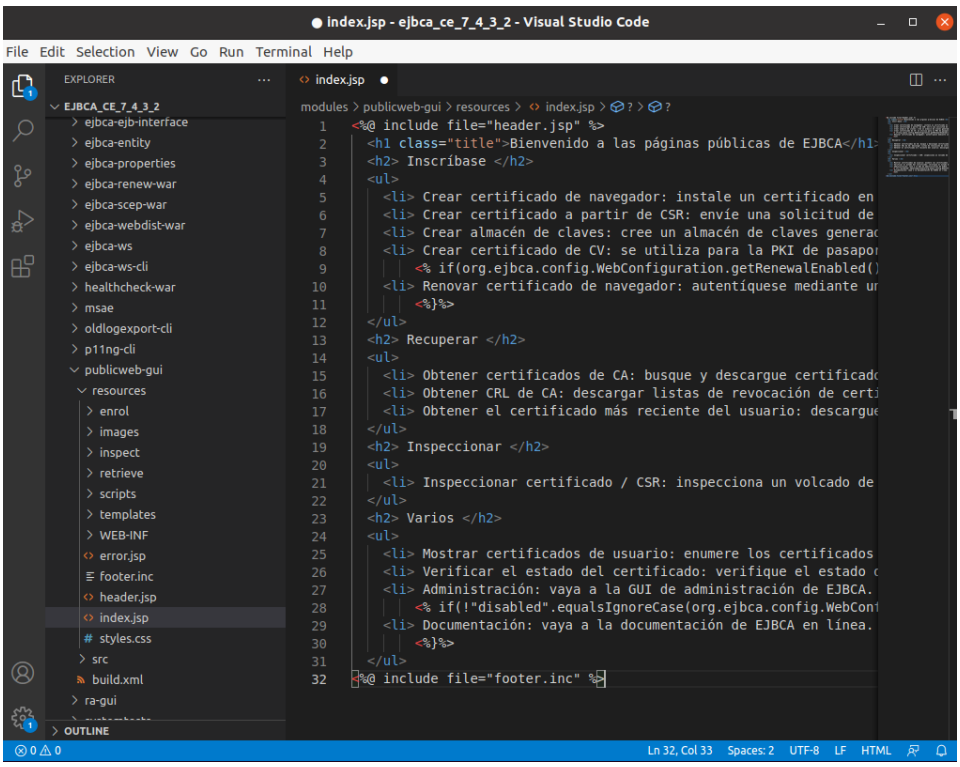
carpeta modules se accede a la carpeta de interfaz pública



3.1.1.3. Se cambia al idioma deseado a todos los archivos necesarios con formato .jsp, el idioma por defecto es el inglés, para este caso se cambia a español.

Figura 69

idioma deseado a todos los archivos necesarios

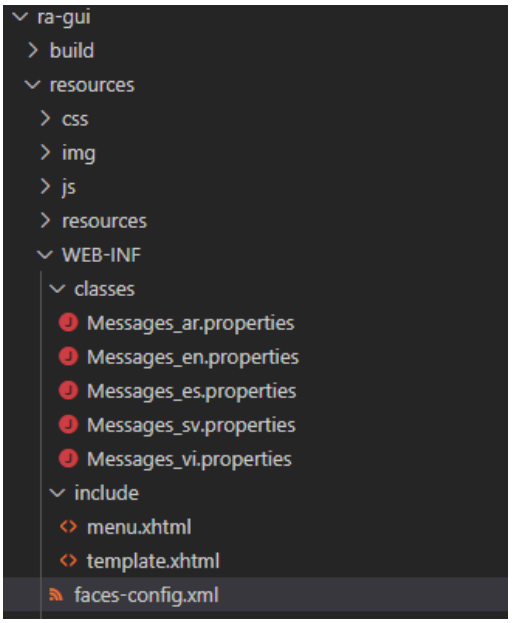


3.1.2. Interfaz de autoridad de registro

3.1.2.1. Dentro de la carpeta módulos, se dirige a la ruta re-gui/resources/WEB-INF y se abre el archivo faces-config.xml

Figura 70

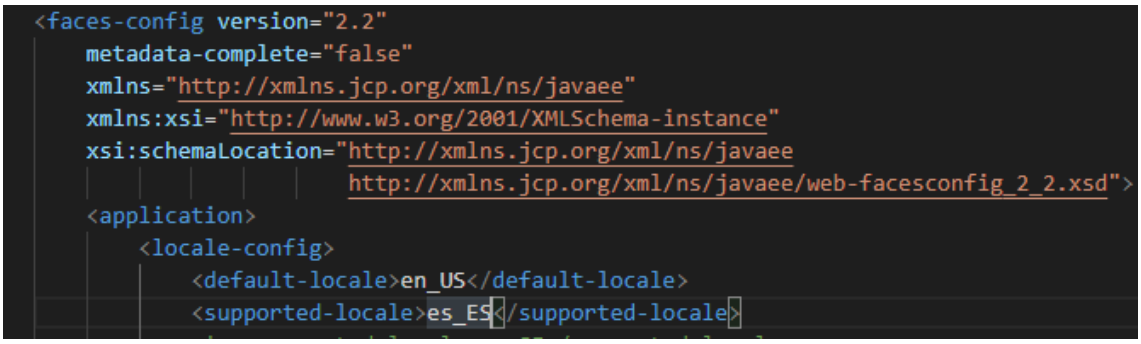
carpeta módulos



3.1.2.2. Se agrega la etiqueta para el idioma español.

Figura 71

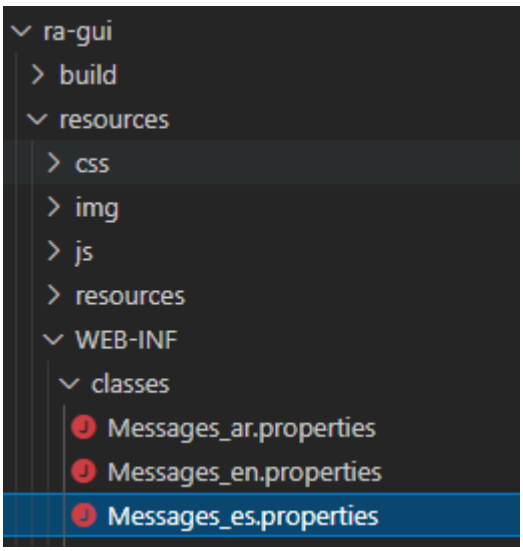
etiqueta para el idioma español



3.1.2.3. f Dentro de la carpeta módulos, se dirige a la ruta re-gui/resources/WEB-INF/classes y se agrega el archivo Messages_es.properties que contiene las traducciones en español.

Figura 72

las traducciones en español

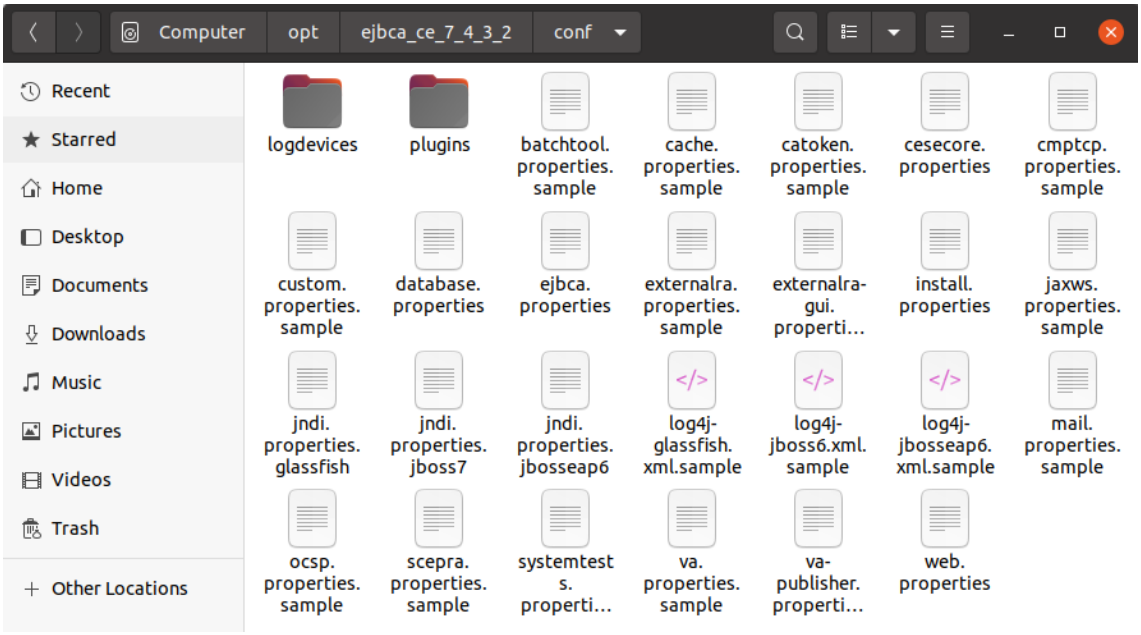


3.1.3. Interfaz de autoridad superadministrador.

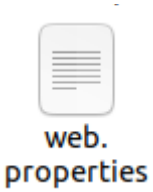
3.1.3.1. Se ingresa al directorio conf de la carpeta donde se encuentra EJBCA.

Figura 73

Interfaz de autoridad superadministrador



3.1.3.2. Se abre el archivo web.properties para configuración los idiomas.



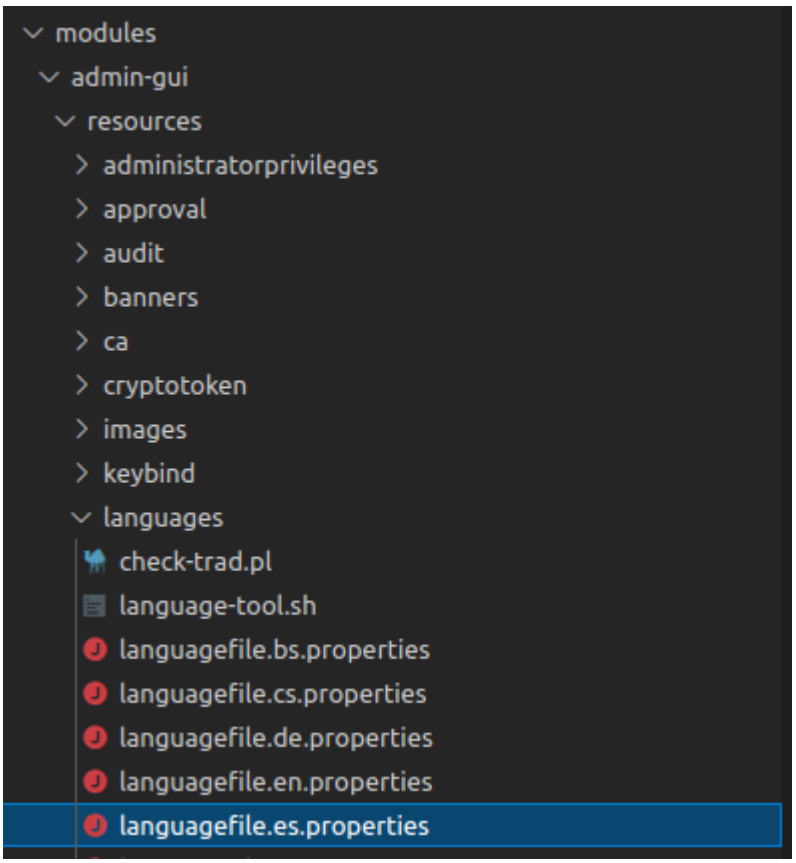
3.1.3.3. Se agrega la línea de código con los lenguajes predeterminados en web.availablelanguages, para este caso se selecciona los idiomas inglés (el cual está configurado y listo para su uso) y español.

```
# Defines the available languages by ISO 639-1 language codes separated with a comma (example: en,fr).
# If you are not sure that you know how to add a new language (languagefile.xx.properties, etc.),
# we suggest you stick with the default the first time you install if you wan't to add your own language.
# Note: Some available languages are incompletely translated (<50%); before adding them, check completeness with the following command:
#       modules/admin-gui/resources/languages/language-tool.sh -s
# When adding languages to this do _NOT_ change the order as this affects the already configured languages for admins, i.e. it's based on
# Default: en,bs,cs,de,fr,ja,pt,sv,uk,zh,vi
web.availablelanguages=en,es
```

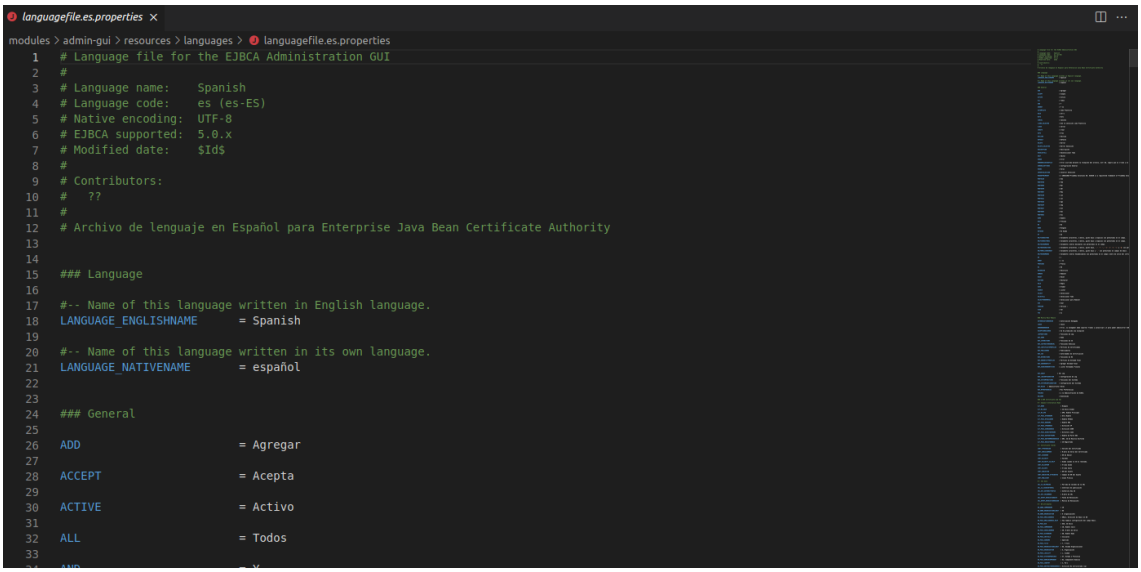
3.1.3.4. Se agrega la línea de código con la codificación de página predeterminada en web.contentencoding, para este caso ISO-8859-1.

```
# Default content encoding used to display JSP pages, for example ISO-8859-1, UTF-8 or GBK.
# Default: UTF-8
web.contentencoding=ISO-8859-1
```

3.1.3.5. Dentro de la carpeta módulos, se dirige a la ruta admin-gui/resources/languages y se abre el archivo languagefile.es.properties.



3.1.3.6. El archivo por defecto solo soporta la serie de la versión 5.0.x.



3.1.3.7. Se actualiza el archivo para que sea compatible con la versión actual.

languagefile.es.properties

modules > admin-gui > resources > languages > languagefile.es.properties

```
# Language file for the EJBCA Administration GUI
#
# Language name:    Spanish
# Language code:    es (es-ES)
# Native encoding:  UTF-8
# EJBCA supported:  7.x
# Modified date:    $Id$
#
# Contributors:
#   Alberto Carrera
#
# Archivo de lenguaje en Español para Enterprise Java Bean Certificate Authority


### Language

#-- Name of this language written in English language.
LANGUAGE_ENGLISHNAME      = Spanish

#-- Name of this language written in its own language.
LANGUAGE_NATIVENAME       = español
```

4. Cambiar los logos

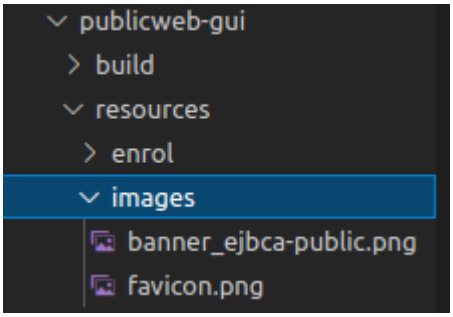
4.1. EJBCA cuenta con tres interfaces principales las cuales son la interfaz pública, interfaz de autoridad de registro e interfaz de superadministrador.

4.1.1. Interfaz pública.

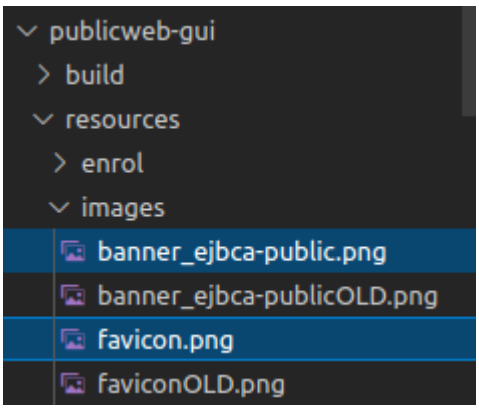
4.1.1.1. En la carpeta modules se accede a la ruta publicweb-gui/resources/images

Figura 74

cambiar los logos



4.1.1.2. Se reemplaza las imágenes actuales con los mismos nombres, en caso de querer conservar el logo antiguo se lo puede renombrar con el subijo OLD.

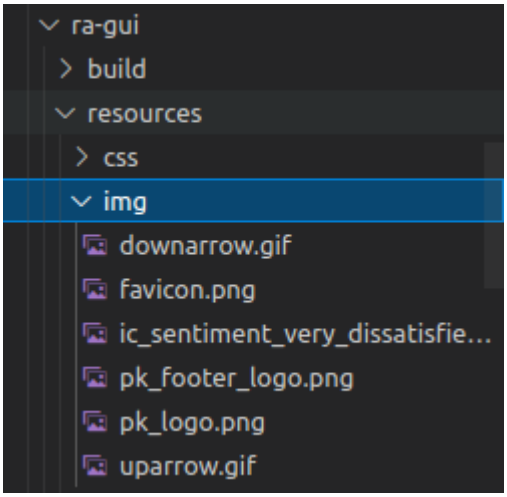


4.1.2. Interfaz de autoridad de registro

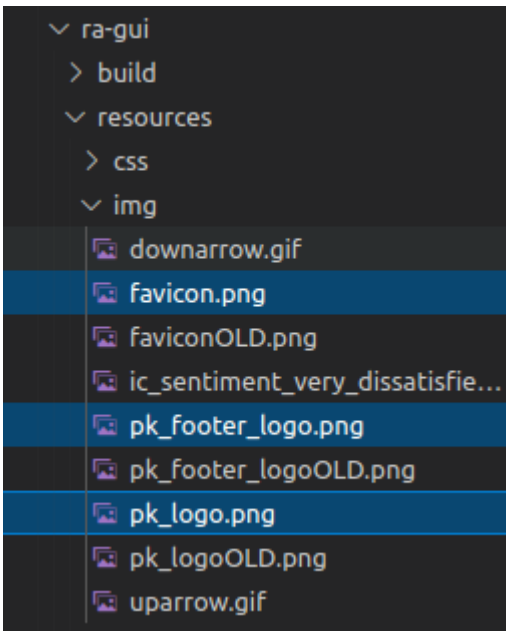
4.1.2.1. En la carpeta modules se accede a la ruta ra-gui/resources/img

Figura 75

Interfaz de autoridad de registro



4.1.2.2. Se reemplaza las imágenes actuales con los mismos nombres, en caso de querer conservar el logo antiguo se lo puede renombrar con el subijo OLD.

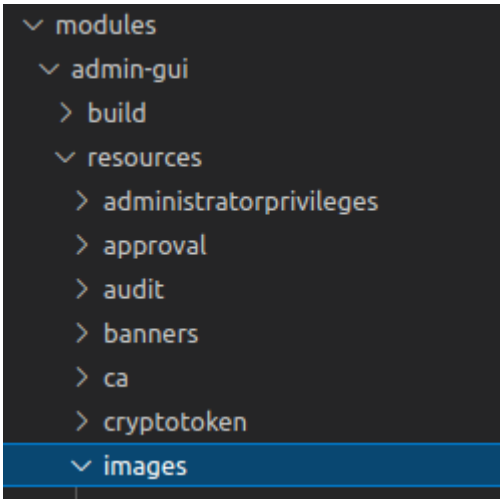


4.1.3. Interfaz de superadministrador.

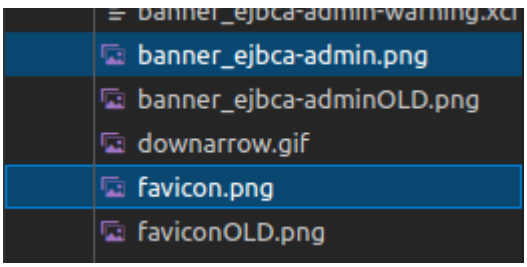
4.1.3.1. En la carpeta modules se accede a la ruta admin-gui/resources/images

Figura 76

Interfaz de superadministrador



4.1.3.2. Se reemplaza las imágenes actuales con los mismos nombres, en caso de querer conservar el logo antiguo se lo puede renombrar con el subijo OLD.



