UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera De Software

TEMA:

"IMPLEMENTACIÓN DE UN SERVICIO DE FIRMA ELECTRÓNICA BASADO EN INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) PARA LA MEJORA DE LA GESTIÓN DOCUMENTAL ESTUDIANTIL EN LA FICA- UTN, ALINEADO CON LAS PRÁCTICAS DE ITIL V4"

Trabajo de grado presentado ante la Ilustre Universidad Técnica del Norte previo a la obtención del título de Ingeniero de Software.

AUTOR:

Jericho Alexander Paspuel Sánchez

DIRECTOR:

PhD. Imbaquingo Esparza Daisy Elizabeth

Ibarra-Ecuador

2026

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003860465		
APELLIDOS Y NOMBRES:	PASPUEL SANCHEZ JERICHO ALEXANDER		
DIRECCIÓN:	IBARRA, Priorato, 4 esquina de Priorato		
EMAIL:	japaspuels@utn.edu.ec, paspuelalexander@gmail.com		
TELÉFONO FIJO:	SN	**TELF. MOVIL**	0960662261

DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DE UN SERVICIO DE FIRMA ELECTRÓNICA BASADO EN INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) PARA LA MEJORA DE LA GESTIÓN DOCUMENTAL ESTUDIANTIL EN LA FICA- UTN, ALINEADO CON LAS PRÁCTICAS DE ITIL V4
AUTOR (ES):	PASPUEL SANCHEZ JERICHO ALEXANDER
FECHA:	27/02/2026
CARRERA/PROGRAMA:	■ **GRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERO DE SOFTWARE
DIRECTOR:	PhD. Imbaquingo Esparza Daisy Elizabeth
ASESOR:	MSc. Rea Peñafiel Xavier Mauricio

CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 27 días, del mes de febrero de 2026

EL AUTOR:

Firma……
Nombre: Jericho Alexander Paspuel Sánchez
CI: 1003860465

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 27 de febrero de 2026

PhD. Imbaquingo Esparza Daisy Elizabeth
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:
Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

Firmado electrónicamente por:
DAISY ELIZABETH IMBAQUINGO ESPARZA
Validar únicamente con FirmaEC

……

PhD. Imbaquingo Esparza Daisy Elizabeth
C.C.: 1002873048

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular "IMPLEMENTACIÓN DE UN SERVICIO DE FIRMA ELECTRÓNICA BASADO EN INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) PARA LA MEJORA DE LA GESTIÓN DOCUMENTAL ESTUDIANTIL EN LA FICA- UTN, ALINEADO CON LAS PRÁCTICAS DE ITIL V4" elaborado por Jericho Alexander Paspuel Sánchez, previo a la obtención del título del Ingeniero en Software, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

Firmado electrónicamente por:
DAISY ELIZABETH IMBAQUINGO ESPARZA
Validar únicamente con FirmaEC

…….

PhD. Imbaquingo Esparza Daisy Elizabeth
C.C.: 1002873048

Firmado electrónicamente por:
XAVIER MAURICIO REA PEÑAFIEL
Validar únicamente con FirmaEC

…….

MSc. Rea Peñafiel Xavier Mauricio
C.C.: 1002485744

DEDICATORIA

A mi hermano David Alejandro Paspuel Sánchez, por ser mi principal motivación y fuerza para culminar mis estudios. Desde donde estés, sé que tu luz me guio en cada paso de este camino, este logro lleva tu nombre en mi corazón.

A mi pareja, por ser mi apoyo incondicional y por su paciencia. Gracias por estar a mi lado en los momentos de cansancio, duda y esfuerzo, recordándome siempre que podría lograrlo, este triunfo también es nuestro.

A mis padres, por inculcarme disciplina, perseverancia, y el valor de la educación. Cada una de sus palabras fue una lección que hoy me permite estar aquí, este logro es tan suyo como mío.

A mis amigos y compañeros, por la experiencias y momentos compartidos. Su apoyo hizo que pueda mejorar como estudiante, profesional y persona, haciendo que este camino sea mucho más llevadero y enriquecedor.

Gracias por creer en mí.

Jericho Alexander Paspuel Sánchez

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a mis padres, por su amor, esfuerzo y sacrificio constante, por ser el pilar fundamental en mi formación personal y profesional, y por inculcarme los valores que hicieron posible culminar esta etapa.

A mis amigos, por su compañía, apoyo y palabras de aliento durante este proceso académico, que hicieron más llevadero cada desafío enfrentado.

Mi gratitud especial a mi directora de tesis, PhD. Imbaquingo Esparza Daisy Elizabeth, por su valioso apoyo en la realización de este proyecto, por su orientación académica y compromiso constante; y a mi asesor, MSc. Rea Peñafiel Xavier Mauricio, por su paciencia, por cada sugerencia brindada y por el tiempo dedicado. Su conocimiento, experiencia y dirección marcaron una diferencia significativa en el resultado final de este trabajo.

A mis docentes, quienes a lo largo de mi formación universitaria compartieron sus conocimientos y experiencias, contribuyendo de manera esencial a mi crecimiento académico y profesional.

A todos quienes formaron parte de este proceso, mi más profundo agradecimiento.