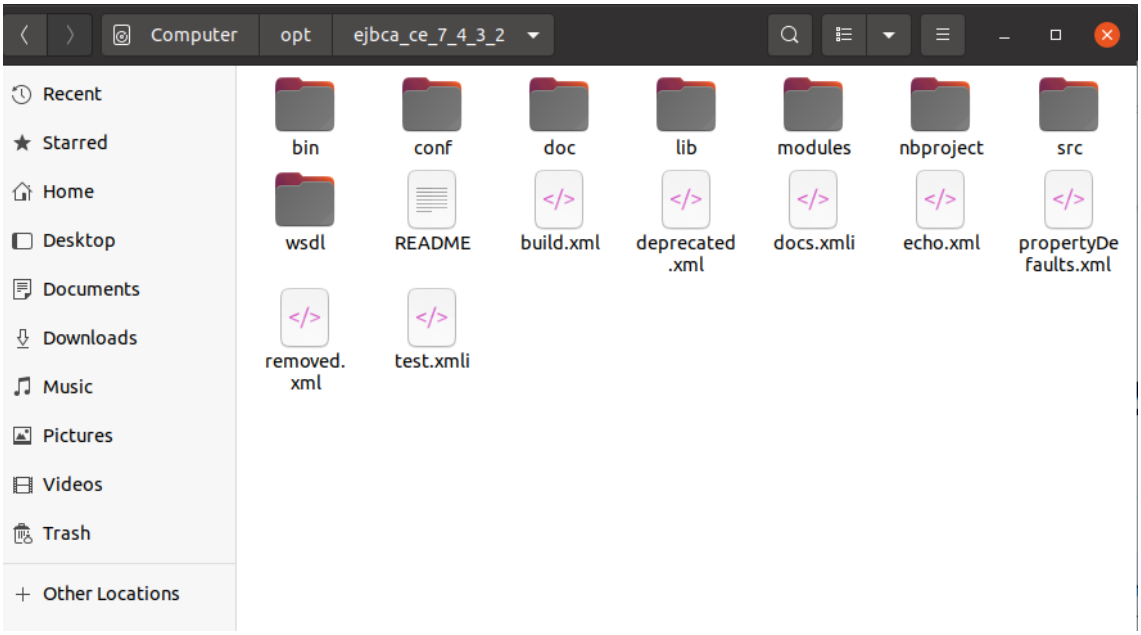
Desplegar e instalar EJBCA

1. Despliegue de EJBCA

    1.1. Se ingresa al directorio donde se encuentra EJBCA, para este caso se encuentra en la carpeta opt/ejbca_ce/7_4_3_2.

Figura 77

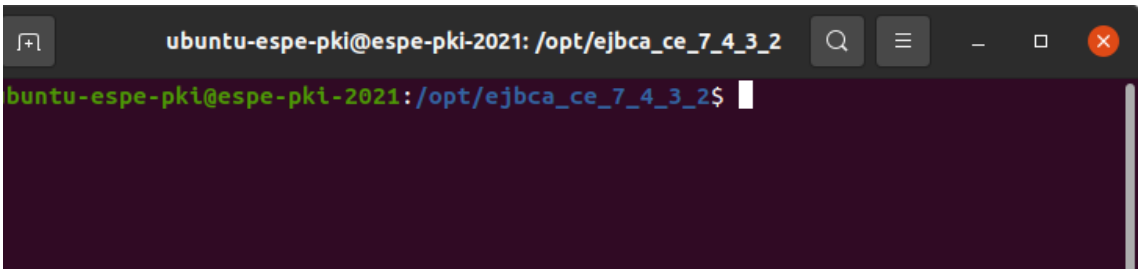
Desplegar e instalar EJBCA



    1.2. Se abre un terminal

Figura 78

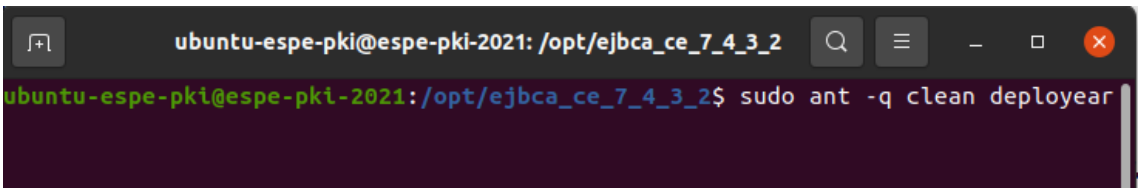
terminal



    1.3. Se despliega EJBCA mediante el comando.

Figura 79

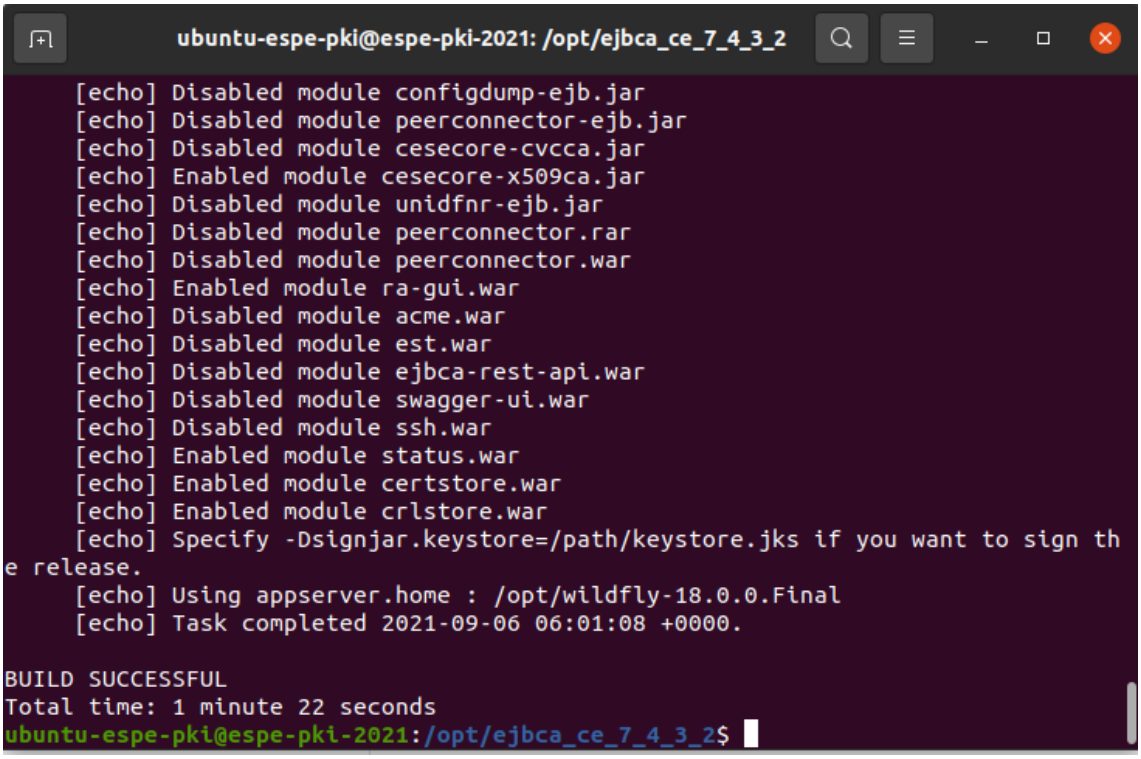
despliegue EJBCA mediante el comando



1.4. Se muestra el mensaje que la construcción ha sido exitosa lo cual indica que la aplicación ya está desplegada en el servidor

Figura 80

mensaje que la construcción ha sido exitosa

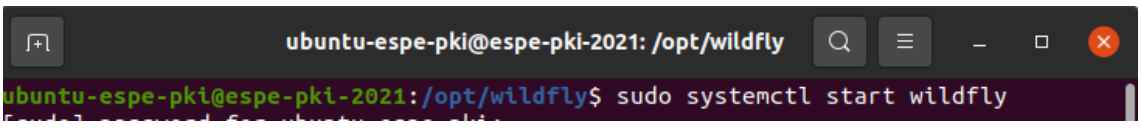


2. Instalación de EJBCA.

2.1. Se debe asegurar que el servidor de aplicaciones debe estar ejecutándose, en caso de no estarlo se ejecuta el comando.

Figura 81

servidor de aplicaciones

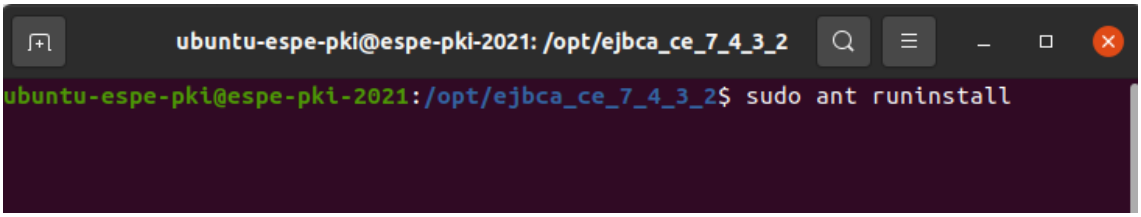


2.2. Se ejecuta el comando el cual creará la CA de gestión, los almacenes de claves TLS para manejar HTTPS, firmados por la CA de administración y el

almacén de claves para el superadministrador inicial. También agregará algunos valores de control de acceso iniciales a la base de datos e información de función para el usuario superadministrador.

Figura 82

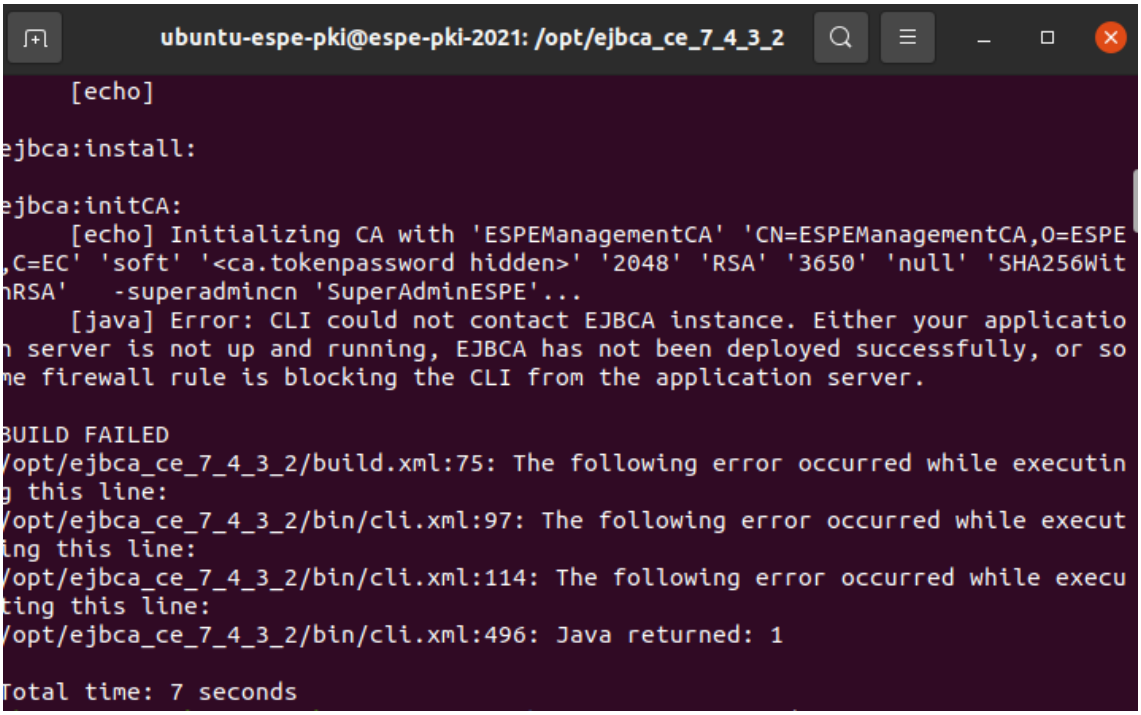
información de función para el usuario



2.2.1. Se suele presentar un error común al ejecutar este paso.

Figura 83

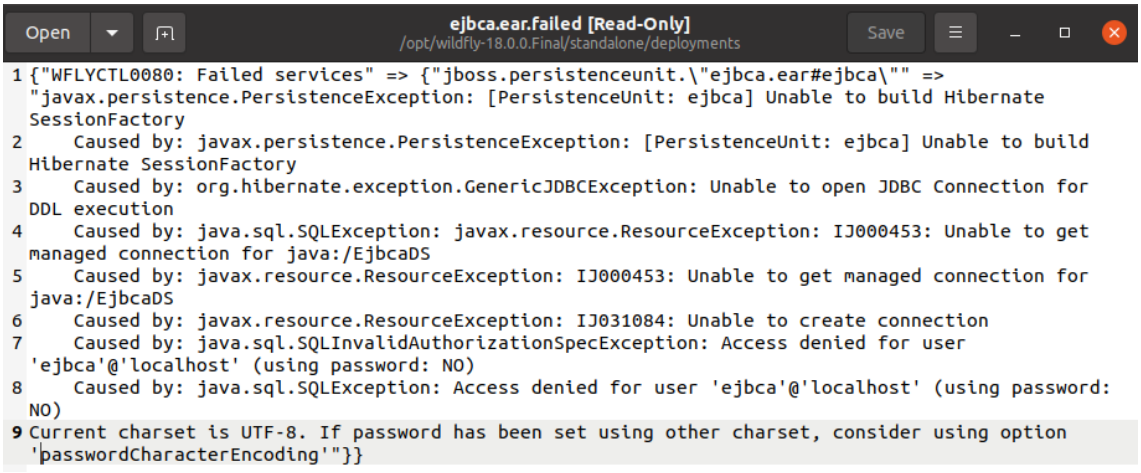
error común



2.2.2. Se busca la carpeta de despliegues del servidor de aplicaciones y se abre el archivo ejbca.ear.failed, en este caso el error fue debido a que la codificación de caracteres no ha sido asignada.

Figura 84

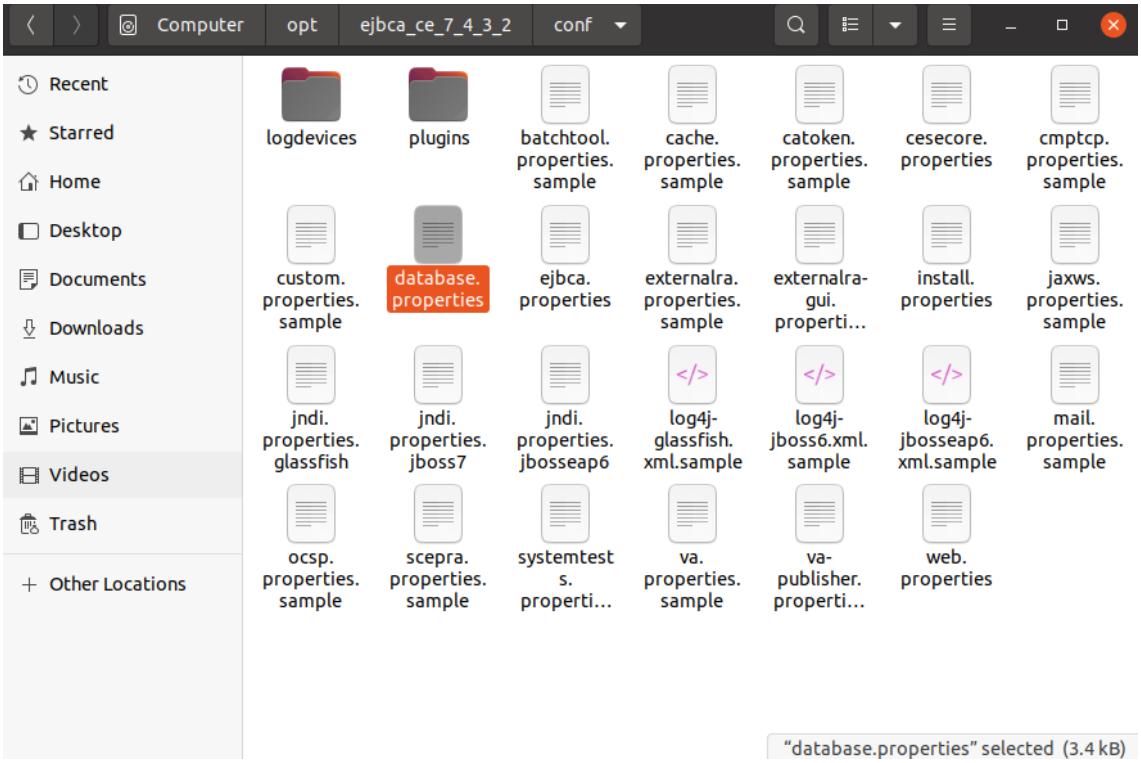
codificación de caracteres



2.2.3. Se ingresa al directorio conf de la carpeta donde se encuentra EJBCA y se abre el archivo database.propierties.

Figura 85

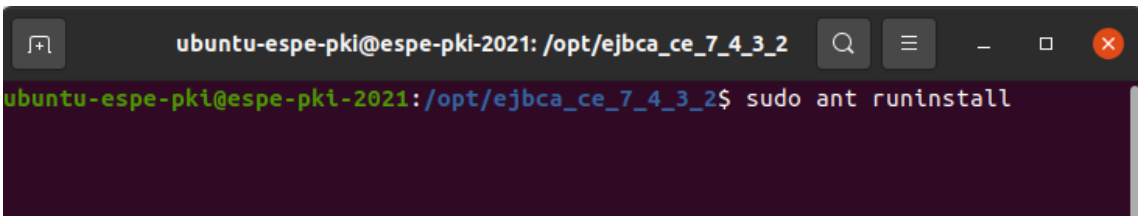
directorio conf



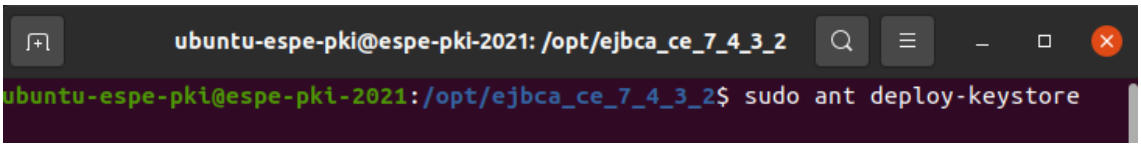
2.2.4. Se agrega la línea de código al final del archivo.

```
81 database.passwordCharacterEncoding=UTF-8
```

2.3. Se ejecuta nuevamente el comando.



2.4. Después de la instalación, se han creado almacenes de claves TLS. Se ejecuta el comando para copiarlos en wildfly_home/standalone/configuration/keystore.



2.5. Se accede desde un navegador al enlace (https://ip_servidor:8443/ejbca/) y se comprueba que esté levantado el servidor.

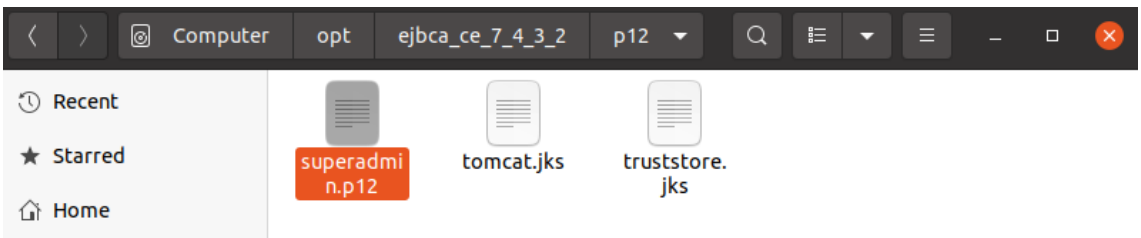
Configuración para operaciones EJBCA

1. Acceder a la consola de administrador con usuario de SuperAdministrador

1.1. Se ingresa al directorio p12 de la carpeta donde se encuentra EJBCA y se ubica el certificado digital con extensión .p12, el cual servirá para iniciar sesión.

Figura 86

Configuración para operaciones EJBCA

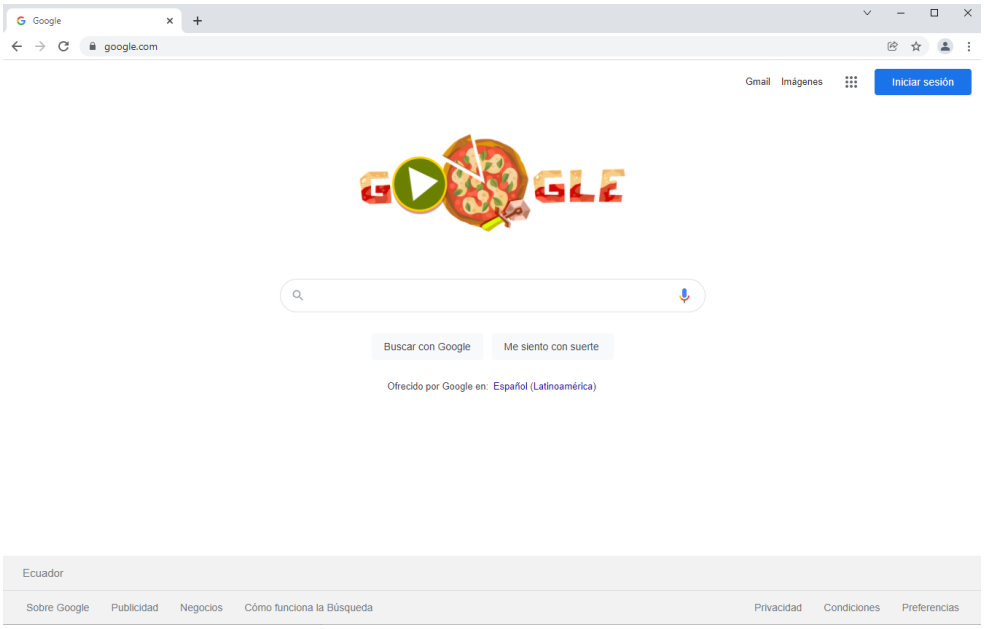


1.2. Para acceder a la consola de administración se debe abrir cualquier navegador, a continuación se detalla como cargar el certificado digital necesario para iniciar sesión en el navegador Google Chrome Versión 96.0.4664.45 de 64 bits.

1.2.1. Se abre el navegador Google Chrome.

Figura 87

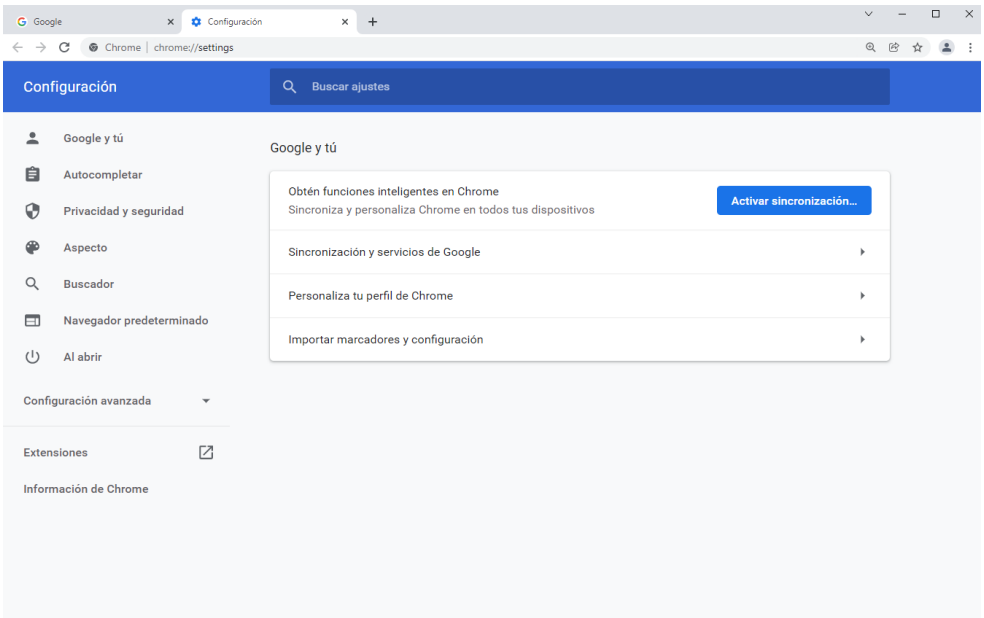
iniciar sesión en el navegador Google Chrome



1.2.2. Se accede a la sección de configuración.

Figura 88

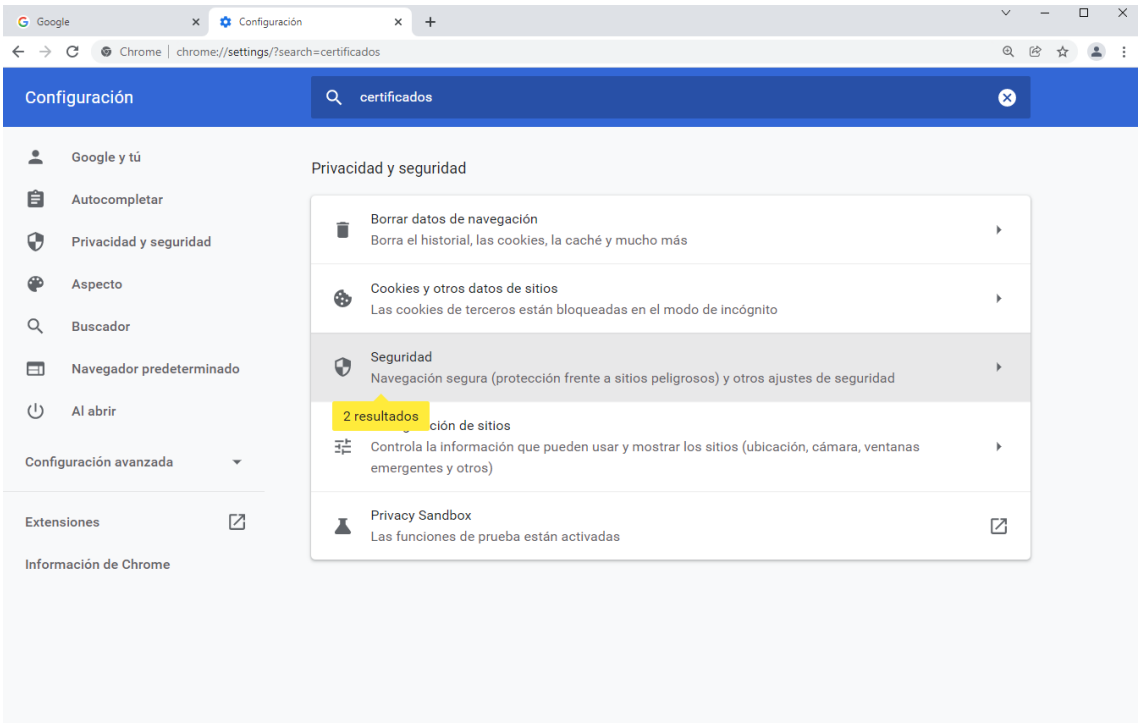
sección de configuración



1.2.3. En la barra de búsqueda se escribe la palabra certificado, en las opciones que muestra se selecciona la de Seguridad.

Figura 89

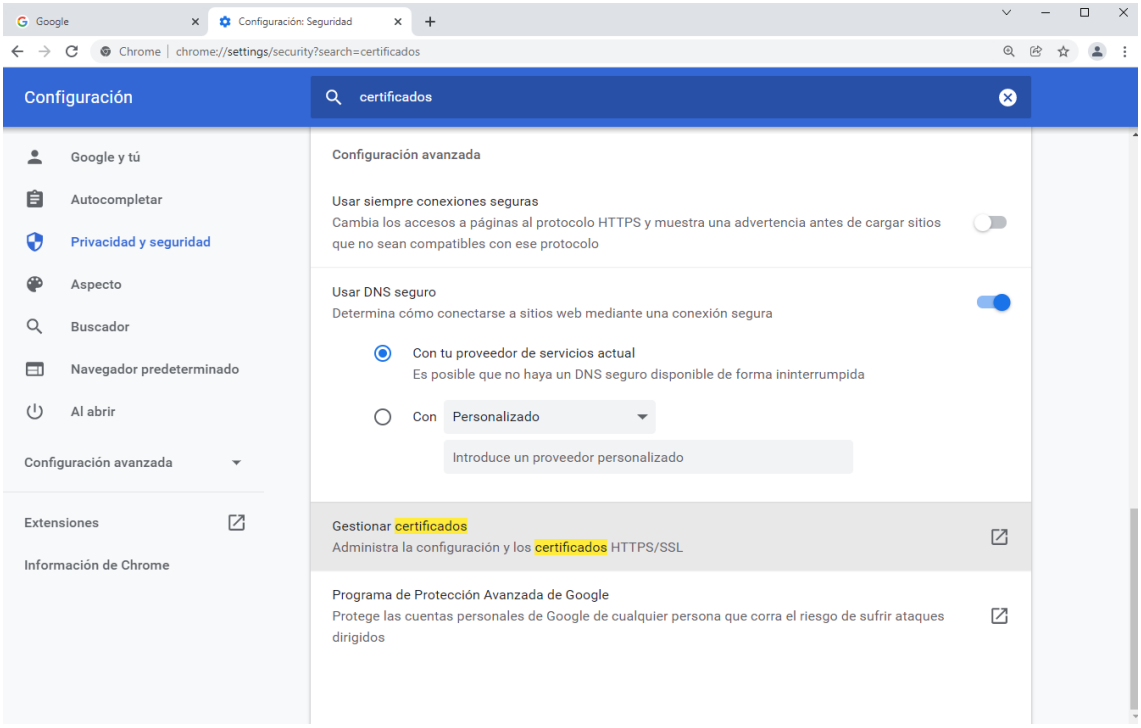
palabra certificada



1.2.4. Se despliega hasta el final y se selecciona en la opción Gestionar certificados.

Figura 90

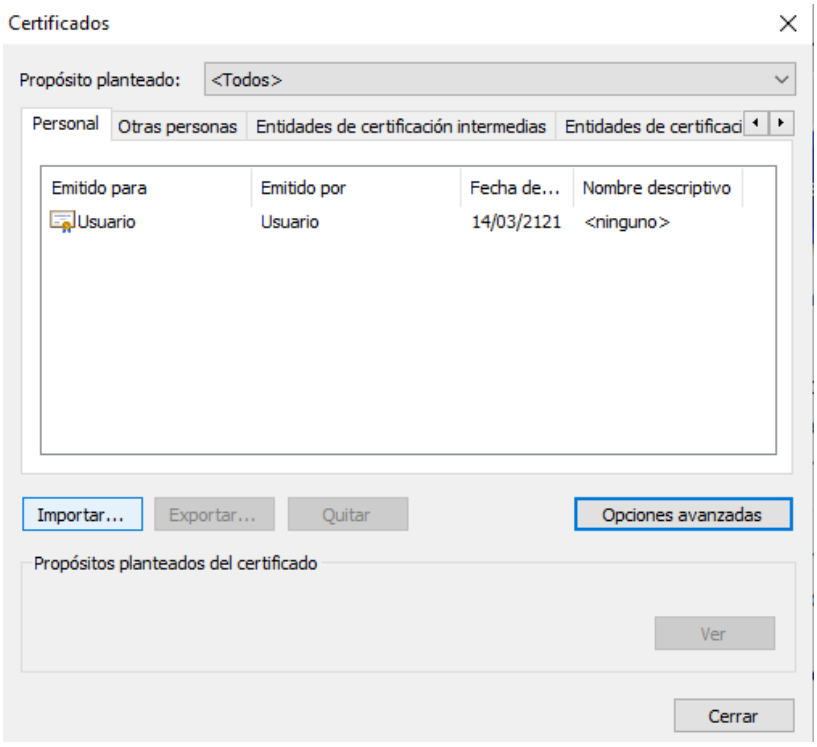
Gestionar certificados



1.2.5. Se abre la ventana de certificados y en la sección Personal se selecciona la opción Importar…

Figura 91

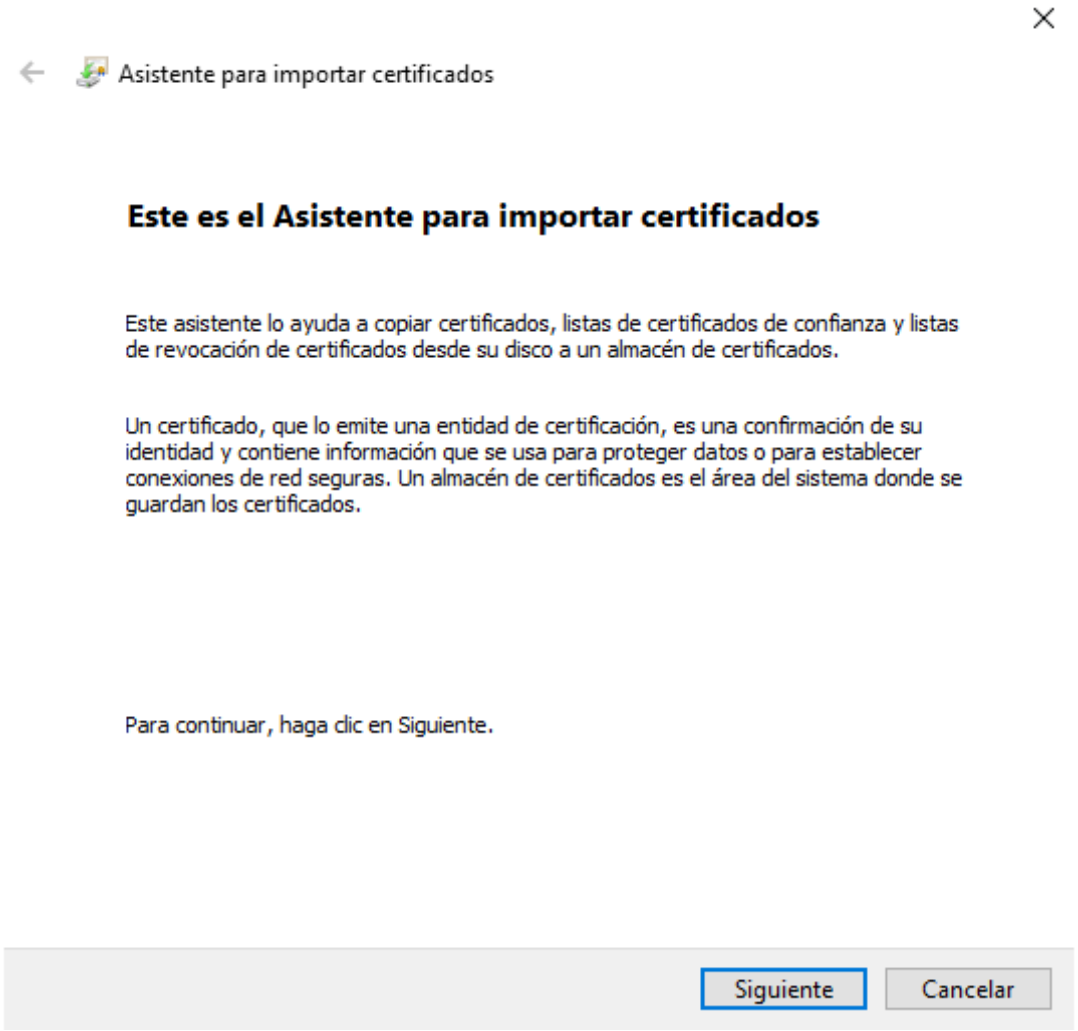
certificados y en la sección Personal se selecciona la opción Importar