Jericho Alexander Paspuel Sánchez

Tabla de contenido

Índice de tablas

Índice de figuras

Resumen

Este trabajo de investigación aborda la implementación de un servicio de firma electrónica basada en infraestructura de clave pública (PKI) para los estudiantes de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte, con el objetivo de optimizar la gestión documental académica, a través del uso de una firma electrónica generada mediante el servicio mencionado anteriormente, garantizando así la autenticidad, integridad, y seguridad de los documentos. Esta iniciativa surge como respuesta a las limitaciones que presentan los métodos y procesos actuales que realiza un estudiante al firmar un documento, ocasionando demoras, costos elevados y el riesgo de pérdida o falsificación de datos.

La implementación del servicio empleó la metodología Design Science Research, estructurada en seis fases: identificación del problema, definición de objetivos, diseño, desarrollo, evaluación y comunicación, complementada con las buenas prácticas de ITIL v4 para una correcta administración del servicio.

El servicio implementado permite a los estudiantes solicitar y obtener su certificado digital en formato. p12, para hacer uso de este en el proceso de firma de documentos electrónicamente con validez técnica. Esto se realiza dentro de un entorno controlado para evaluar funcionalidad, seguridad y facilidad de uso. Los resultados muestran mejoras significativas en eficiencia, en la reducción de los tiempos de manejo, y una buena receptividad entre los usuarios, quienes apreciaron la simplicidad de uso y la fiabilidad del sistema. De manera adicional, se llevó a cabo un breve estudio sobre el procedimiento legal que requiere ARCOTEL para una futura certificación como Entidad de Certificación. Se concluye que la solución presentada refuerza la transformación digital en la FICA-UTN y establece las bases para una posible expansión institucional, ayudando a que la gestión documental sea más ágil, segura y sostenible.

Palabras clave: Infraestructura de clave pública, firma electrónica, certificado digital, certificación, software libre.

Abstract

This research work addresses the implementation of an electronic signature service based on public key infrastructure (PKI) for students of the Faculty of Engineering in Applied Sciences (FICA) of the Universidad Técnica del Norte, with the objective of optimizing academic document management, through the use of an electronic signature generated by the aforementioned service, thus guaranteeing the authenticity, integrity, and security of the documents. This initiative arose as a response to the limitations presented by the current methods and processes used by a student to sign a document, causing delays, high costs and the risk of loss or falsification of data.

The implementation of the service used the Design Science Research methodology, structured in six phases: identification of the problem, definition of objectives, design, development, evaluation and communication, complemented with ITIL v4 best practices for a correct administration of the service.

The implemented service allows students to request and obtain their digital certificate in .p12 format, to make use of it in the process of signing documents electronically with technical validity. This is done within a controlled environment to evaluate functionality, security and ease of use. The results show significant improvements in efficiency, in the reduction of handling times, and a good receptivity among users, who appreciated the simplicity of use and reliability of the system. Additionally, a brief study was carried out on the legal procedure required by ARCOTEL for a future certification as a Certification Entity. It is concluded that the solution presented reinforces the digital transformation at FICA-UTN and establishes the basis for a possible institutional expansion, helping to make document management more agile, secure and sustainable.

Keywords: Public key infrastructure, electronic signature, digital certificate, certification, free software.

LISTA DE SIGLAS

LEC. Ley de Comercio Electrónico, Firmas y Mensajes de Datos

XCA. X Certificate and Key Management

OPENCA. Open Certificate Authority

PGP. Pretty Good Privacy

EJBCA. Enterprise JavaBeans Certificate Authority

DRS. Design Science Research

SVS. Sistema de Valor del Servicio

TI. Tecnologías de la Información

ARCOTEL. Agencia de Regulación y Control de las Telecomunicaciones

PKI. Infraestructura de Clave Pública

ITIL. Information Technology Infrastructure Library

CRL. Lista de Certificados Revocados

OCSP. Protocolo de Estado de Certificados en línea

SSL/TLS. Certificados de Servidor

RA. Autoridad de Registro

CA. Autoridad de Certificación

RootCA. Autoridad Certificadora Raíz

SubCA. Autoridades Certificadoras Subordinada

EE. Entidad Final

UTN. Universidad Técnica del Norte

FICA. Facultad de Ingeniería en Ciencias Aplicadas

VS Code. Visual Studio Code

CAPÍTULO I

INTRODUCCIÓN

En el siguiente capítulo se presenta el planteamiento del problema relacionado con la gestión documental estudiantil en la FICA-UTN, destacando las limitaciones del uso de procesos manuales y firmas físicas. Se expone la justificación del proyecto, los objetivos general y específicos que orientan la investigación, el alcance de la propuesta y la metodología empleada basada en Design Science Research junto con prácticas de ITIL V4, estableciendo así las bases conceptuales y estructurales para el desarrollo del servicio de firma electrónica basado en PKI.

1.1 Planteamiento del problema.

En la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte (UTN), la gestión documental estudiantil se realiza de forma manual, dependiendo de firmas físicas, en documentos impresos. Esto genera retrasos, costos por uso de papel, riesgos de alteración o pérdida de información y falta de interoperabilidad [1].

Causas principales:

1. Falta de un servicio de firma electrónica, lo que compromete la autenticidad y seguridad de los documentos digitales [2].
2. Procesos manuales que alargan los tiempos de validación y aprobación [1].
3. Desconocimiento sobre los beneficios y seguridad de la firma electrónica, retrasando su adopción [2].

Estas limitaciones provocan demoras por traslados físicos, riesgos de falsificación y altos costos operativos, afectando la productividad y la confianza en la validez de la información.

Como solución, se propone implementar un servicio de firma electrónica basada en PKI, que optimizará la gestión documental mediante digitalización segura.