1.2.6. Se da clic en siguiente.

Figura 92

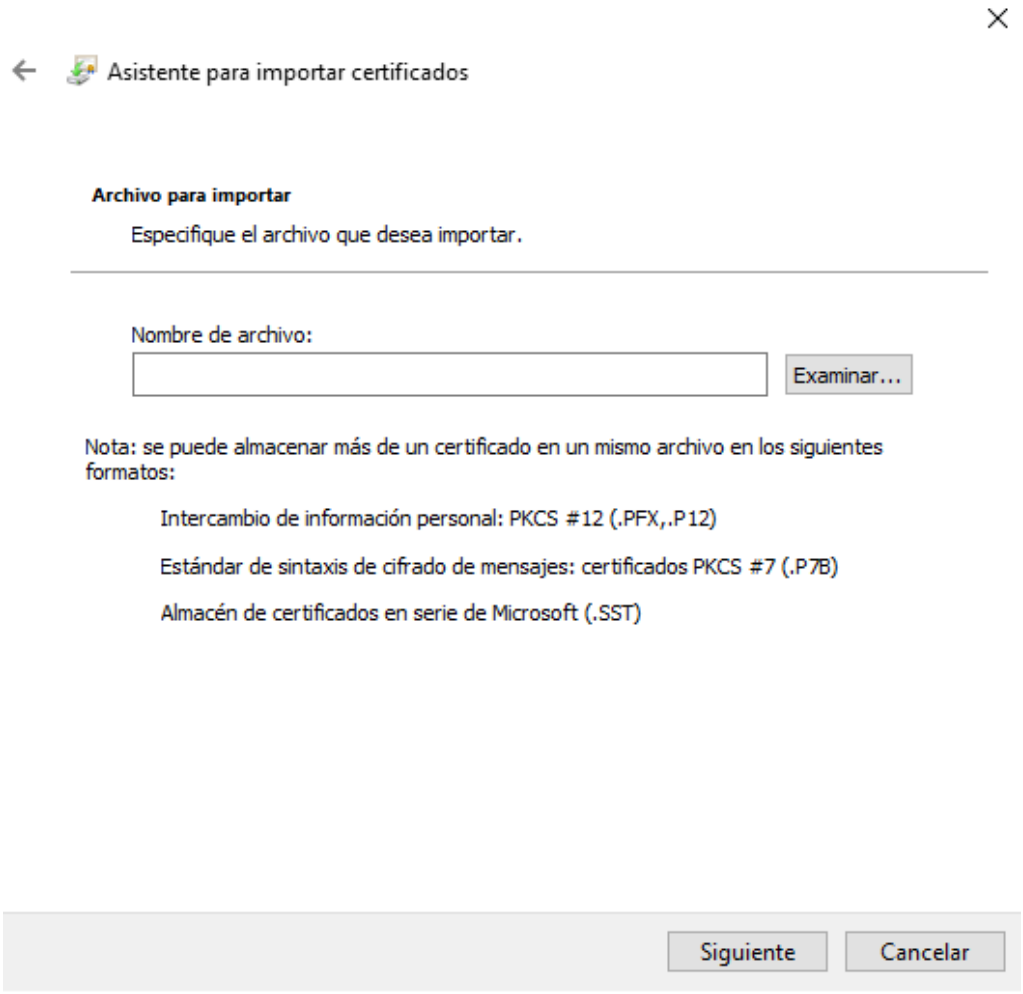
asistente para importar certificados



1.2.7. Se da clic en Examinar… para buscar el certificado digital mostrado en pasos anteriores.

Figura 93

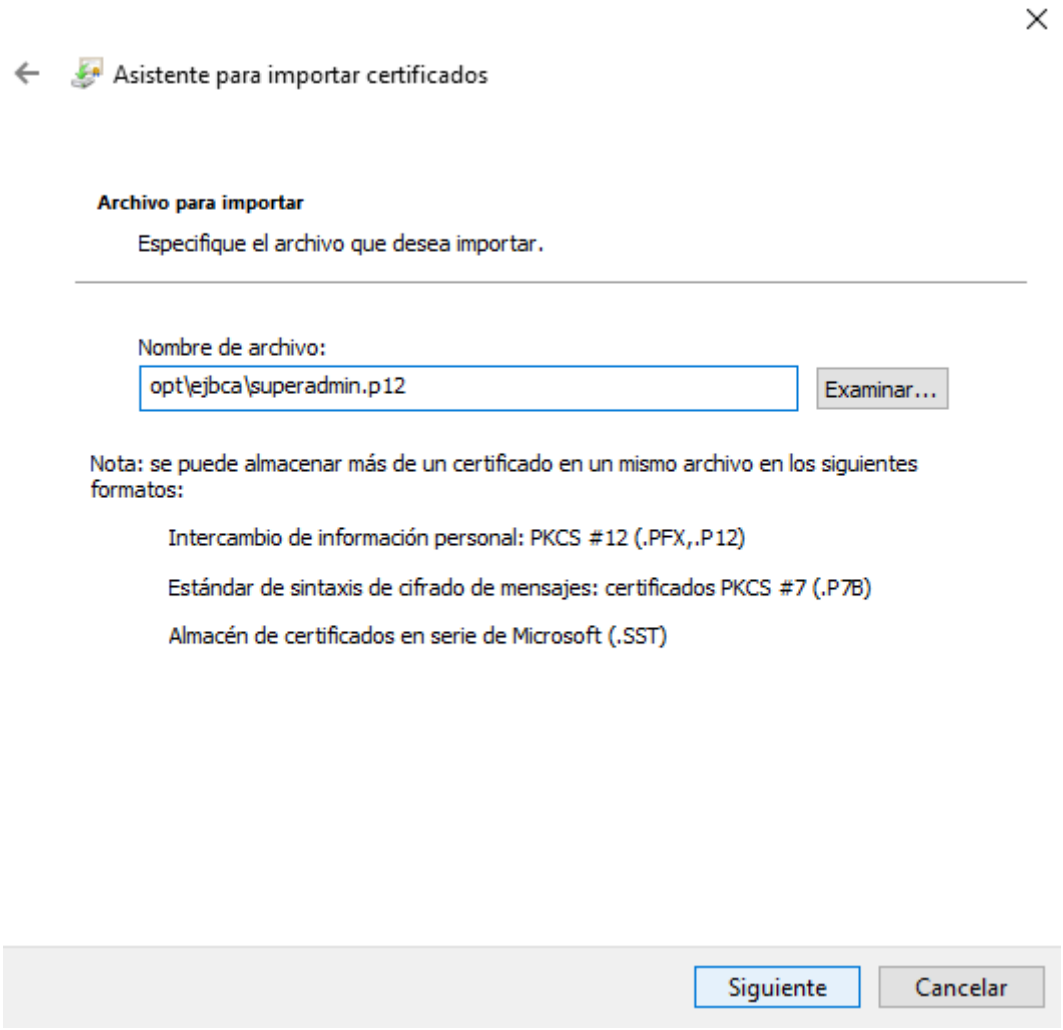
certificado digital



1.2.8. Una vez cargado el certificado se da clic en Siguiente.

Figura 94

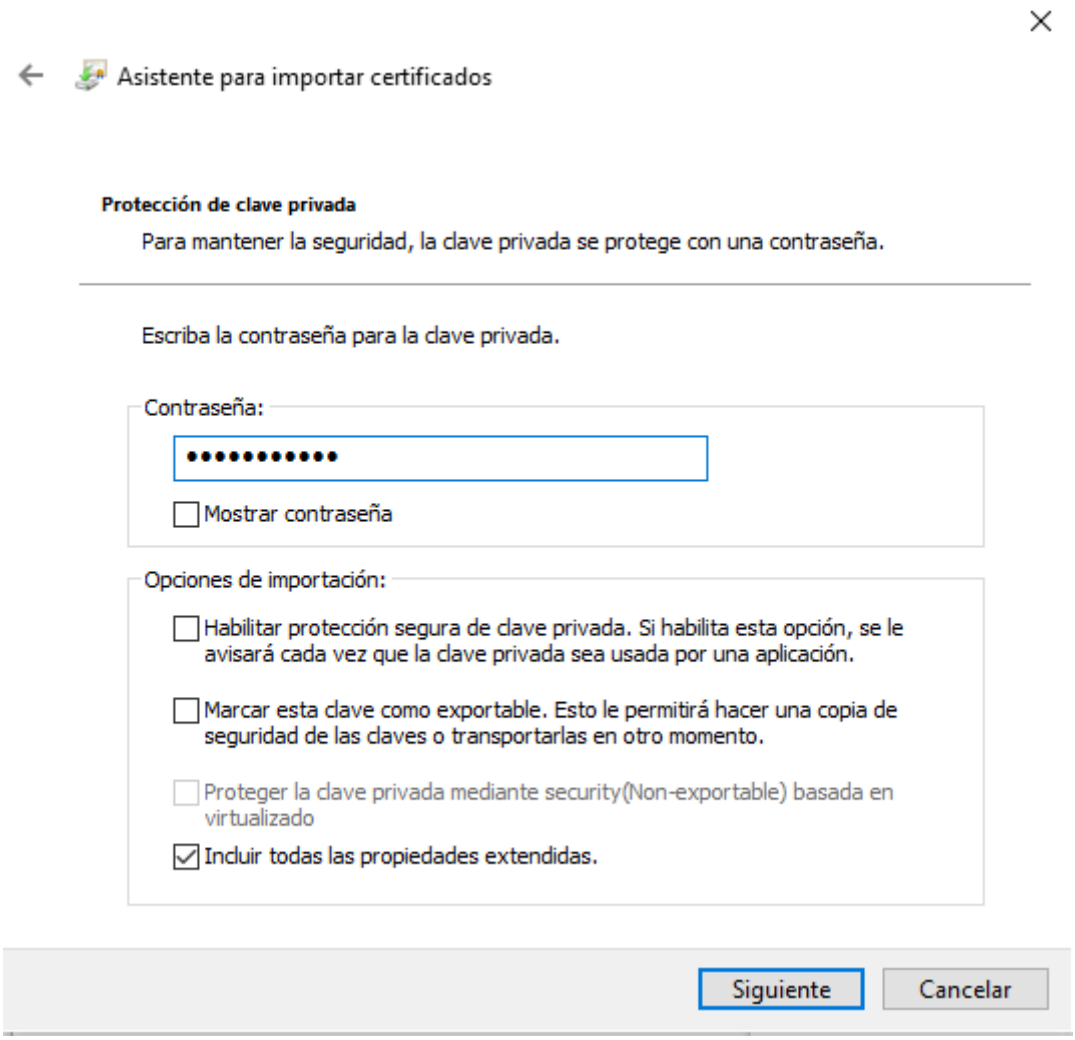
certificado cargado



1.2.9. Se ingresa la contraseña del certificado, la cual fue definida en la sección de configuración de EJBCA, y se da clic en Siguiente.

Figura 95

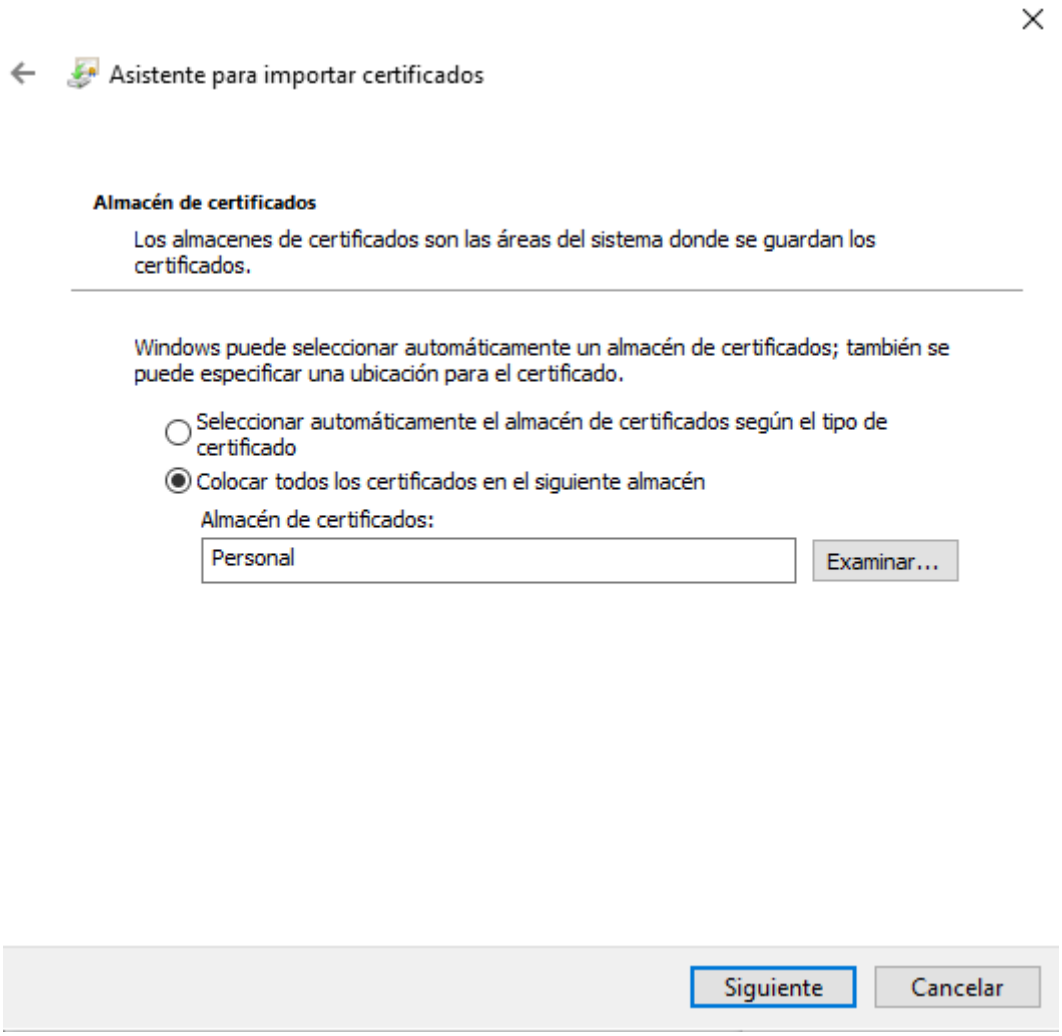
sección configuración



1.2.10. Se da clic en Siguiente para colocar el certificado en el almacén personal.

Figura 96

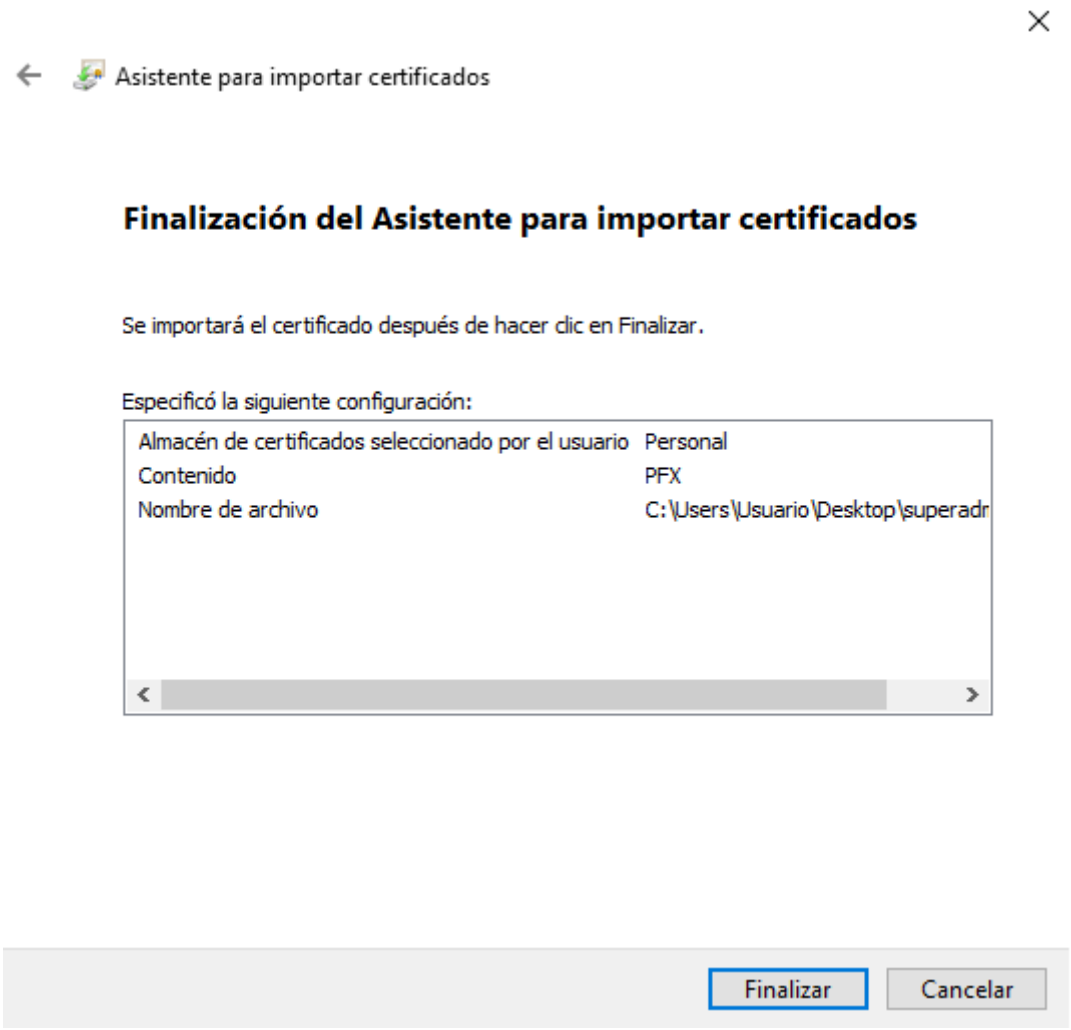
almacén de certificados



1.2.11. Se da clic en Finalizar con lo cual indica que la importación ha culminado exitosamente.

Figura 97

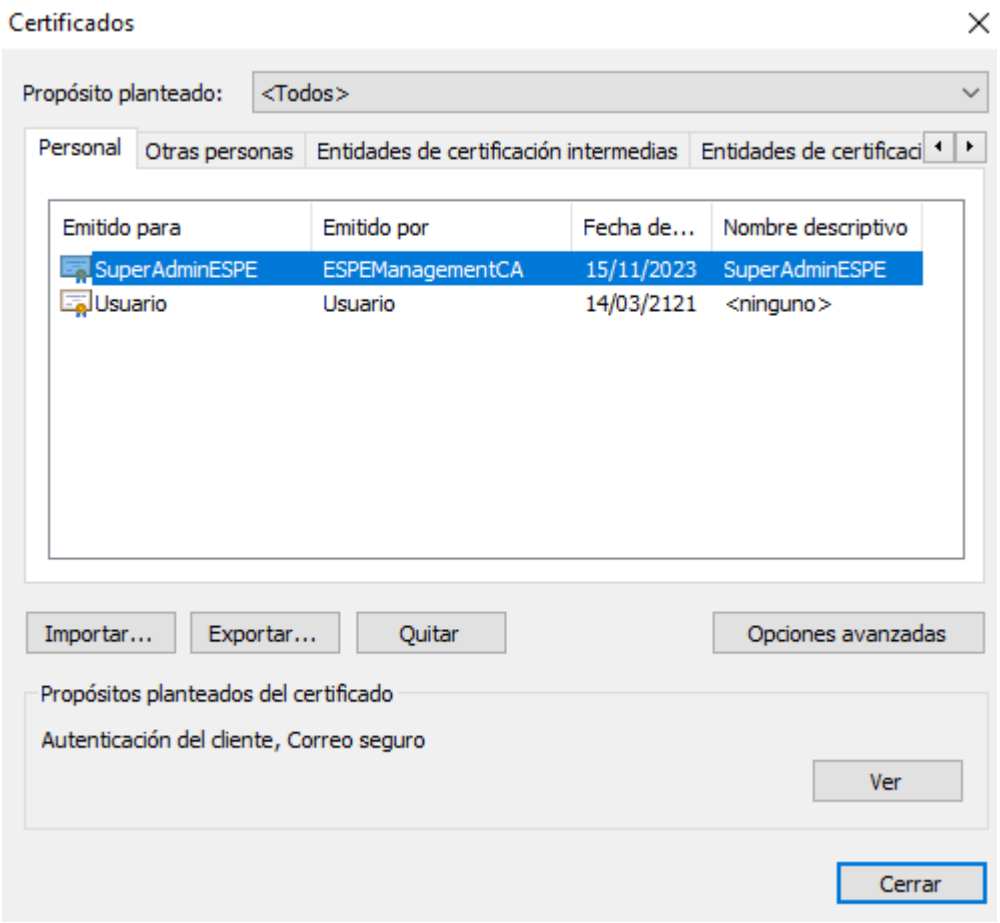
finalizar asistente certificados



1.2.12. Se verifica que el certificado ha sido cargado y se da clic en Cerrar.

Figura 98

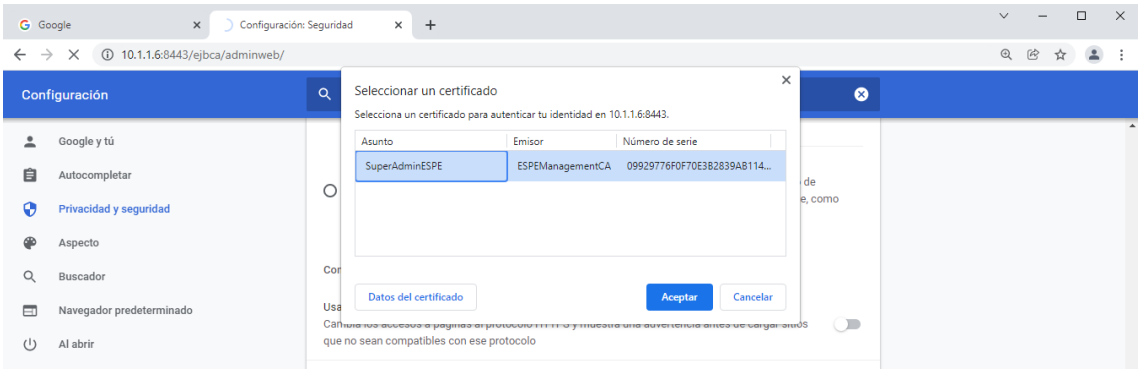
certificado cargado



1.3. Se accede al enlace (https://ip_servidor:8443/ejbca/adminweb/), automáticamente el navegador solicita un certificado para autenticar identidad, se selecciona el certificado cargado en pasos anteriores y se da clic en aceptar.

Figura 99

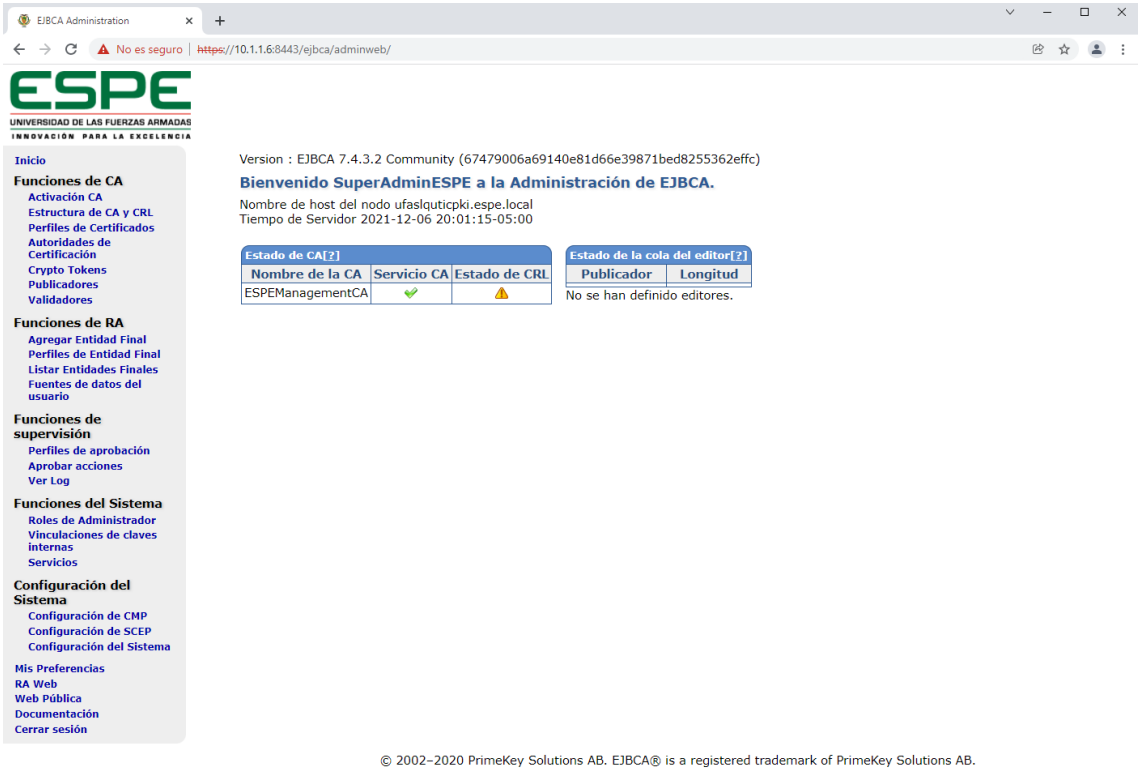
certificado cargado automáticamente



1.4. El sistema acepta el certificado seleccionado y muestra la consola con las opciones de Super Administrador.

Figura 100

opciones de Super Administrador



2. Funciones de CA

2.1. Crear Autoridad de Certificación

2.1.1. Se sitúa en el menú y se selecciona la opción Autoridad de Certificación con la finalidad de crear una.

Figura 101

funciones de CA

2.1.2. Se sitúa en la opción de Agregar CA y se ingresa el nombre de la autoridad a crear, posteriormente se da clic en el botón Crear…

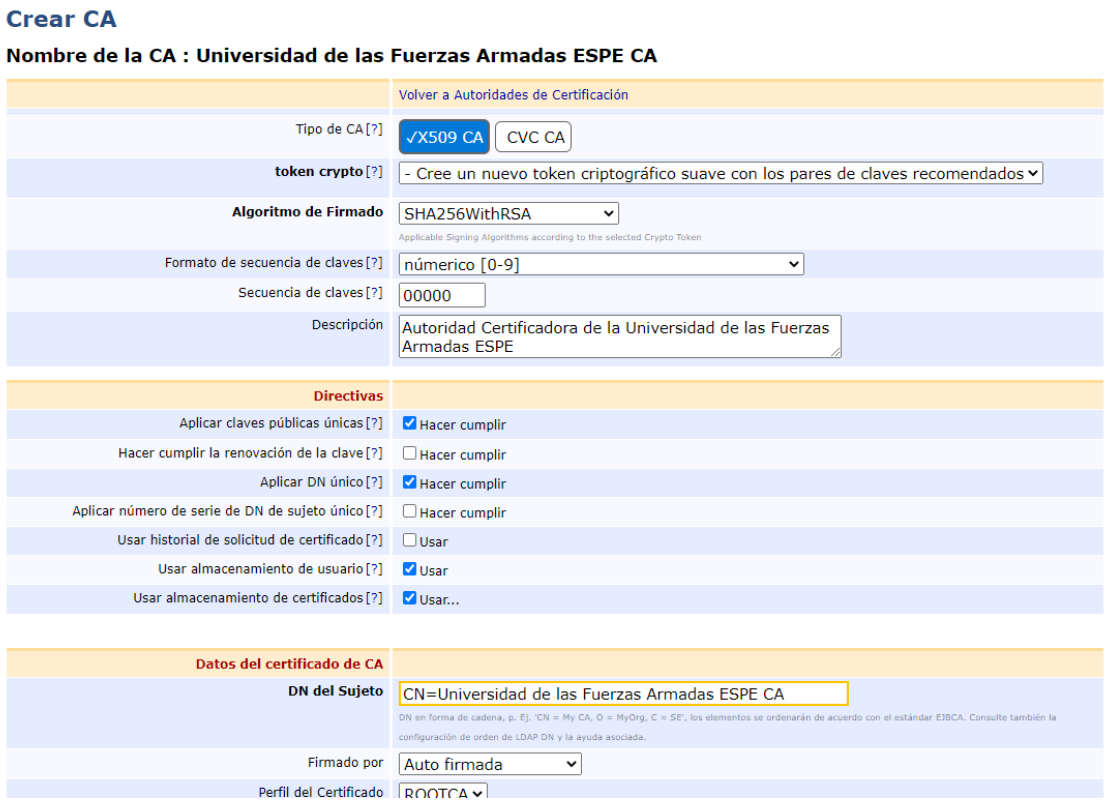
Figura 102

opción de Agregar CA

2.1.3. Se completa los datos para crear una autoridad de certificación y una vez terminado se presiona en el botón Crear al final del formulario.

Figura 103

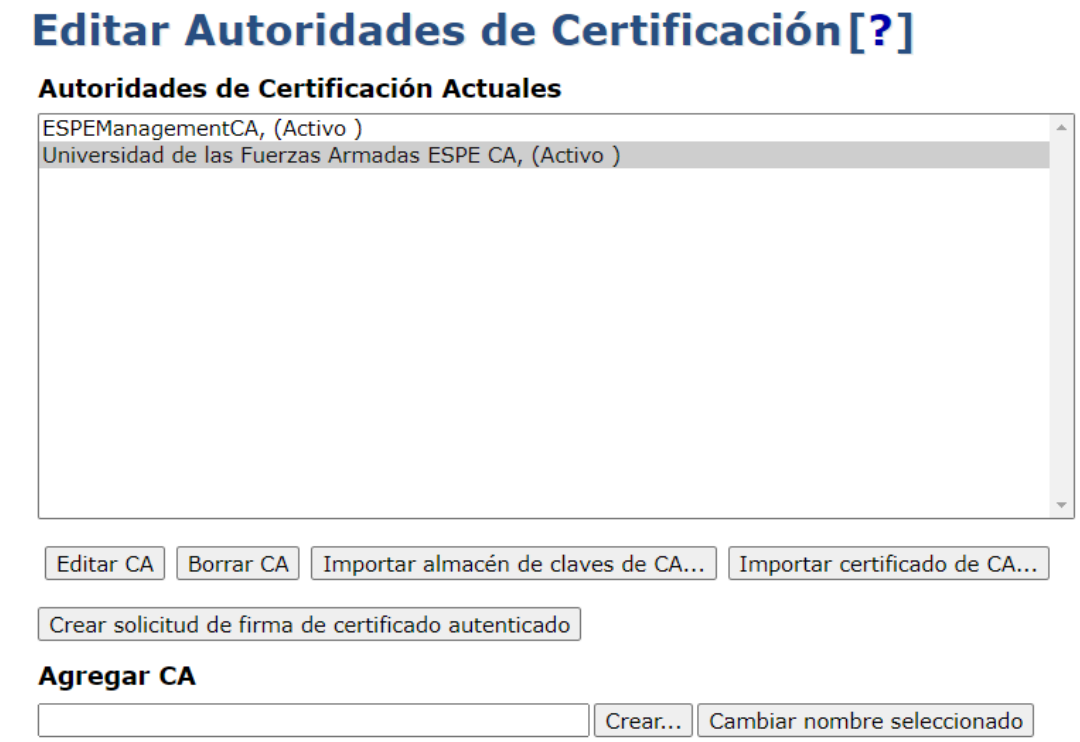
autoridad de certificación



2.1.4. Se comprueba que la Autoridad de Certificación se encuentre en la lista, lo cual significa que ha sido creada con éxito.

Figura 104

Autoridad de Certificación

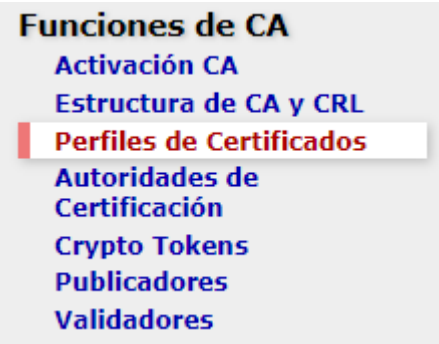


2.2. Crear Perfil de Certificado

2.2.1. Se sitúa en el menú y se selecciona la opción Perfiles de Certificado con la finalidad de crear uno.

Figura 105

Perfiles de Certificado



2.2.2. Dado que existen perfiles ya creados se puede tomar como plantillas estos por lo que para hacerlo se selecciona la opción Clonar del Perfil por defecto llamado ENDUSER.

Figura 106

opción Clonar del Perfil por defecto llamado ENDUSER

2.2.3. Se ingresa un nombre al perfil y se da clic en el botón Crear desde plantilla.

Figura 107

editar perfiles de certificados

2.2.4. Se verifica la creación del nuevo perfil y se selecciona la opción Editar.

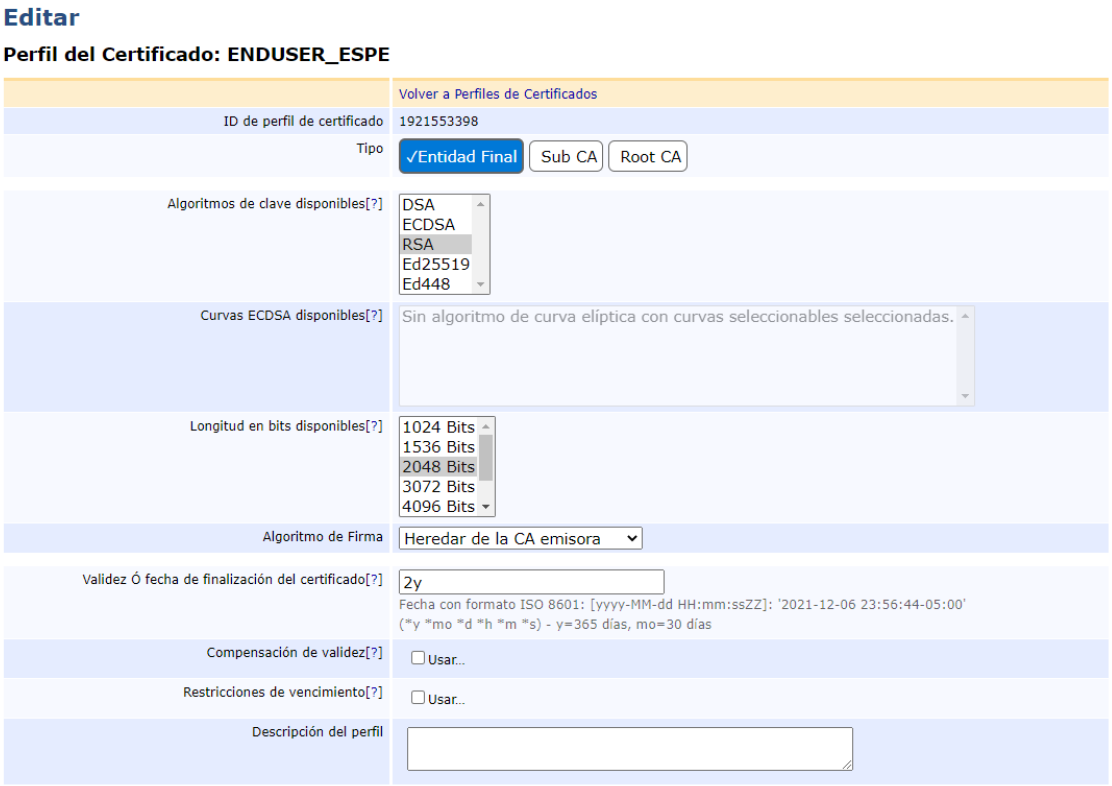
Figura 108

verifica la creación del nuevo perfil

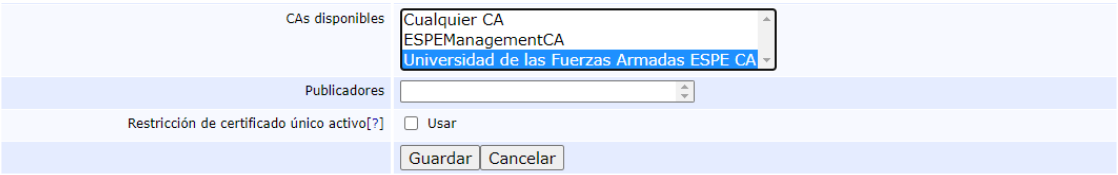
2.2.5. Se completa los datos para editar el perfil de certificado.

Figura 109

datos para editar el perfil de certificado



2.2.6. En la opción de CAs disponibles se selecciona la Autoridad de Registro creada en pasos anteriores y posteriormente se da clic en Guardar al final del formulario.



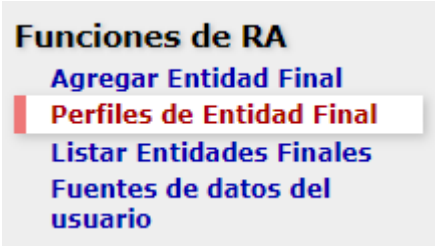
3. Funciones de RA

3.1. Agregar Perfil de Entidad Final

3.1.1. Se sitúa en el menú y se selecciona la opción Perfiles de Entidad Final con la finalidad de crear uno.

Figura 110

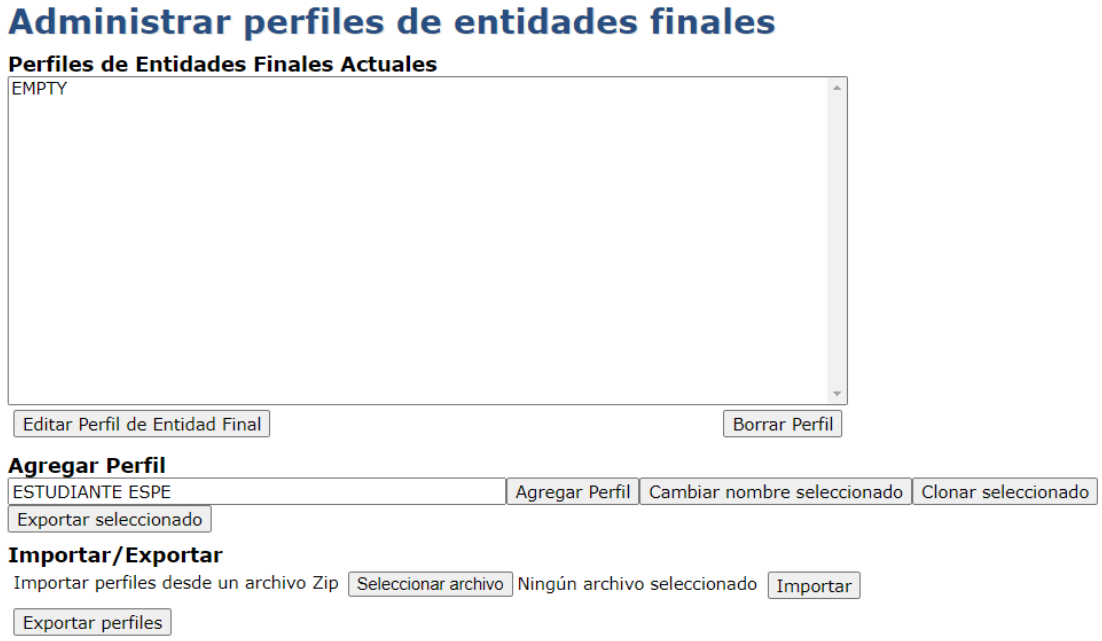
Perfil de Entidad Final



3.1.2. Se ingresa el nombre del nuevo Perfil y se da clic en el botón Agregar Perfil.

Figura 111

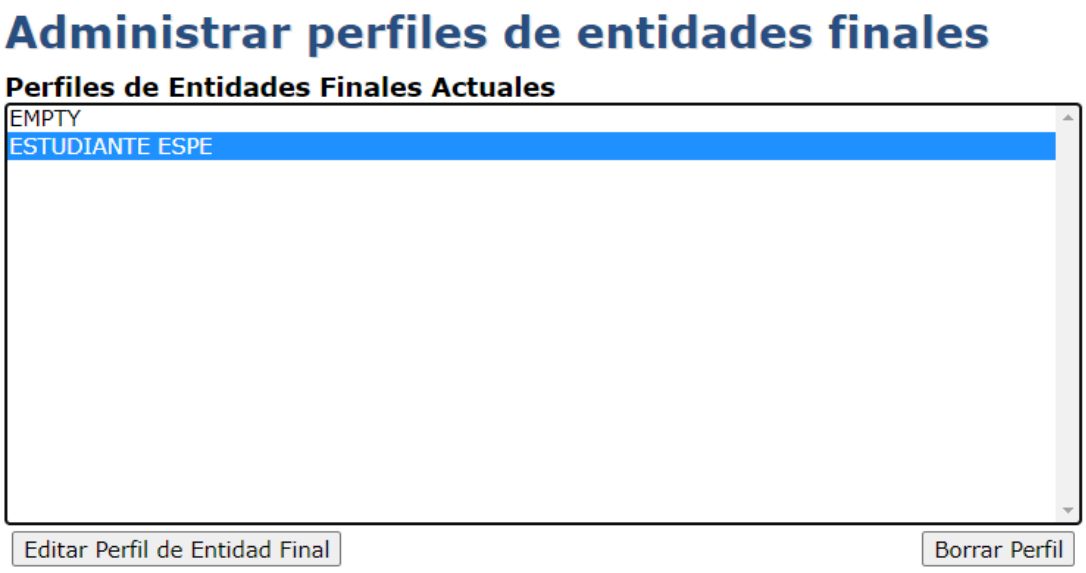
nombre del nuevo Perfil



3.1.3. En listado se selecciona el perfil agregado y se da clic en la opción Editar Perfil de Entidad Final.

Figura 112

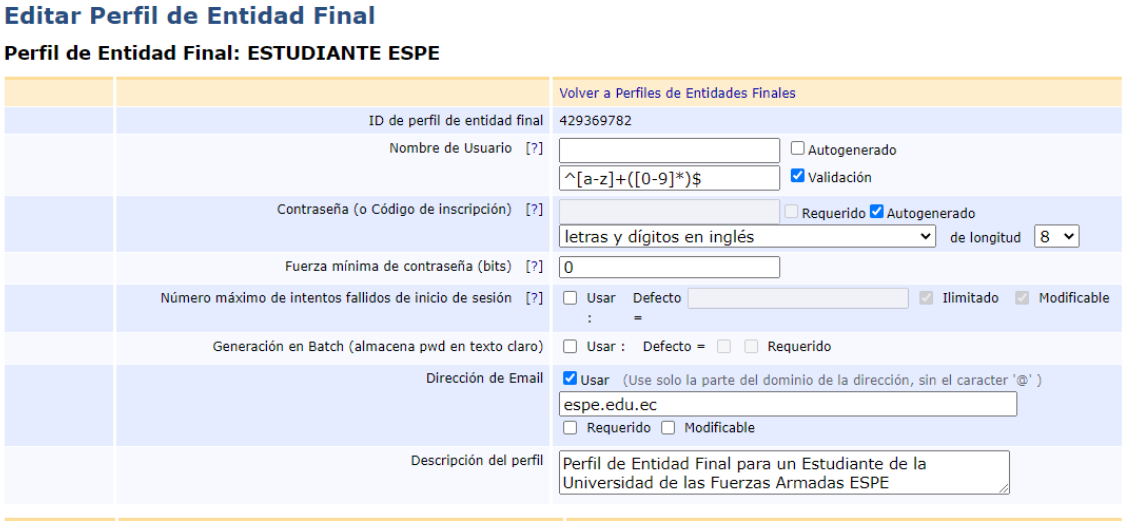
administrar perfiles



3.1.4. Primeramente se modifica los campos de validación para nombre de usuario, características de la contraseña autogenerada, dominio del correo electrónico institucional y descripción.

Figura 113

campos de validación para nombre de usuario



3.1.5. Se agrega los campos del nombre de distinción, los cuales son, nombre común, dirección de correo electrónico, identificador único y organización, cada campo cuenta con sus respectivas validaciones.

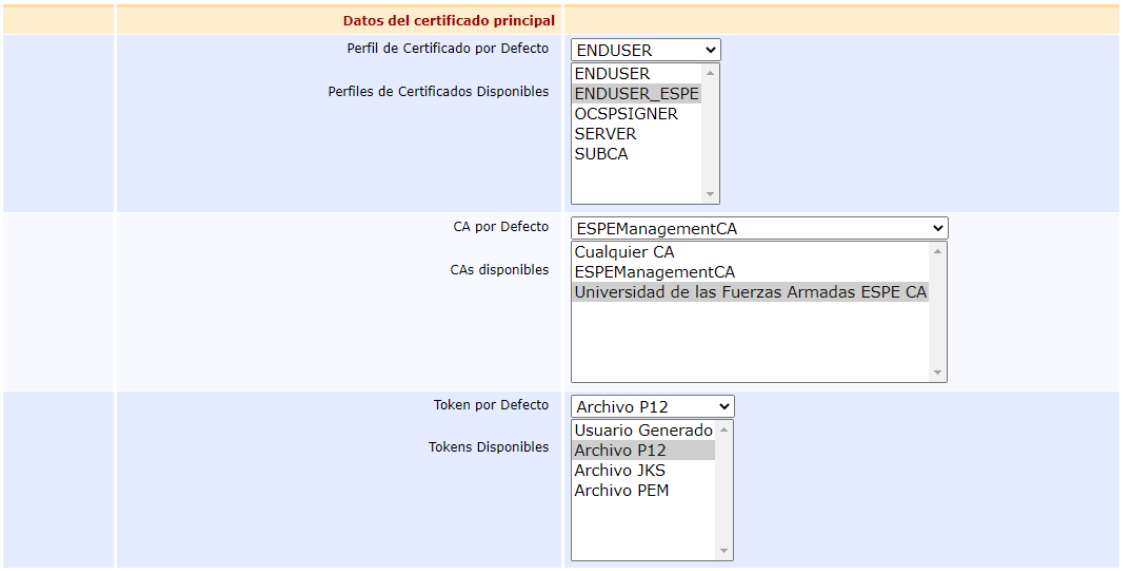
Figura 114

campos del nombre de distinción

3.1.6. Se selecciona los datos del certificado principal en los cuales se selecciona los creados en pasos anteriores.

Figura 115

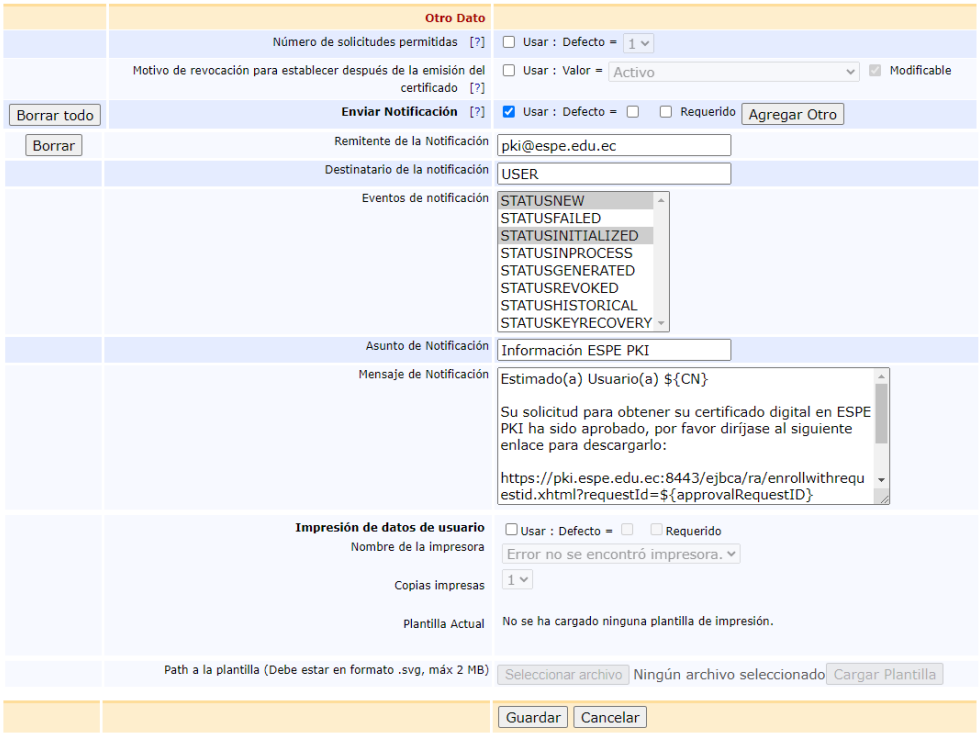
datos del certificado principal



3.1.7. Se agrega los campos para enviar notificaciones por correo electrónico y se da clic en el botón Guardar.

Figura 116

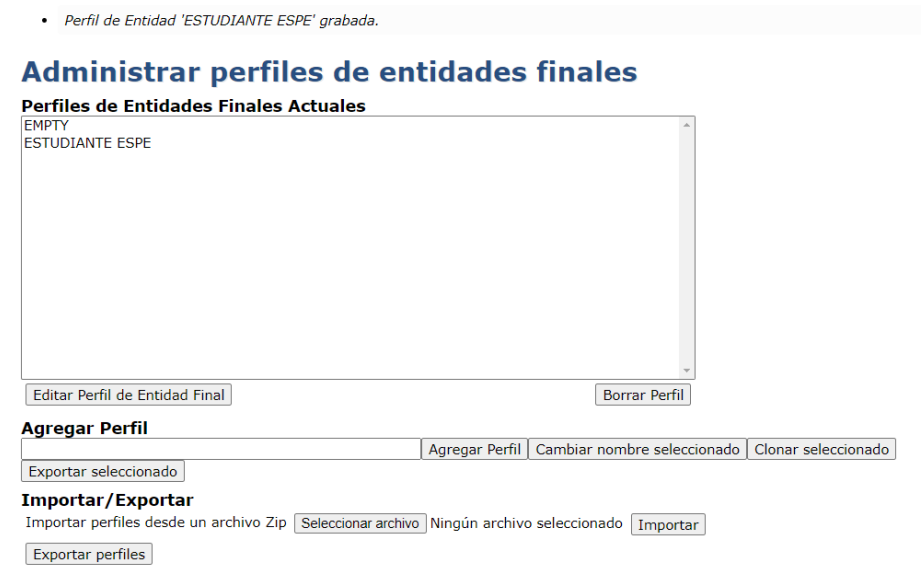
campos para enviar notificaciones



3.1.8. El sistema regresará a la pantalla de gestión de perfiles de entidades finales mostrando un mensaje qué indica que la entidad ha sido grabada.