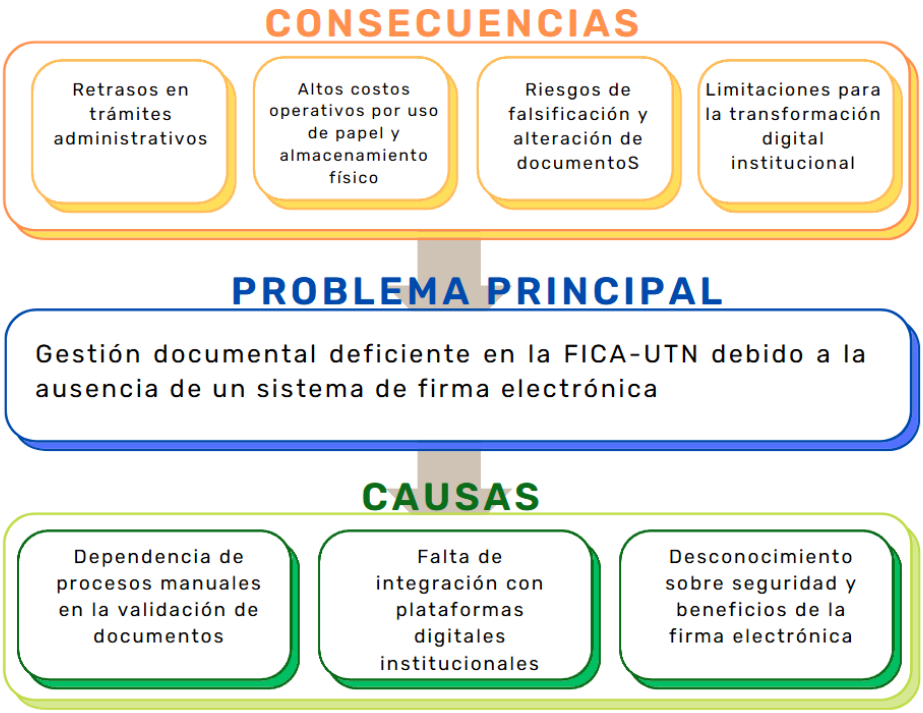


Figura: 1 Árbol de problemas

1.2 Justificación

Ante la necesidad de agilizar y asegurar los procesos administrativos, la FICA-UTN enfrenta limitaciones derivadas de una gestión documental mayormente manual. Para resolver esto, se plantea el desarrollo de un servicio de firma electrónica basado en PKI, orientado a digitalizar la validación de documentos con garantías de autenticidad, integridad y trazabilidad.

El proyecto no solo responde a una necesidad institucional, sino que también constituye una oportunidad de aplicar conocimientos en ingeniería de software, seguridad informática y criptografía.

El sistema busca facilitar un cambio cultural hacia la transformación digital, reduciendo la dependencia del papel y mejorando la eficiencia operativa. Su impacto abarca ámbitos técnicos, económicos y educativos: promueve la transparencia, ahorra recursos y fortalece competencias digitales. A futuro, puede servir como base para acreditaciones tecnológicas internas y expansión a otras facultades. Guiado por la metodología Design Science Research e ITIL V4, este proyecto busca implementar un servicio funcional y escalable, que contribuya a la modernización sostenible de los procesos documentales en la FICA-UTN.

Esta iniciativa se alinea con el Objetivo de Desarrollo Sostenible (ODS) Nº 9: Industria, Innovación e Infraestructura, al fomentar el desarrollo de infraestructuras digitales resilientes, promover la innovación tecnológica en el ámbito educativo y fortalecer capacidades institucionales mediante soluciones sostenibles.

1.3 Objetivos

1.3.1 Objetivo general

Implementar un servicio de Firma electrónica basado en PKI para optimizar la gestión documental de estudiantes en la FICA-UTN, garantizando seguridad, integridad y eficiencia en los procesos administrativos.

1.3.2 Objetivos específicos

- Elaborar el marco teórico sobre el análisis de estructuras y funcionamiento del servicio de firma electrónica.
- Implantar el Servicio de firma electrónica en la facultad FICA de la UTN, utilizando ITIL V4.
- Evaluar la seguridad y satisfacción de los usuarios involucrados respecto al servicio de firma electrónica implementado, mediante la aplicación de encuestas estructuradas, con el fin de identificar su usabilidad, aceptación y posibles oportunidades de mejora.

1.4 Alcance

Este proyecto propone el diseño, desarrollo y evalúo de un servicio de firma electrónica basado en infraestructura de clave pública (PKI) para la gestión documental de estudiantiles en la FICA-UTN. Se analizarán tecnologías criptográficas y certificados digitales para definir los requerimientos técnicos y funcionales del servicio.

El servicio permitirá solicitar, aprobar y descargar un archivo de extensión “.p12" con su certificado digital y firma electrónica, con el que podrán firmar documentos, garantizando autenticidad, integridad y seguridad.

Tendrá una interfaz accesible y será probado en un entorno controlado para verificar su funcionamiento, seguridad y compatibilidad. Estas pruebas permitirán realizar mejoras antes de una implementación completa.

Adicionalmente, se incluirá una breve investigación del proceso de validación legal requerido para que el sistema pueda ser reconocido oficialmente por el ente

regulador ecuatoriano (ARCOTEL), documentando los requisitos técnicos, legales y administrativos necesarios para una futura acreditación como Entidad de Certificación. Esta exploración será de carácter informativo y no implica la ejecución de dicho proceso en este proyecto.