Figura 117

pantalla de gestión de perfiles



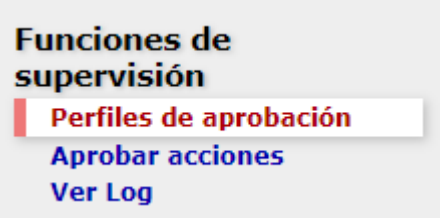
4. Funciones de supervisión

4.1. Agregar Perfil de Aprobación

4.1.1. Se sitúa en el menú y se selecciona la opción Perfiles de aprobación con la finalidad de crear uno.

Figura 118

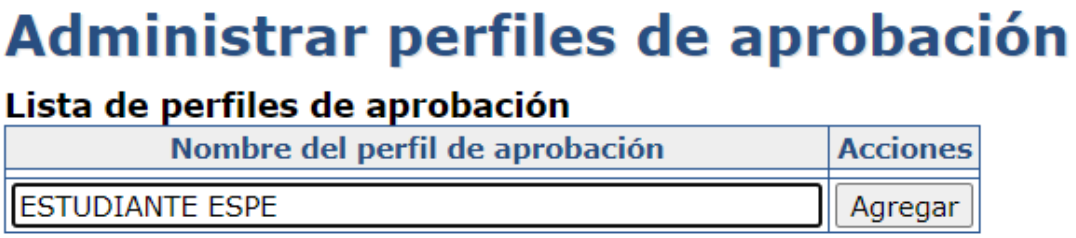
menú y selección de la opción Perfiles



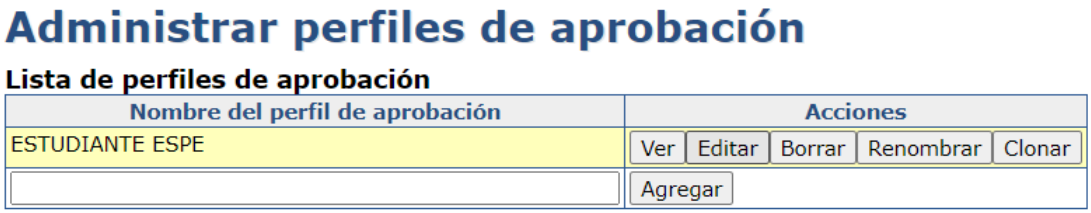
4.1.2. Se ingresa un nombre al perfil y se da clic en el botón Agregar.

Figura 119

nombre al perfil



4.1.3. El sistema crea el perfil de aprobación.



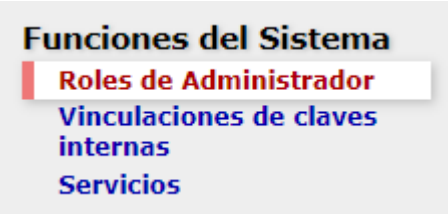
5. Funciones del Sistema

5.1. Agregar Roles

5.1.1. Se sitúa en el menú y se selecciona la opción Roles de Administración con la finalidad de crear uno.

Figura 120

funciones del sistema



5.1.2. Se selecciona la opción de Agregar.

Figura 121

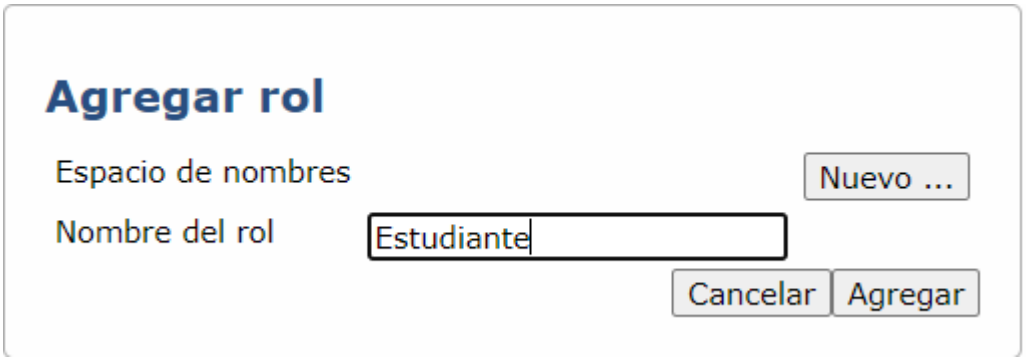
privilegios de administrador

5.1.3. Agregar Rol de Estudiante

5.1.3.1. Se ingresa el nombre al rol de Estudiante y se pulsa en el botón Agregar.

Figura 122

Agregar Rol de Estudiante



5.1.3.2. El sistema muestra el mensaje de Rol Agregado y se procede a dar clic en la opción Miembros.

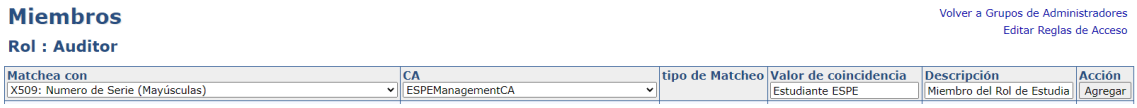
Figura 123

rol agregado

5.1.3.3. Se agrega los campos para crear un miembro que iguale con el valor de nombre común del certificado que se creará en pasos posteriores, por último se presiona el botón Agregar.

Figura 124

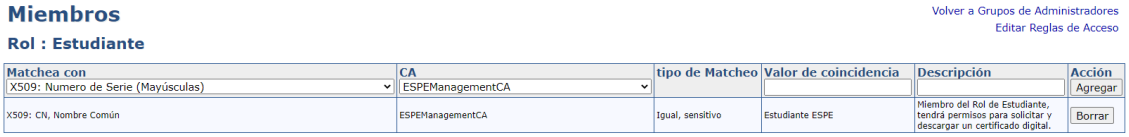
campos para crear un miembro



5.1.3.4. El sistema muestra el miembro agregado, se da clic en la opción Editar Reglas de Acceso.

Figura 125

miembro agregado

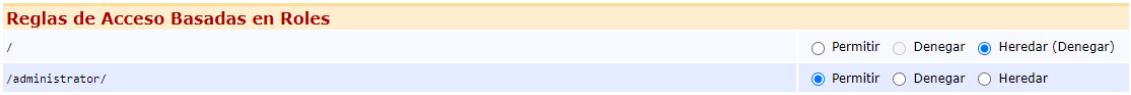


5.1.3.5. Se selecciona la opción Modo Avanzado para editar las reglas de Acceso para el Rol Estudiante.

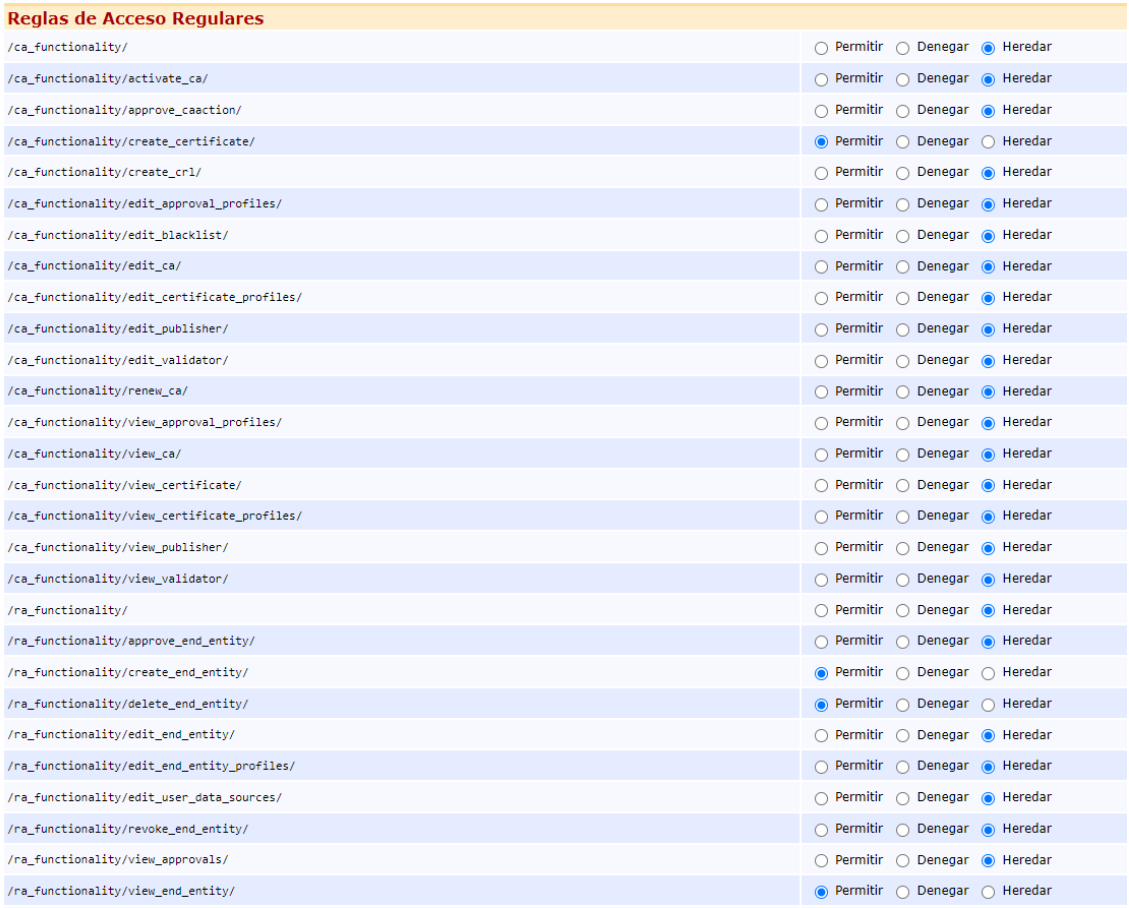
5.1.3.6. En la sección de Reglas de Acceso Basadas en Roles se agrega permisos de administrador.

Figura 126

opción Modo Avanzado



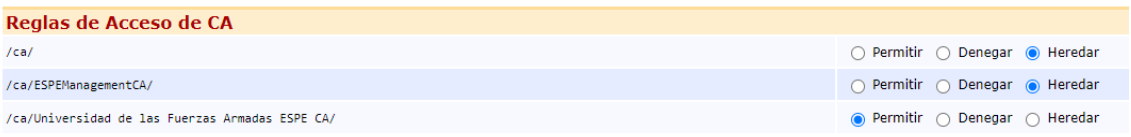
5.1.3.7. En la sección de Reglas de Acceso Regulares se agrega permisos de crear certificado, crear entidad final, eliminar entidad y ver entidad final.



5.1.3.8. En la sección de Reglas de Acceso de Autoridad de Certificación se permite el acceso a la autoridad creada en pasos anteriores.

Figura 127

Reglas de Acceso de Autoridad



5.1.3.9. En la sección de Reglas de Acceso de Perfiles de Entidades Finales se agrega permisos de crear entidad final y ver entidad final del perfil de Estudiante creado en pasos anteriores.

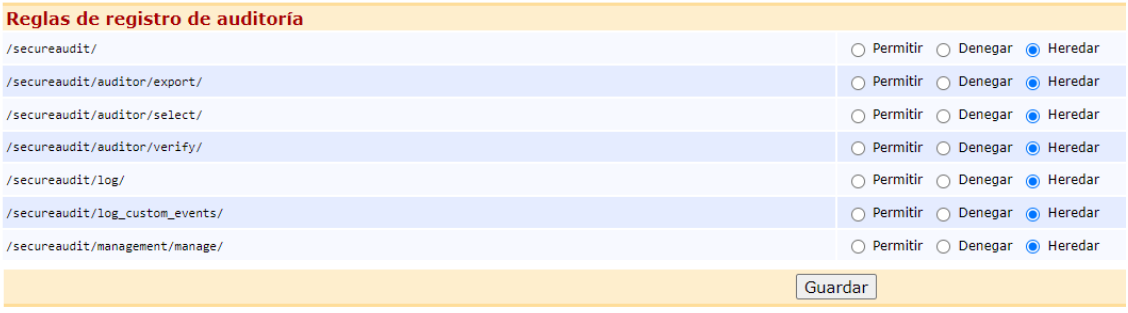
Figura 128

Reglas de Acceso de Perfiles de Entidades

5.1.3.10. Se deja todas las demás opciones por defecto en Heredar y se da clic en Guardar al final del formulario.

Figura 129

opciones por defecto en Heredar

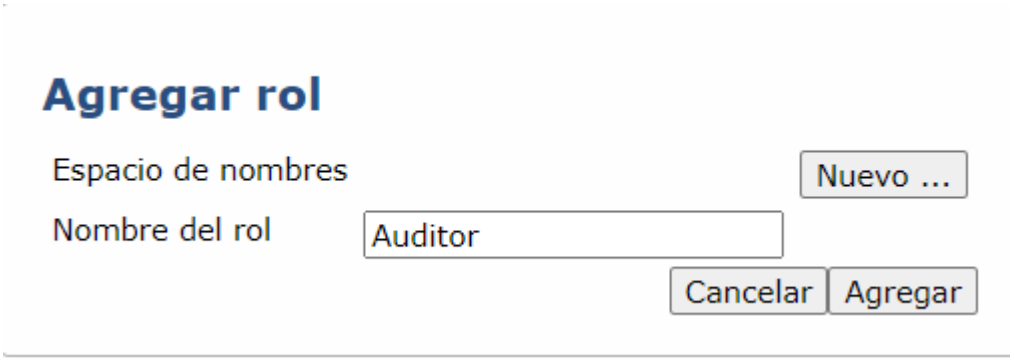


5.1.4. Agregar Rol de Auditor.

5.1.4.1. Se ingresa el nombre al rol de Auditor y se pulsa en el botón Agregar.

Figura 130

nombre al rol de Auditor



5.1.4.2. El sistema muestra el mensaje de Rol Agregado y se procede a dar clic en la opción Miembros.

Figura 131

mensaje de Rol Agregado

5.1.4.3. Se agrega los campos para crear un miembro que iguale con el valor de nombre común del certificado que se creará en pasos posteriores, por último se presiona el botón Agregar.

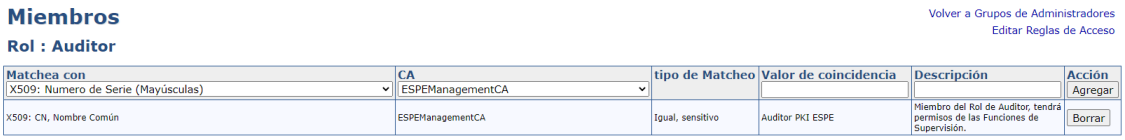
Figura 132

crear un miembro

5.1.4.4. El sistema muestra el miembro agregado, se da clic en la opción Editar Reglas de Acceso.

Figura 133

miembro agregado



5.1.4.5. Se selecciona la opción de Auditor en el campo de Plantilla de rol, se selecciona la Autoridad de Certificación creada en pasos anteriores como la única autorizada para este rol y se selecciona el perfil de entidad final correspondiente, por último se da clic en el botón Guardar.

Figura 134

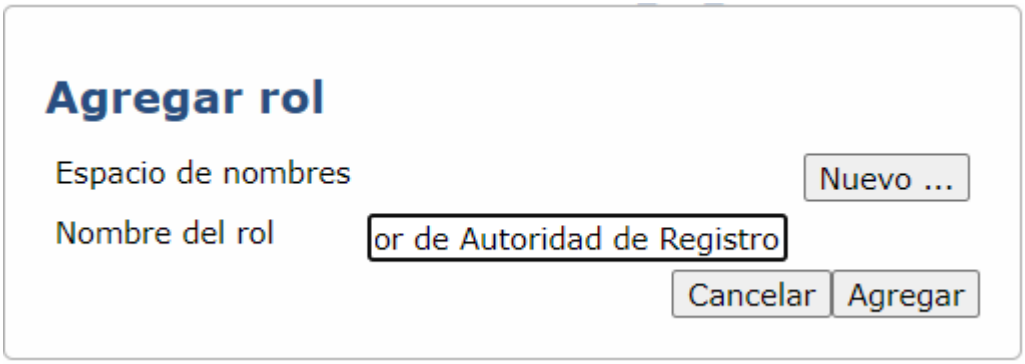
opción de Auditor en el campo

5.1.5. Agregar Rol de Administrador de Autoridad de Registro.

5.1.5.1. Se ingresa el nombre al rol de Administrador de Autoridad de Registro y se pulsa en el botón Agregar.

Figura 135

Rol de Administrador de Autoridad de Registro



5.1.5.2. El sistema muestra el mensaje de Rol Agregado y se procede a dar clic en la opción Miembros.

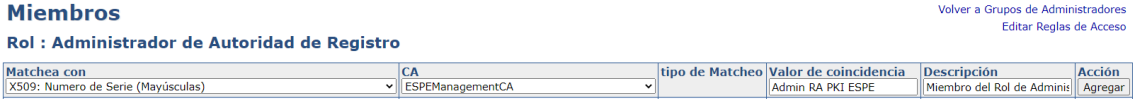
Figura 136

Mensaje de Rol Agregado

5.1.5.3. Se agrega los campos para crear un miembro que iguale con el valor de nombre común del certificado que se creará en pasos posteriores, por último se presiona el botón Agregar.

Figura 137

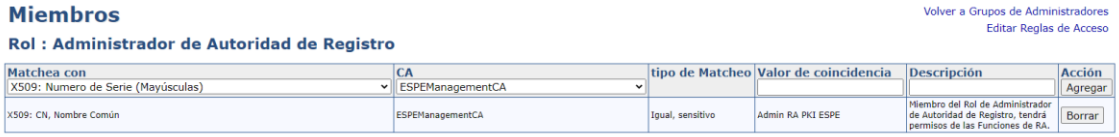
campos para crear un miembro



5.1.5.4. El sistema muestra el miembro agregado, se da clic en la opción Editar Reglas de Acceso.

Figura 138

sistema muestra el miembro agregado



5.1.5.5. Se selecciona la opción de Administradores de RA en el campo de Plantilla de rol, se selecciona la Autoridad de Certificación creada en pasos anteriores como la única autorizada para este rol y se selecciona el perfil de entidad final correspondiente, por último se da clic en el botón Guardar.

Figura 139

opción de Administradores de RA

5.1.6. Agregar Rol de Administrador de Autoridad de Certificación.

5.1.6.1. Se ingresa el nombre al rol de Administrador de Autoridad de Certificación y se pulsa en el botón Agregar.

Figura 140

nombre al rol de Administrador de Autoridad de Certificación

5.1.6.2. El sistema muestra el mensaje de Rol Agregado y se procede a dar clic en la opción Miembros.

Figura 141

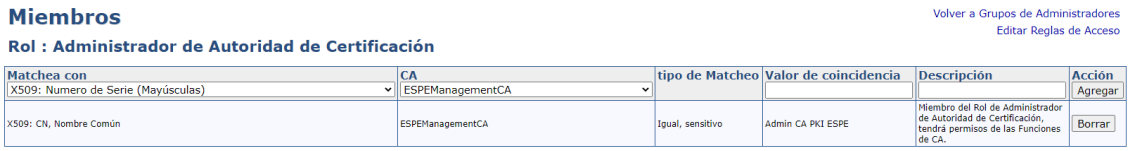
mensaje de Rol Agregado

5.1.6.3. Se agrega los campos para crear un miembro que iguale con el valor de nombre común del certificado que se creará en pasos posteriores, por último se presiona el botón Agregar.

Figura 142

campos para crear un miembro

5.1.6.4. El sistema muestra el miembro agregado, se da clic en la opción Editar Reglas de Acceso.



5.1.6.5. Se selecciona la opción de Administradores de CA en el campo de Plantilla de rol, se selecciona la Autoridad de Certificación creada en pasos anteriores como la única autorizada para este rol, por último se da clic en el botón Guardar.

Figura 143

campos para crear un miembro

6. Web de Autoridad de Registro.

6.1. Crear Entidad Final para los Roles creados.

6.1.1. Se sitúa en el menú y se selecciona la opción RA Web con la finalidad de acceder a la consola de Autoridad de Registro.

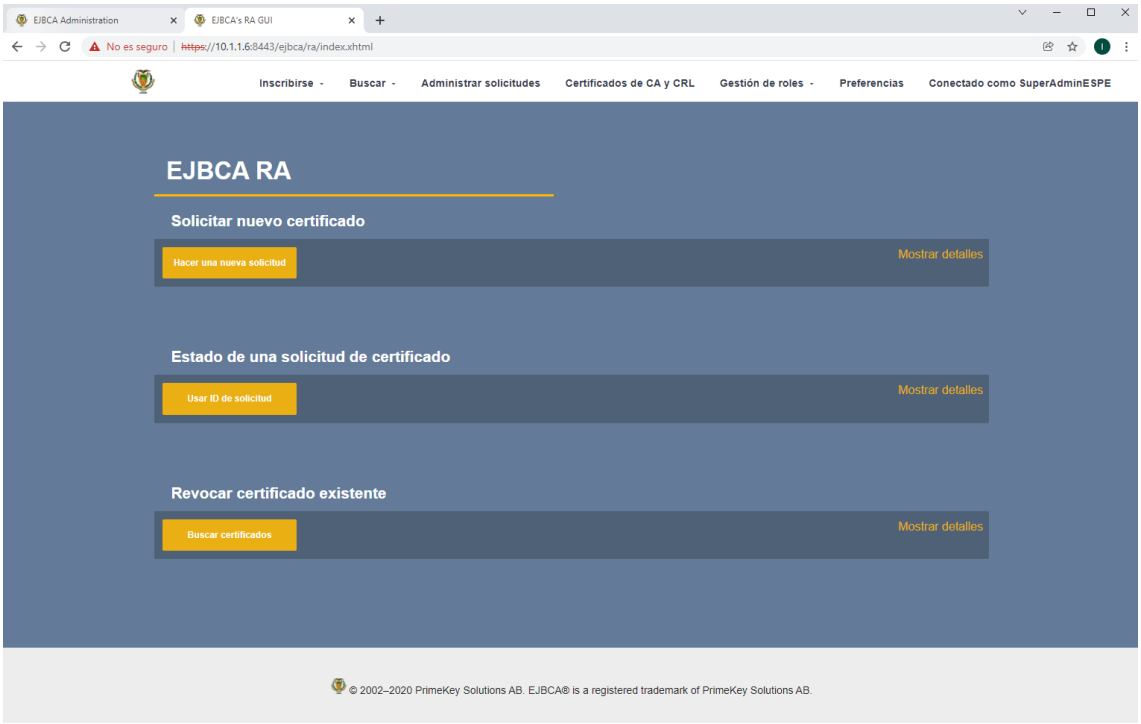
Figura 144

Web de Autoridad de Registro

6.1.2. El sistema redirige a la consola de Autoridad de Registro, posteriormente se pulsa en Hacer una nueva solicitud.

Figura 145

sistema redirige a la consola de Autoridad

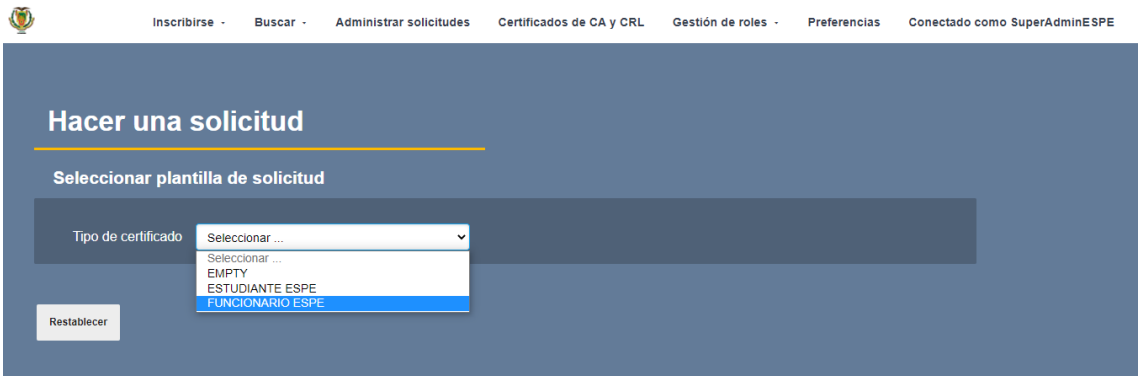


6.1.3. Entidad Final de Auditor

6.1.3.1. Se selecciona el tipo de certificado de FUNCIONARIO ESPE.

Figura 146

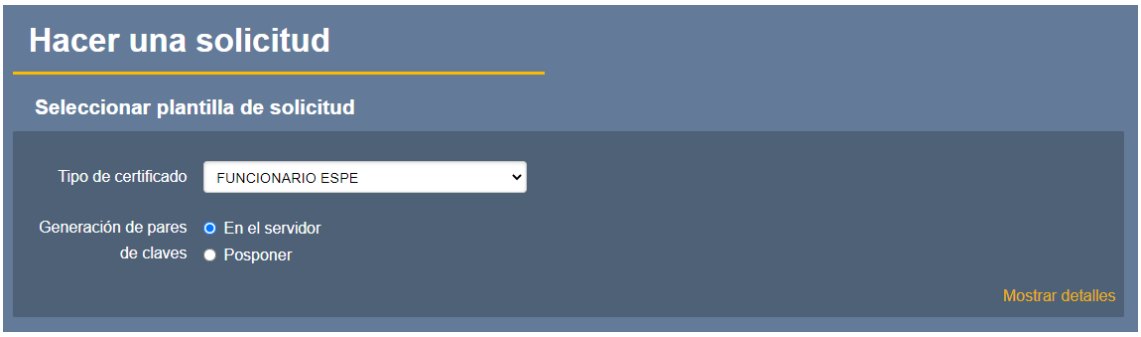
entidad final de auditor



6.1.3.2. Se marca la casilla de En el servidor para la Generación de pares de clave.

Figura 147

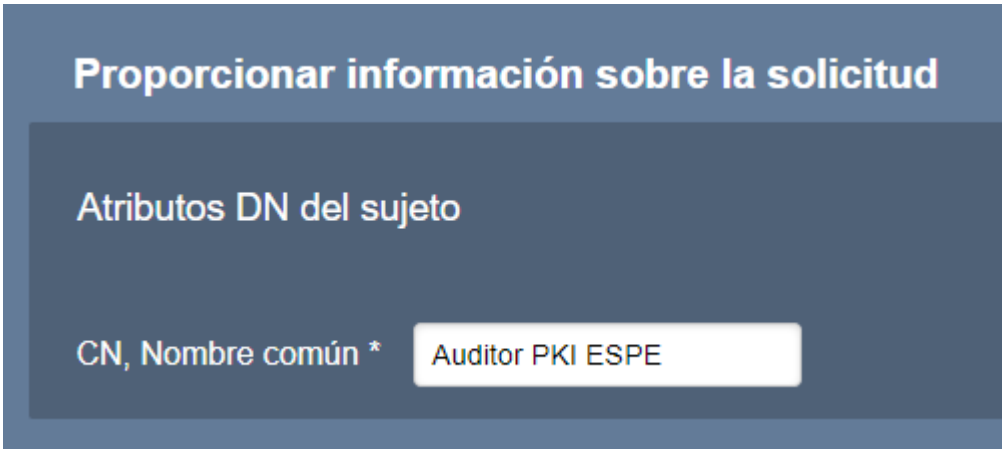
casilla para la generación de pares clave



6.1.3.3. Se ingresa los Atributos del nombre de distinción del sujeto.

Figura 148

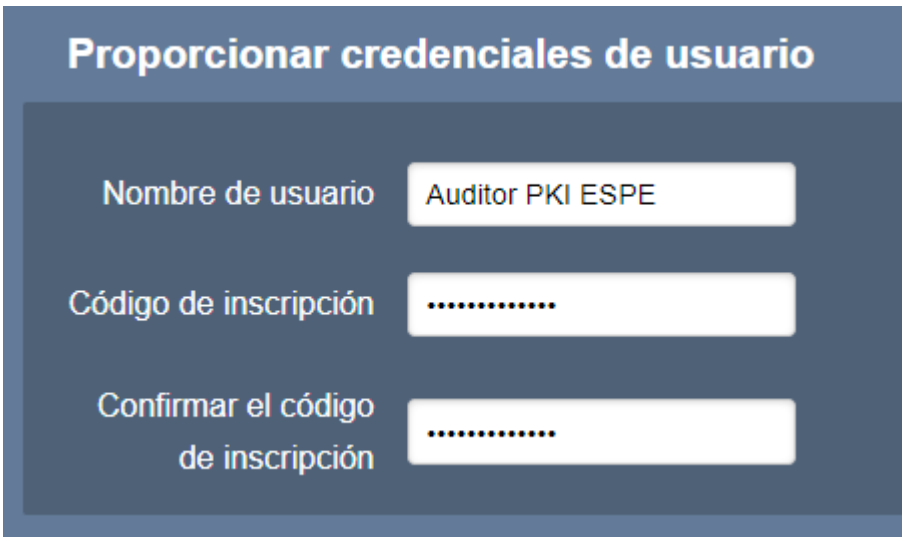
Atributos del nombre de distinción



6.1.3.4. Se proporciona las credenciales de usuario.

Figura 149

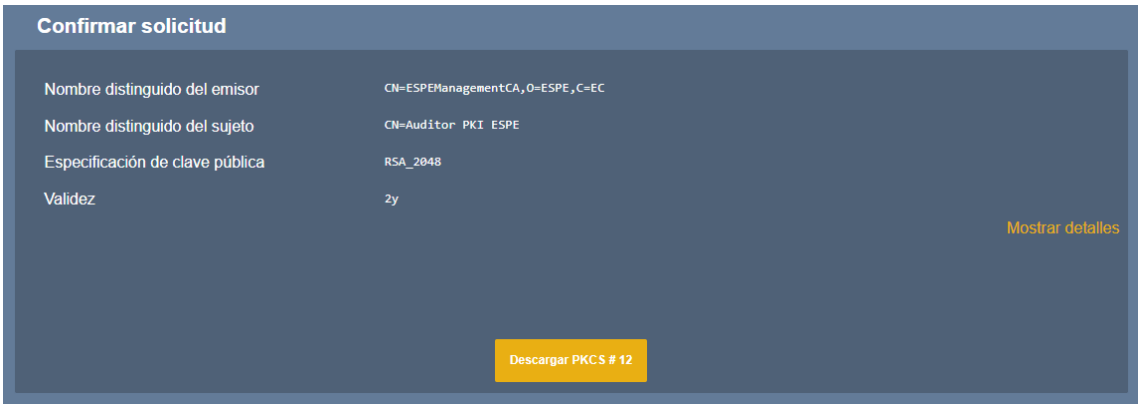
credenciales de usuario



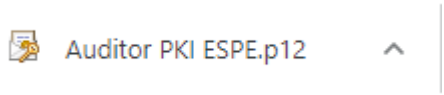
6.1.3.5. Se verifica los datos ingresados de la solicitud y se presiona en Descargar PKCS # 12.

Figura 150

datos ingresados de la solicitud



6.1.3.6. El sistema descarga inmediatamente el certificado digital en el formato seleccionado.

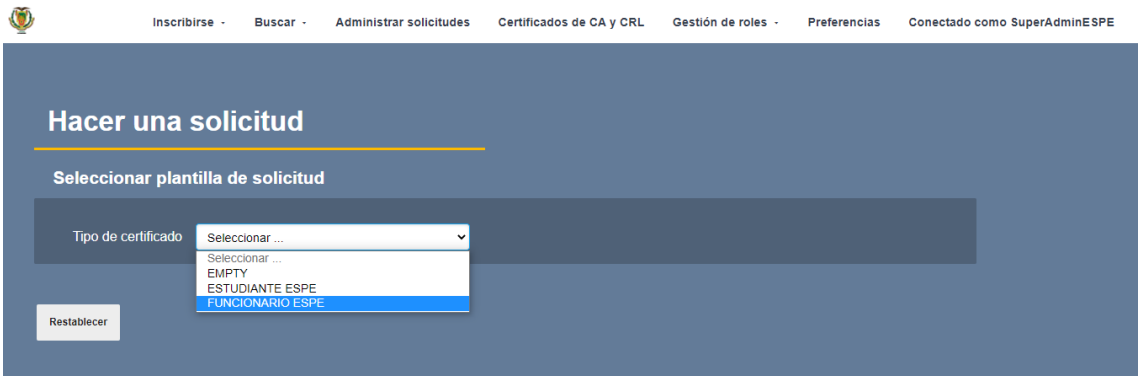


6.1.4. Entidad Final de Autoridad de Registro

6.1.4.1. Se selecciona el tipo de certificado de FUNCIONARIO ESPE.

Figura 151

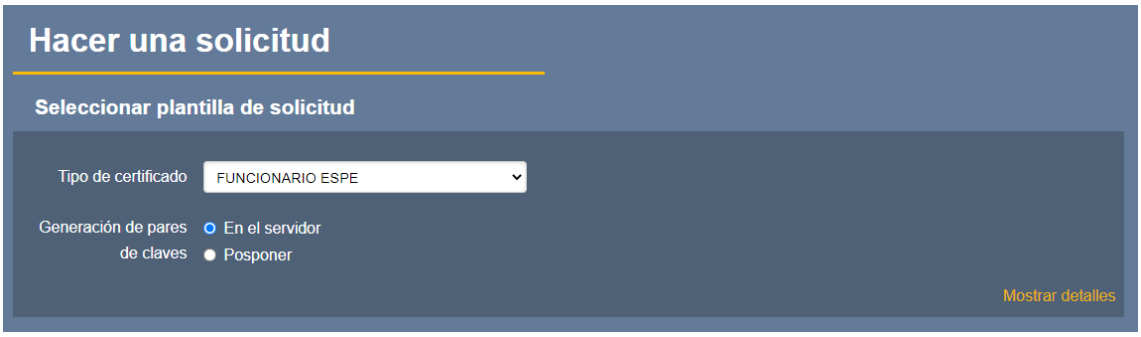
Entidad Final de Autoridad de Registro



6.1.4.2. Se marca la casilla de En el servidor para la Generación de pares de clave.

Figura 152

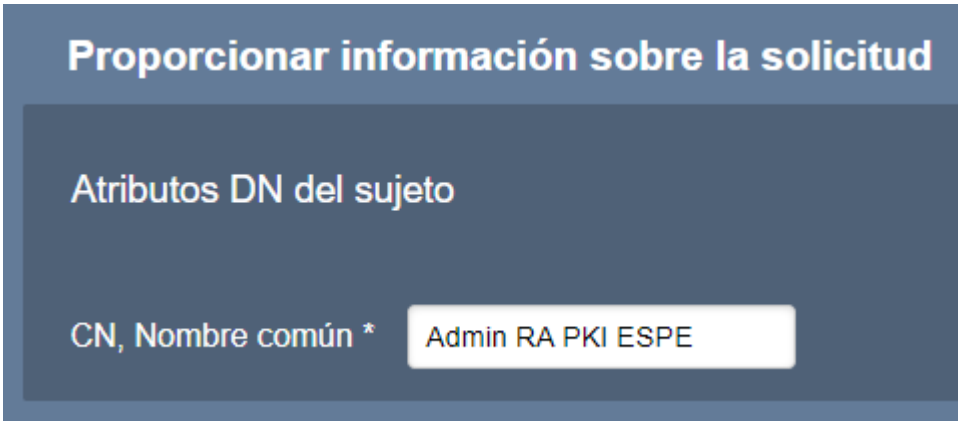
casilla de En el servidor para la Generación de pares de clave



6.1.4.3. Se ingresa los Atributos del nombre de distinción del sujeto.

Figura 153

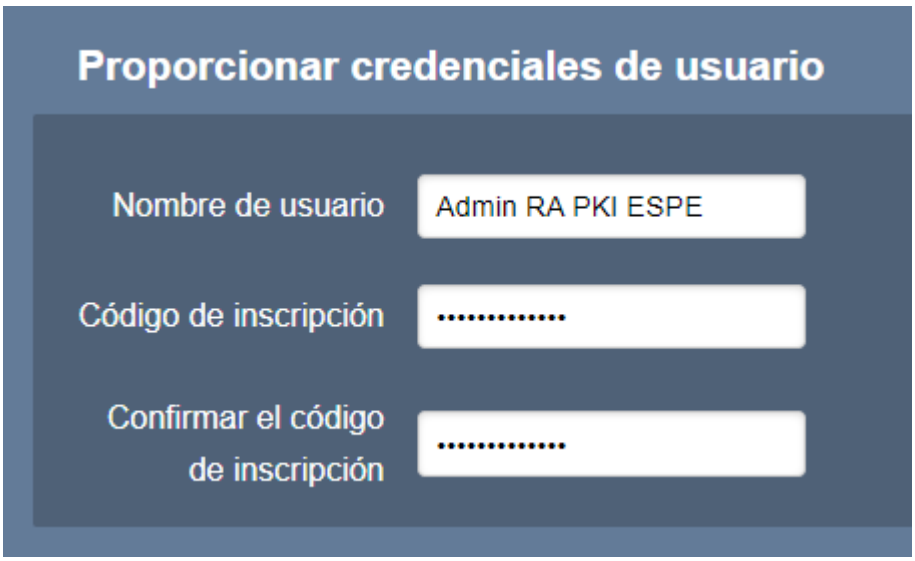
Atributos del nombre de distinción del sujeto



6.1.4.4. Se proporciona las credenciales de usuario.

Figura 154

Se proporciona las credenciales de usuario

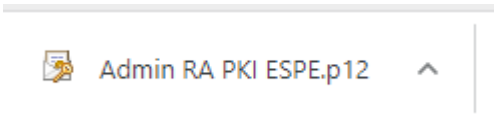


6.1.4.5. Se verifica los datos ingresados de la solicitud y se presiona en Descargar PKCS # 12.

Figura 155

datos ingresados de la solicitud

6.1.4.6. El sistema descarga inmediatamente el certificado digital en el formato seleccionado.

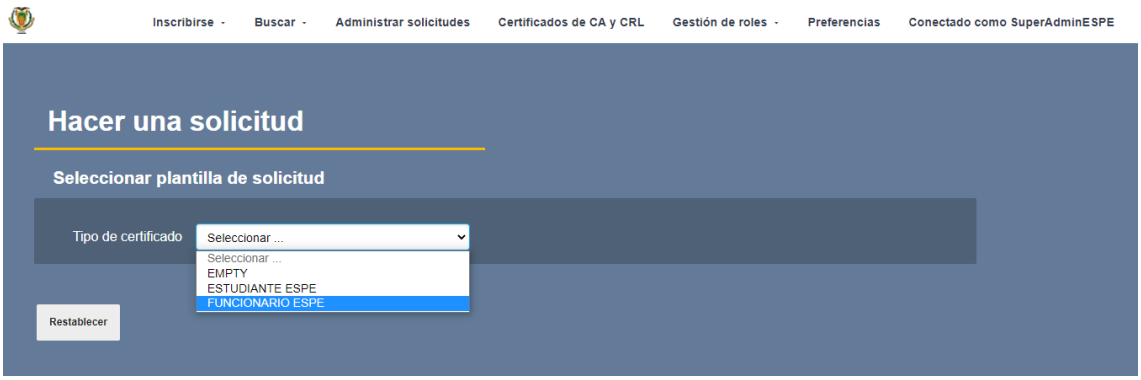


6.1.5. Entidad Final de Autoridad de Certificación

6.1.5.1. Se selecciona el tipo de certificado de FUNCIONARIO ESPE.

Figura 156

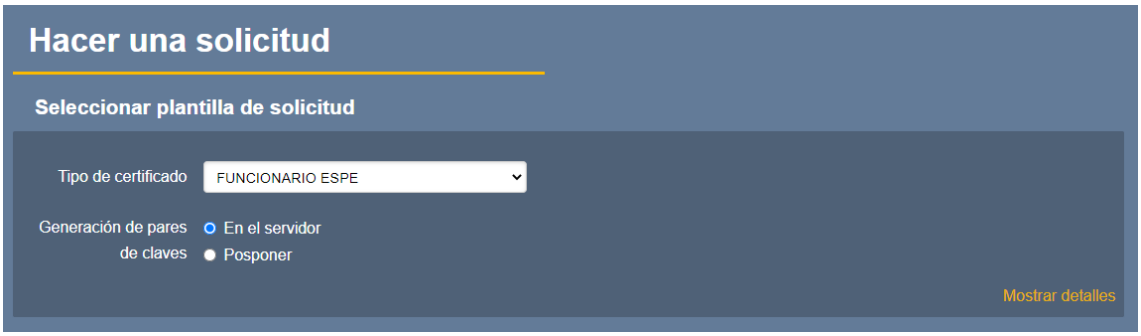
sistema descarga inmediatamente el certificado digital



6.1.5.2. Se marca la casilla de En el servidor para la Generación de pares de clave.

Figura 157

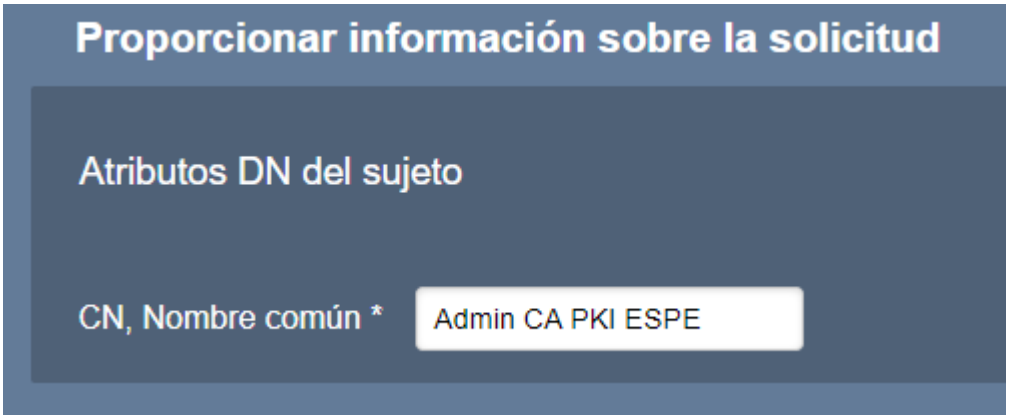
casilla de En el servidor para la Generación de pares de clave