Finalmente, se evaluará la percepción de los usuarios involucrados como estudiantes, personal administrativo y entidades finales sobre la usabilidad y aceptación del servicio de firma electrónica. Esta retroalimentación permitirá identificar oportunidades de mejora antes de considerar una posible ampliación del sistema a otras facultades, en el marco de la transformación digital de la UTN. Cabe destacar que el presente estudio se limita al uso interno y no contempla procesos de acreditación oficial ante organismos externos.

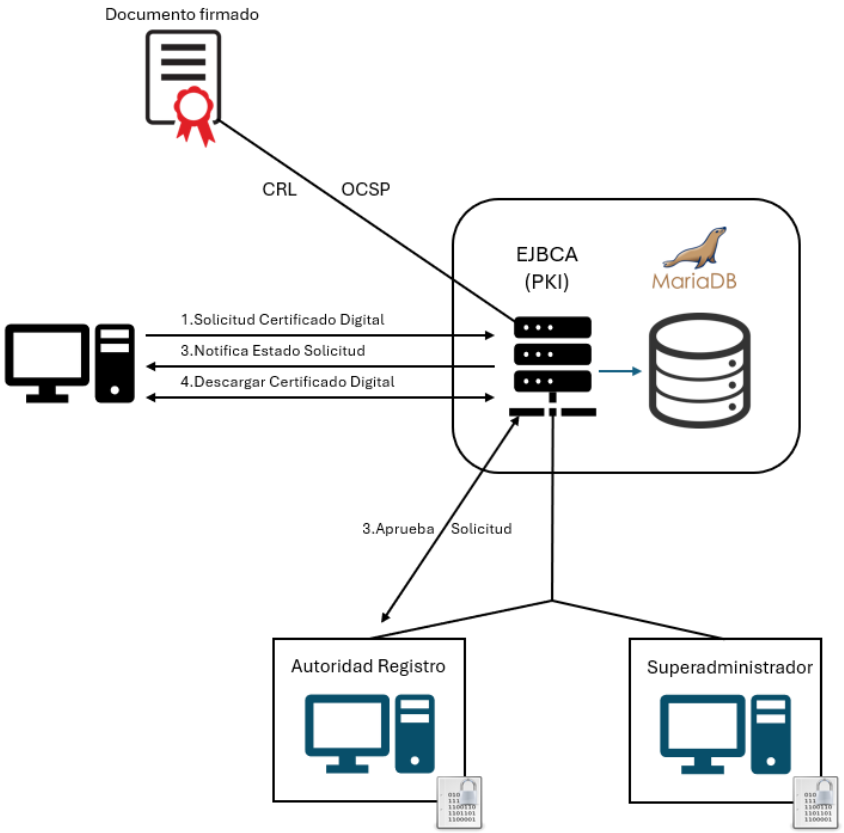


Figura: 2 Arquitectura del sistema de firma electrónica

1.5 Metodología

La metodología seleccionada para este proyecto es Design Science Research (DSR), ampliamente utilizada en áreas como la informática y la ingeniería de sistemas. Este enfoque se basa en crear y desarrollar soluciones tecnológicas, también conocidas

como artefactos, que pueden ser sistemas, modelos o algoritmos, con el fin de resolver problemas específicos de manera práctica.

1.5.1 Metodología Science Research

Esta metodología puede variar dependiendo de las necesidades, pero según Peffers [3], el proceso de DSR se compone de seis fases que guían la investigación de manera estructurada.

- Identificación y justificación del problema
- Objetivos de la solución
- Diseño y desarrollo
- Demostración
- Evaluación
- Comunicación

En las dos primeras etapas de esta metodología se trabajan aspectos clave que corresponden al Capítulo I del proyecto, ya que en ellas se identifica el problema central y se explican las razones por las cuales debe ser atendido. A partir de ese análisis, se formulan los objetivos que guiarán el desarrollo de la solución.

En la tercera etapa, se examinan los requerimientos técnicos y funcionales que se necesitarán para construir el servicio, y luego se lleva a cabo su implementación.

La cuarta fase está enfocada en ejecutar pruebas sobre el sistema creado, con el fin de comprobar que cumple adecuadamente su función. Luego, en la quinta fase, se analiza el desempeño obtenido durante las pruebas para determinar qué tan efectivo y eficiente es el servicio. Este análisis puede apoyarse en encuestas aplicadas a los usuarios que utilizaron el servicio, con el objetivo de recoger opiniones que permitan identificar posibles mejoras.

Finalmente, en la sexta etapa se exponen los resultados alcanzados, junto con la solución construida, para demostrar su valor, tanto a nivel institucional como académico.

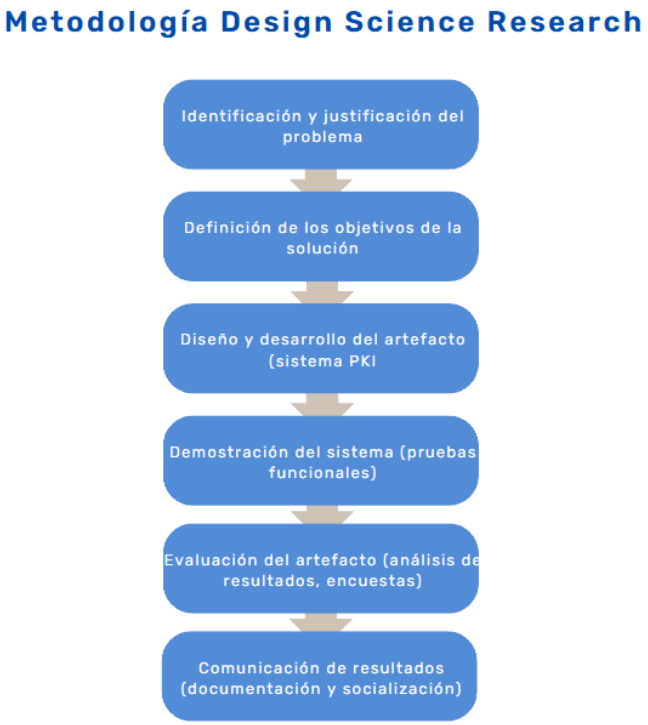


Figura: 3 Fases de la metodología Design Science Research

CAPÍTULO II

MARCO TEÓRICO

En el siguiente capítulo se desarrollan los fundamentos teóricos que sustentan la investigación, abordando conceptos relacionados con ITIL v4 y la gestión de servicios de TI, así como los principios de criptografía, firma electrónica, certificados digitales e infraestructura de clave pública (PKI). Además, se analiza el marco legal ecuatoriano aplicable y se revisan trabajos similares, proporcionando el sustento técnico, normativo y conceptual necesario para la implementación del servicio propuesto.

2.1 **ITIL**

ITIL (Information Technology Infrastructure Library), es una biblioteca de conceptos y mejores prácticas que ayudan a fortalecer un servicio de TI de acuerdo con las necesidades de la empresa. Esta biblioteca garantiza que una organización que depende de las tecnologías de la Información y Comunicación, para lograr sus objetivos comerciales y necesidades de negocios, brinde a los clientes servicios de calidad [4].

2.1.1 ITIL V4

Lanzada en 2019 como la última actualización hasta la actualidad. Aparece en necesidad a la adaptación de la transformación digital y al surgimiento de nuevas tecnologías, que han cambiado la forma de organizar las actividades de una organización de TI. Esta versión tiene un diseño flexible, ágil y orientado al usuario, concentrándose en el ciclo de vida del servicio y la introducción de un nuevo concepto, como la orientación del servicio hacia el valor [4].

2.1.2 Enfoque de gestión de servicios

El sistema de valor del servicio (SVS) es un enfoque holístico, que se basa en un método integral que busca que el personal de una entidad y sus actividades designadas, funcionen como una sola para generar valor. El SVS incluye elementos, acciones y métodos que colaboran entre sí para alcanzar las metas y resultados esperados [5].

Los elementos esenciales del SVS son los siguientes:

- **Gobierno:** Se relaciona con el grupo de normas, funciones, responsabilidades y procedimientos para dirigir y regular la utilización eficiente de los recursos de TI y las decisiones estratégicas.

- **Gestión de servicios:** Consiste en un conjunto de competencias orientadas a generar valor para los clientes mediante el diseño, la entrega y la mejora continua de servicios de calidad.
- **Mejora continua:** Se trata de la habilidad de revisar y optimizar de forma ininterrumpida la efectividad de los procesos y servicios, fundamentándose en el conocimiento adquirido y los comentarios recogidos mediante la experiencia y la evaluación de resultados.
- **Prácticas de gestión de servicios:** Se refieren a métodos concretos y orientaciones prácticas que permiten desarrollar tareas y alcanzar objetivos relacionados con la administración de servicios en el ámbito de las tecnologías de la información. La versión ITIL v4 propone una variedad de métodos, como la gestión de incidencias, de cambios, de problemas y la administración general de servicios de TI, entre otros.

2.2 Criptografía y seguridad

La preocupación por mantener la información segura ha aumentado significativamente con los años. En la época previa a la era digital, esta protección se realizaba por medios físicos, como el uso de cajas fuertes. Sin embargo, con la llegada de las computadoras, surgieron nuevas herramientas orientadas a preservar los datos en formato digital, siendo el cifrado uno de los mecanismos más utilizados.

2.2.1 Criptografía

El término criptografía proviene del griego, donde “kriptos” significa oculto y “graphos” hace referencia a la escritura. Juntas, estas palabras implican la idea de disimular la información, empleando algún método que haga un mensaje incomprensible. Esta ciencia surge de una parte de las matemáticas llamada “Teoría de la Información”, término que fue introducido por el matemático Claude Elwood Shannon en mil novecientos cuarenta y ocho. La meta fundamental de esta área es salvaguardar la información utilizando códigos y procedimientos matemáticos.

Al hablar sobre la protección de datos, no solo implica resguardar la información del acceso no autorizado. En este contexto, hay tres conceptos fundamentales que son esenciales para salvaguardar la información: confidencialidad, integridad y autenticidad. La confidencialidad implica que solo las partes autorizadas pueden comprender un mensaje, mientras que para los demás, debe permanecer oculto. La integridad asegura que

el contenido del mensaje se mantenga inalterado durante su envío, garantizando que siempre se reciba lo mismo. La autenticidad permite verificar el origen del mensaje, asegurando que provenga de una fuente fiable. Para conseguir esto, se utilizan métodos como las firmas y certificados digitales, entre otros [6].

2.2.2 Métodos de criptografía

Hoy en día hay dos tipos de técnicas criptográficas contemporáneas: la encriptación con clave privada o criptografía simétrica y la encriptación con clave pública o criptografía asimétrica. La idea de una clave está relacionada con el control de acceso físico, como ocurre con una cerradura o un candado que solo pueden abrirse utilizando una llave determinada. Por lo tanto, en el ámbito de la criptografía, se define como clave a un recurso digital que permite restringir y permitir el acceso a la información, y esta clave generalmente consiste en una secuencia de caracteres que debe ser única y mantener su secreto.