6.1.5.3. Se ingresa los Atributos del nombre de distinción del sujeto.

Figura 158

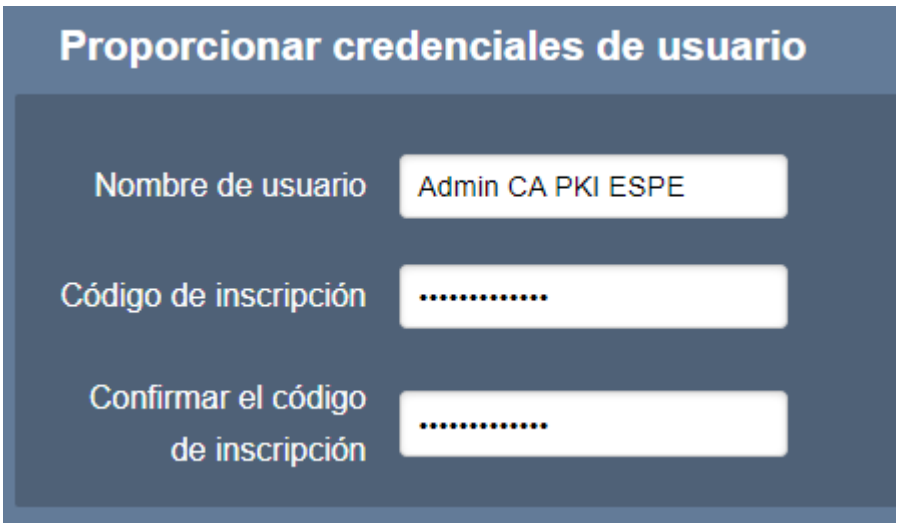
Atributos del nombre de distinción del sujeto



6.1.5.4. Se proporciona las credenciales de usuario.

Figura 159

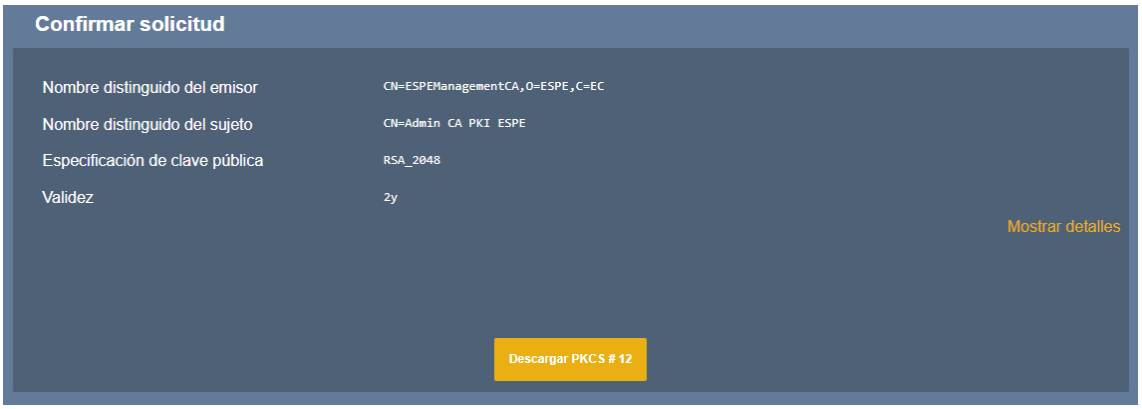
proporción credenciales



6.1.5.5. Se verifica los datos ingresados de la solicitud y se presiona en Descargar PKCS # 12.

Figura 160

datos ingresados de la solicitud



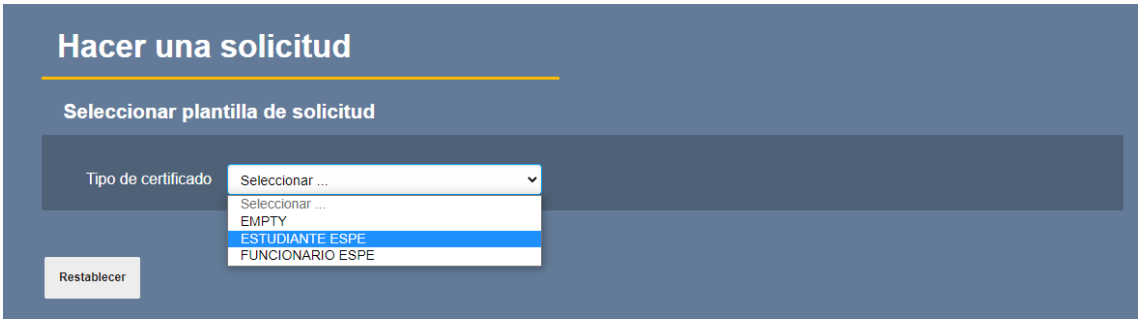
6.1.5.6. El sistema descarga inmediatamente el certificado digital en el formato seleccionado.

6.1.6. Entidad Final de Estudiante

6.1.6.1. Se selecciona el tipo de certificado de ESTUDIANTE ESPE.

Figura 161

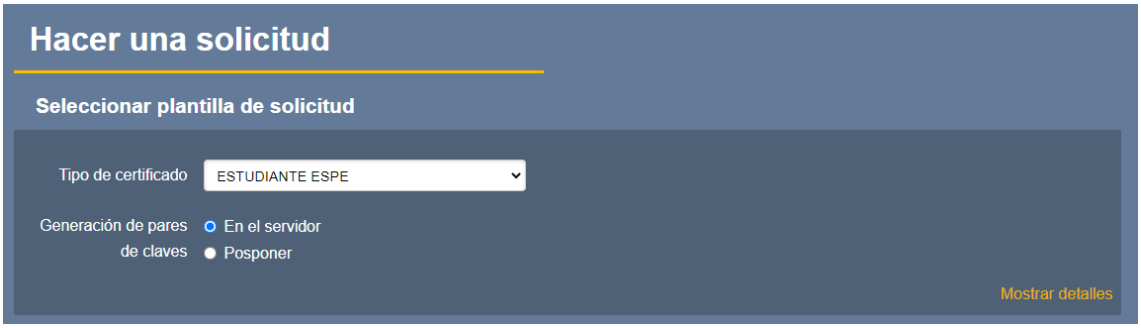
tipo de certificado de ESTUDIANTE ESPE



6.1.6.2. Se marca la casilla de En el servidor para la Generación de pares de clave.

Figura 162

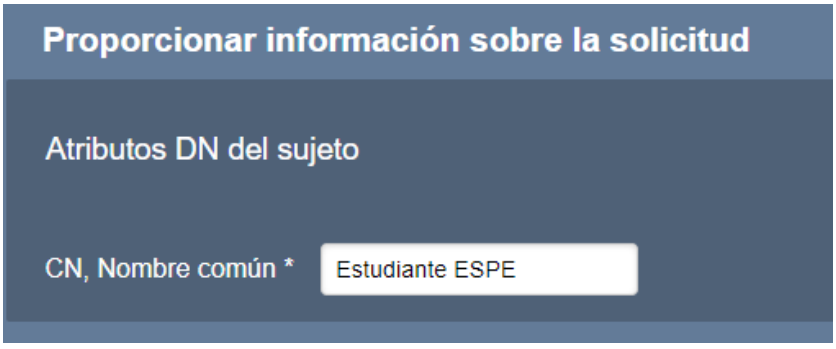
casilla de En el servidor para la Generación de pares de clave



6.1.6.3. Se ingresa los Atributos del nombre de distinción del sujeto.

Figura 163

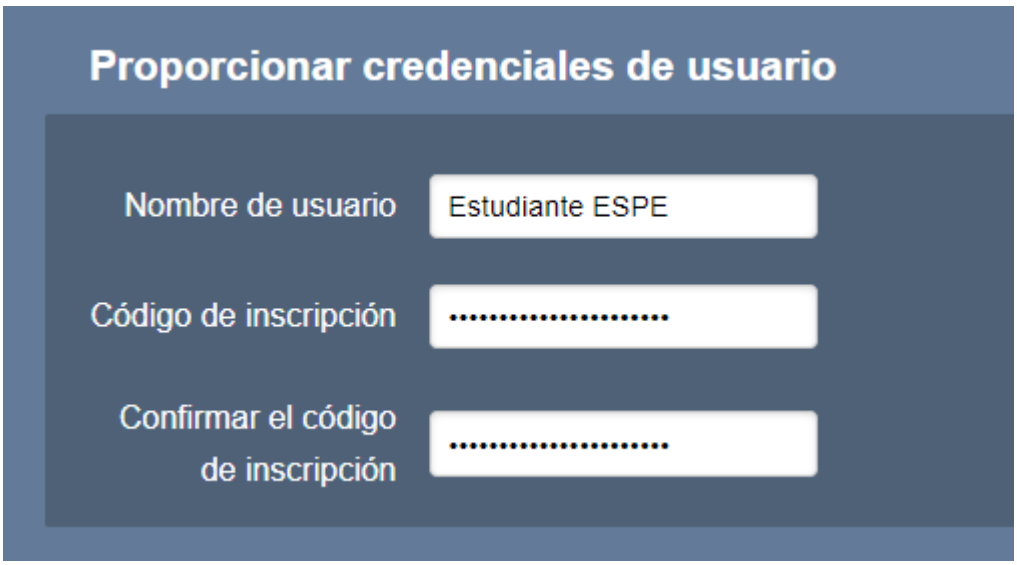
Ingreso los Atributos del nombre



6.1.6.4. Se proporciona las credenciales de usuario.

Figura 164

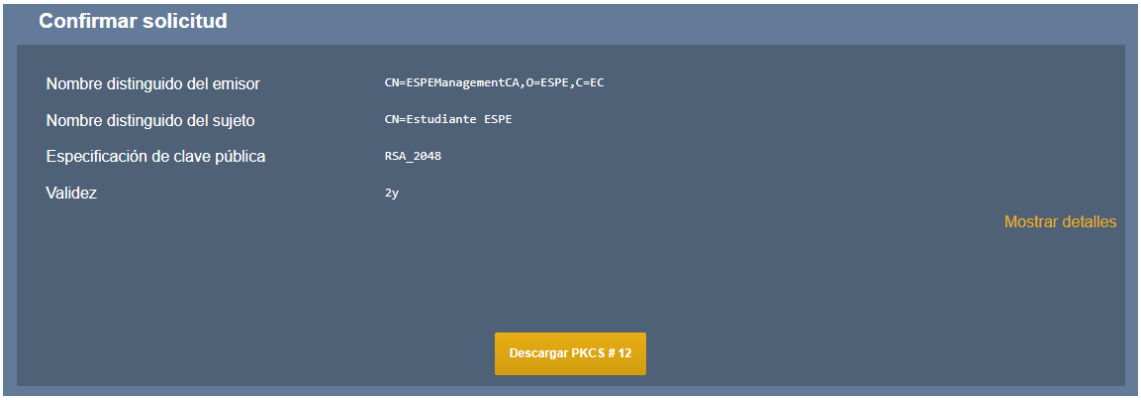
proporciona las credenciales de usuario



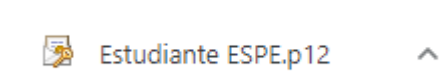
6.1.6.5. Se verifica los datos ingresados de la solicitud y se presiona en Descargar PKCS # 12.

Figura 165

Descargar PKCS



6.1.6.6. El sistema descarga inmediatamente el certificado digital en el formato seleccionado.



Capacitación de usuario

Se ha creado un manual de usuario para la solicitud de certificados digitales de la entidad, que para el presente caso de estudio está representado por un estudiante de la Universidad de las Fuerzas Armadas ESPE, el manual inicia desde

el ingreso a la aplicación con privilegios de estudiante, el proceso de llenar el formulario de solicitud con los datos necesarios para la generación del certificado, tales como el número identificador único otorgado por la universidad, los nombres completos y el correo electrónico institucional, con estos datos se enviará la notificación de que la solicitud ha sido aprobada, también se describe cómo descargar el certificado digital desde la aplicación web y por último como firmar un documento en formato PDF con su verificación de firma. Ver Anexo 1.

Asimismo, se ha creado un manual de usuario para el manejo de la autoridad de Registro, desde el ingreso a la aplicación con privilegios de administrador hasta la gestión de solicitudes de certificado digital por parte de la entidad final cuyo final tiene la aprobación o rechazo de los mismos. Ver Anexo 2.

Evaluación y entrega del sistema

La evaluación del software requiere tener en cuenta ciertos factores que son fundamentales previos a su entrega, el más importante es el de la funcionalidad del software, que se refiere a la manera en que soporta los procesos para los que fue implementado; también se debe considerar los aspectos técnicos. El proyecto ha sido evaluado en estos aspectos por los usuarios y expertos en el tema, tal como se puede ver durante todo el proceso de implementación, las encuestas y los anexos presentados al final. Dado este antecedente se procede a entregar el sistema totalmente instalado en los servidores de la universidad con sus respectivos manuales entre los cuales se encuentra todo el proceso desde la instalación, configuración y uso, al Departamento de Ciencias de la Computación y a la UTIC.

Capítulo V

Conclusiones

La transferencia de información cada día se incrementa en el Ecuador y el mundo entero; de la misma forma los ciberataques y ciberdelincuentes aprovechan las vulnerabilidades para obtener información casi siempre con motivos económicos.

La falta de presupuesto no ha sido un limitante para la implementación del proyecto en la Universidad de las Fuerzas Armadas “ESPE”; con el uso adecuado de herramientas de software libre, se creó una PKI que genera certificados digitales que ayudan a los alumnos a firmar documentos otorgándoles seguridad y confianza.

Se realizó una investigación sobre las herramientas de software libre para generar PKI, obteniendo como resultado que la mejor opción es JEBCA que posee características idóneas de implementación y utilización.

Una de las partes más importantes fue la creación de las políticas y procedimientos sobre el uso de la PKI que fueron construidas bajo lineamientos muy similares a las que manejan instituciones de certificación acreditadas tal como el Banco Central del Ecuador, el consejo de la Judicatura entre otros.

Todos los alumnos de la universidad de las fuerzas armadas “ESPE” son los principales beneficiarios de la PKI, que es muy intuitiva y fácil de utilizar, además cuenta con todas las guías y manuales para su uso.

La instalación, implementación y capacitación se realizó en las instalaciones de la UTIC, siendo ellos los encargados del manejo y administración de la herramienta además de que poseen recursos y conocimientos necesarios para una adecuada utilización.

Se han cumplido con los objetivos planteados evidenciando que la herramienta de certificación es muy útil para los alumnos de la universidad, otorga mayor confianza y seguridad en la transferencia de información.

Recomendaciones

Al momento de diseñar una solución tecnológica, es necesario utilizar tecnologías modernas que tengan aceptación en el mercado, de este modo se puede mejorar su ciclo de vida y mejorar su mantenimiento y aplicación.

Se recomienda que la capacitación del personal de operadores de la herramienta debe ser minucioso y permanente, ya que de ellos dependerá el correcto funcionamiento y el éxito de la aplicación propuesta.

Se debe realizar un estudio minucioso de las normas, códigos y leyes relacionadas con un proyecto de transformación digital, como el de firma electrónica, certificación y transferencia de datos. El el punto de partida para cumplir con un proceso de calidad y evita errores que perjudiquen el ciclo de vida de la certificación.

Se recomienda la difusión de buenas prácticas y uso de herramientas tecnológicas como la firma digital, certificado electrónico y protección de los mensajes de datos a toda la comunidad, teniendo en cuenta su gran utilidad y beneficios que brindan en el ámbito de seguridad al momento de realizar transferencias telemáticas.

Referencias

Abril, A. (2013). Análisis de riesgos en seguridad de la información. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, 39-53.

Altamirano, J. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Revista Ibérica de Sistemas y Tecnologías de Información*, 112-134.

Antillano, A. (2007). ¿Qué son las políticas de seguridad? *Urvio. Revista Latinoamericana de Estudios de Seguridad*, 147-177.

Arrieta, L. J. (2017). Firma Digital Móvil Basada en Criptografía Hash. *Ciencias Multidisciplinarias*, 22-36.

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/

Boiero, F. (2014). FORTALECIMIENTO DE LA SEGURIDAD DE LAS COMUNICACIONES MEDIANTE LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA. *Cytal*, 339-344.

Bravo, L. (2020). El modelo de ITIL v4 se enfoca en el valor del servicio y posee información como: • Entender conceptos principales de la gestion de servicios de TI. • Dimensiones del servivio y principios guias de ITIL. • Los componentes del sistema de valor de servic. *Dominio de las ciencias*, 1510-1534.

Carvajal, A. (2007). PKI y firmas digitales: aplicaciones reales. *Revista Inventum*, 13-26.

Castro, F. (2015). Gestor de Certificados Digitales con PKI. *Universidad Carlos III de Madrid Escuela Politécnica Superior*, 1-155.

CEDIA EC. (25 de Julio de 2014). *Universidad de las Fuerzas Armadas "ESPE"*. Obtenido de Universidad de las Fuerzas Armadas "ESPE": https://www.espe.edu.ec/

Cedillo, J. A. (2006). Creación de Patrones de Criptografía PGP Para Aplicaciones Utilizando Linux. *Polibits*, 1-34.

Córdoba, M. (2012). *Gestión Financiera.* Bogota: Ecoe Ediciones .

Delgado, V. (2006). Introducción a la Criptografía: tipos de algoritmos. *Canales de mecánica y electricidad*, 42-46.

Dussan, A. (2006). Políticas de seguridad informática. *Entramado*, 86-92.

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

Fernández, S. (2004). LA CRIPTOGRAFÍA CLÁSICA. *Sigma* , 119-142.

Figueroa, J. (2017). La seguridad informática y la seguridad de la información. *Polo del conocimiento*, 145-154.

García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. *Un estudio comparado*, 743-778.

García, F. Y. (2018). Análisis de la firma digital con base en la infraestructura de clave pública. *Hamut'ay*, 94-104.

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

Hernádez, J. (2008). Repudio de firmas electrónicas en infraestructuras de clave pública. *Departamento de Informática, Grupo SeTI, Universidad Carlos III de Madrid*, 34-51.

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

Lee, M. (2013). A Criptografia Funciona Como Proteger Sua Privacidade na Era da Vigilância em Massa. *Fundação da Liberdade de Imprensa*, 1-33.

Longueira, A. (Febrero de 2019). Diseño e implementación de una infraestructura PKI con HSM y renovación automatica de certificados para sistemas empotrados industriales. Oviedo.

Mieres, J. (Enero de 2009). Ataques informaticos. Debilidades de seguridad comúnmente explotadas. *Evil fingers*, 1-17.

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.

Ormaza, A. (2016). Information Security Policy: A systematic review of its concepts. *Política de Seguridad de la Información: Una revisión sistemática de su concepto*, 1-17.

Ormaza, D. (2017). Implementación de la Firma Digital en la Universidad de Buenos Aires. *Gestión de las TICs para la Investigación y la Colaboración*, 1-13.

Paredes, G. G. (2006). INTRODUCCIÓN A LA CRIPTOGRAFÍA. *Revista Digital Universitaria*, 1-17.

Pérez, S. (2018). Análisis del protocolo IPSec: el estándar de seguridad en IP. *Telefónica Investigación y Desarrollo*, 51-64.

Rendón, L. (Julio de 2020). Importancia de la capacitación y concientización de los empleados respecto a la seguridad de la información como un factor clave de éxito en la prevención del fraude informático. *Importancia de la capacitación y concientización de los empleados respecto a la seguridad de la información como un factor clave de éxito en la prevención del fraude informático* . Bogota, Bogota, Colombia: UNIVERSIDAD MILITAR NUEVA GRANADA FACULTAD DE CIENCIAS ECONÓMICAS ESPECIALIZACIÓN EN CONTROL INTERNO.

Solinas, M. (2013). Implementación de una infraestructura de clave pública con herramientas de software libre. *Anales JAIIO. JSL.*, 107-117.

Talens, S. (2012). Introducción a los certificados digitales. *InfoCentre*, 1-15.

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

Téllez, E. (2018). TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS. *IUS ET SCIENTIA*, 19-39.

Travieso, M. (2003). La Criptografía como elemento de la seguridad informática. *ACIMED*, 11-17.

Urquijo, Y. (2012). Esquema de confianza basado en Infraestructura de clave pública (PKI) para el intercambio de información clínica electrónica en el sistema XAVIA HIS. *Revista Cubana de Informática Médica* , 1-14.

Velasco, R. D. (2006). CRIPTOGRAFÍA, UNA NECESIDAD MODERNA. *Revista Digital Universitaria*, 1-9.

Velásquez, A. (2003). MODELO DE GESTIÓNDE OPERACIONESPARA PYMESINNOVADORAS. *Revista escuela de administración de negocios* , 66-87.

Villalba, T. (2014). Evaluación de software para entidades de certificación. *Ventana Informática*, 91-102.

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.

Zuñiga, J. (2015). LA INFORMACIÓN COMO ACTIVO ESTRATEGICO EN LA ADMINISTRACION DE LA PYME COMO -ZONA CENTRO COAHUILA. *Red Internacional de Investigadores en CompetitividadMemoria del IX Congreso*, 2162-2181.

Anexos