2.2.3 Criptografía simétrica

Este tipo de codificación utiliza una única clave para codificar y decodificar un mensaje. Por ejemplo, supongamos que una persona llamada Alex quiere enviar un mensaje privado a otra persona llamada Gema. Lo primero que tiene que hacer Alex es codificar el mensaje usando su clave antes de enviárselo a Gema. Sin embargo, para que Gema pueda decodificarlo, necesita conocer la clave de Alex. Este sistema suele ser efectivo, pero presenta un inconveniente. En primer lugar, Alex debe revelar su clave personal a Gema. Además, si desea compartir un mensaje con más personas, tendría que crear una clave personal para cada una de ellas.

Figura: 4 Criptografía de clave primaria

2.2.4 Criptografía asimétrica

Este método emplea un par de claves: una de ellas es accesible públicamente, mientras que la otra se mantiene en secreto. En este esquema, el mensaje se codifica

usando la clave privada, y únicamente puede ser interpretado correctamente al aplicar su clave pública asociada. Siguiendo el ejemplo previo, si Alex desea enviar un mensaje privado a Gema, debe cifrarlo usando su llave privada y luego remitirlo a Gema. Para que Gema descifre el mensaje, necesita disponer de la llave pública de Alex. De esta manera, se resuelve el inconveniente de intercambiar la llave privada para el descifrado del mensaje y, además, ya no es necesario crear n llaves privadas, sino que se requiere generar n llaves públicas.

Figura: 5 Criptografía de clave pública

2.2.5 Amenazas a la seguridad en PKI y firma electrónica

La infraestructura de clave pública (PKI) y la firma electrónica son pilares fundamentales para garantizar la autenticidad, integridad y no repudio en las transacciones digitales. Sin embargo, como cualquier sistema tecnológico, no están exentas de vulnerabilidades y amenazas que podrían comprometer su fiabilidad y la confianza en los procesos que sustentan. La proliferación de ciberataques y ciberdelincuentes hace indispensable comprender los riesgos asociados para implementar contramedidas efectivas que salvaguarden la información y las identidades digitales [7].

A continuación, se presenta una tabla que detalla las principales amenazas a la seguridad de la PKI y la firma electrónica, junto con una breve descripción de cada una.

Amenaza	**¿En qué consiste?**	**¿Qué consecuencias puede tener?**	**¿Cómo se puede prevenir o reducir el riesgo?**
Ataques a la Autoridad Certificadora (CA)	Ocurren cuando un atacante logra acceder o controlar una CA, permitiéndole	Esto pone en riesgo toda la infraestructura, ya que se pueden generar firmas	Es clave proteger la CA con medidas de seguridad física y lógica, auditorías regulares y

	emitir certificados falsos o alterar los existentes.	digitales falsas sin que el usuario lo note.	validaciones como OCSP o CRL.
Robo de claves privadas	Sucede cuando un tercero logra obtener la clave privada de un usuario, ya sea mediante malware, acceso físico o técnicas de engaño.	Permite suplantar al titular de la clave y firmar documentos en su nombre, lo cual compromete la integridad y autenticidad de la información.	Usar dispositivos seguros (como tokens o smartcards), cifrado, contraseñas fuertes y autenticación multifactor.
Ingeniería social	Se basa en manipular a las personas para obtener acceso a información confidencial o inducirlas a realizar acciones perjudiciales, como firmar documentos falsos.	A pesar de que los sistemas sean seguros, el error humano puede permitir accesos no autorizados o comprometer documentos.	La capacitación de los usuarios, el uso de autenticación fuerte y una cultura de ciberseguridad ayudan a reducir este riesgo.
Certificados digitales falsificados	Implica la creación de certificados que parecen legítimos, aprovechando CA vulnerables o algoritmos débiles.	Puede engañar a los usuarios, haciéndoles confiar en identidades falsas o sitios inseguros.	Verificar la procedencia del certificado, usar algoritmos criptográficos actualizados y confiar solo en autoridades reconocidas.

Ataques de intermediario (Man-in-the-Middle)	Un tercero intercepta la comunicación entre el usuario y la CA o entre otros actores del sistema PKI, sin que las partes lo noten.	Puede modificar datos, redirigir solicitudes o interferir en la validación de firmas.	Proteger las comunicaciones con cifrado (como TLS) y validar adecuadamente los certificados.
Uso de algoritmos inseguros	Algunos algoritmos criptográficos han sido superados por la capacidad de cómputo actual o tienen fallas conocidas.	Se vuelve posible romper la seguridad del sistema, descifrar mensajes o falsificar firmas.	Actualizar periódicamente los algoritmos usados y seguir recomendaciones internacionales (por ejemplo, NIST).
Pérdida o robo de dispositivos de firma	Cuando un token, smartcard o dispositivo que almacena una clave privada cae en manos equivocadas.	El atacante podría firmar documentos legítimos como si fuera el usuario original.	Añadir protecciones como PIN, bloqueo biométrico, y tener mecanismos para revocar inmediatamente las credenciales.
Problemas en la revocación de certificados	Si los sistemas que notifican sobre certificados comprometidos (como CRL o servidores OCSP) fallan o no están actualizados.	Los certificados que ya no deberían ser válidos podrían seguir usándose, poniendo en riesgo a los usuarios.	Mantener al día las listas de revocación, contar con servidores redundantes y monitorear constantemente.
Configuraciones incorrectas	Se refiere a errores al configurar	Pueden abrir puertas a	Seguir buenas prácticas de

	servidores, certificados o políticas de seguridad dentro del sistema PKI.	atacantes, invalidar firmas o causar interrupciones en el servicio.	configuración, automatizar procesos y hacer pruebas de seguridad regularmente.
Riesgos internos (personal malintencionado)	Individuos dentro de la organización con acceso privilegiado podrían abusar de su posición para comprometer el sistema.	Representa una de las amenazas más críticas, ya que pueden generar certificados falsos o desactivar controles.	Implementar controles de acceso por rol, dividir responsabilidades y registrar todas las actividades del sistema.

Tabla 1 Clasificación de Amenazas que Afectan la Confianza en la Firma Electrónica.

2.3 Fundamentos de la firma electrónica

La firma electrónica consiste en un conjunto de elementos, como datos personales del firmante y características técnicas definidas durante su creación, que actúan como un medio de identificación para el firmante, teniendo el mismo peso legal que una firma en papel [8].

Es indispensable disponer de un certificado digital. Este es un archivo electrónico que contiene datos personales del titular y permite verificar su identidad. Este certificado es proporcionado por una Autoridad Certificadora, encargada de validar y autenticar la información personal, certificando así a la persona para que pueda realizar la firma electrónica.

La firma electrónica, mediante varias tecnologías, se convierte en una herramienta digital que asegura la veracidad, la integridad y la inviolabilidad de los datos transmitidos a través de medios digitales [9]. Al utilizar la firma electrónica para firmar un archivo, la información personal del individuo, como su identificación y correo electrónico, se incorpora en el archivo; así, el firmante está de alguna manera validando y reconociendo el contenido del archivo. De este modo, cualquier individuo que reciba este archivo puede comprobar sin dificultad su origen y su veracidad, teniendo confianza en la información contenida en el documento [10].

2.3.1 Operatividad de la firma electrónica

La operación de la firma electrónica se fundamenta en la aplicación de métodos criptográficos asimétricos que conectan de manera digital la identidad de un individuo con el contenido de un archivo.

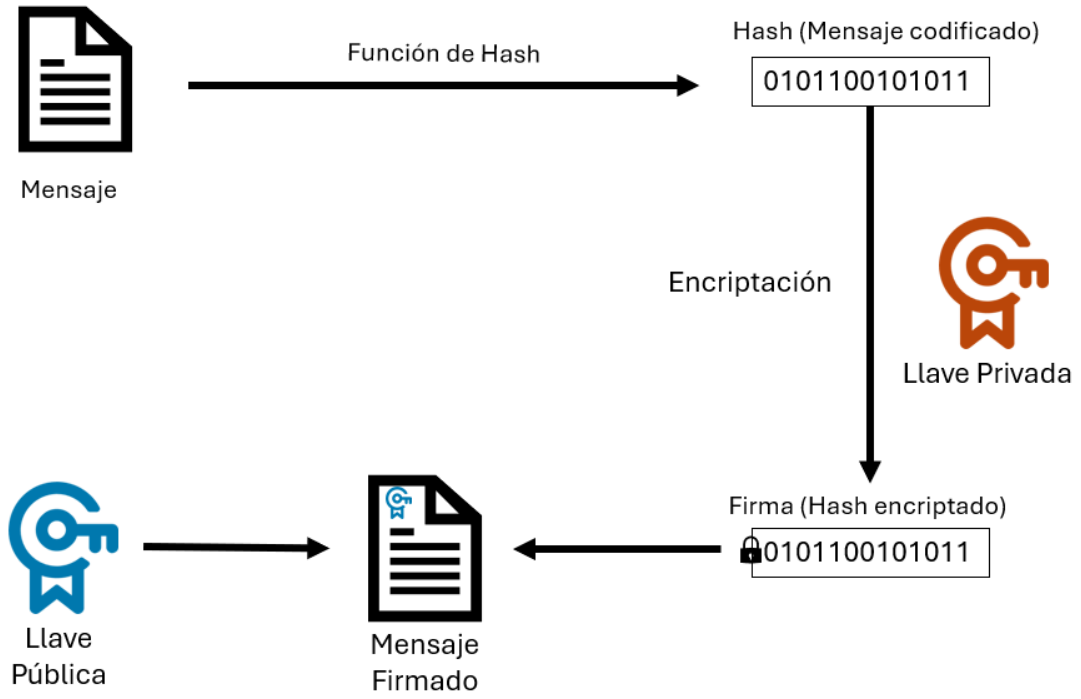


Figura: 6 Firma electrónica: proceso de firma

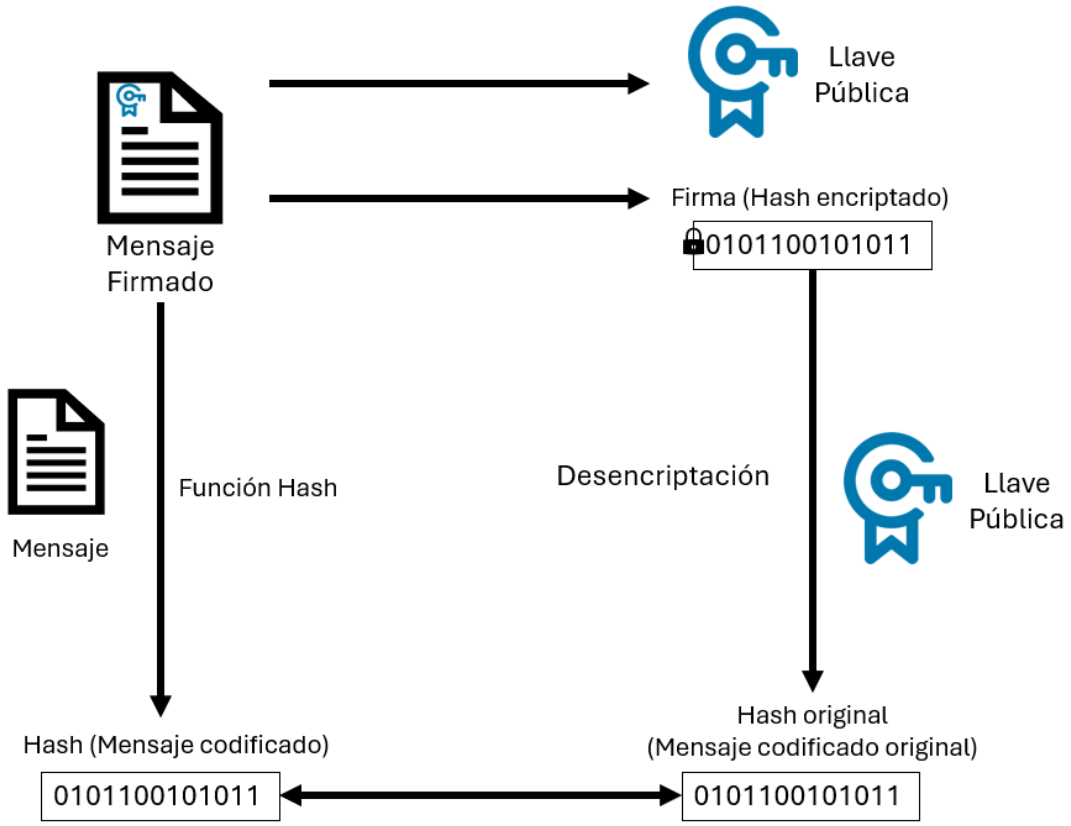


Figura: 7 Firma electrónica: proceso de verificación

El funcionamiento fundamental de una firma electrónica se detalla a continuación:

- **Firma**: El proceso comienza con la creación de un resumen del contenido, generado a través de funciones hash aplicadas al mensaje original. Esto produce un mensaje codificado, conocido como hash resultante o simplemente hash. Este hash se cifra con la clave privada del firmante, resultando en un hash cifrado, que se denomina firma. Esta firma se une al mensaje de datos original, junto a la clave pública del firmante, completando así la firma electrónica del mensaje de datos.
- **Comprobación de la firma:** Quien recibe un mensaje que ha sido firmado electrónicamente obtiene tres elementos: el mensaje en sí, la firma y la clave pública del firmante. Para llevar a cabo la comprobación, la persona encargada vuelve a aplicar una función hash al mensaje recibido. Luego, se desencripta la firma o el hash encriptado utilizando la clave pública del firmante, lo que permite recuperar el hash original creado por el firmante. Por último, la persona encargada de la verificación compara el hash recién generado con el hash original del firmante; si ambos coinciden, se considera que la firma es auténtica, de lo contrario, se invalida.

2.4 Certificados digitales

El certificado digital es un archivo electrónico diseñado para identificar a una persona y habilitarla para firmar documentos en entornos digitales. En su interior se almacena información personal del titular. La firma electrónica se basa en técnicas de criptografía asimétrica, las cuales operan mediante un par de claves: una privada, que se mantiene en secreto, y una pública, que puede compartirse. Ambas claves están relacionadas entre sí y forman parte del contenido del certificado digital.

2.4.1 Tipos de certificados digitales

Aunque todos los certificados digitales comparten una estructura común definida por el estándar ITU-T X.509, pueden dividirse en diferentes tipos. Las dos principales formas de clasificación se basan en el nivel de verificación aplicado y en el propósito para el cual fueron emitidos.

A. Clasificación por nivel de validación

Este criterio se centra en los certificados de servidor (SSL/TLS) y establece la profundidad con la que la Autoridad de Certificación verifica la identidad del solicitante antes de emitir el certificado.

- **Validación de Dominio (DV – Domain Validation):** Es la forma más simple de validación. La CA solo confirma que el solicitante tiene autoridad sobre el nombre de dominio asociado al certificado. Son rápidos de obtener y económicos, pero ofrecen menor confianza [11].
- **Validación de Organización (OV - Organization Validation):** Aparte de verificar el control del dominio, la CA también valida la existencia legal de la organización solicitante (nombre, ciudad, país). Estos certificados brindan un nivel de confianza mayor, ya que presentan información confirmada de la organización en los detalles del certificado [11].
- **Validación Extendida (EV – Extended Validation):** Este tipo de certificado garantiza el máximo nivel de seguridad y credibilidad. Antes de otorgar este tipo de certificado, la entidad emisora debe confirmar exhaustivamente tanto la autenticidad como la existencia legal de la organización, guiándose por los lineamientos establecidos por el CA/Browser Forum [11].

B. Clasificación por uso o propósito

Esta clasificación se enfoca en el propósito por el cual se expide el certificado.

- **Certificados de Servidor (SSL/TLS):** Su función es validar la identidad de un servidor web y facilitar una comunicación segura entre el servidor y el usuario a través del protocolo HTTPS [11].
- **Certificados de Firma de Código (Code Signing):** Son empleados por programadores para autenticar digitalmente sus aplicaciones y software. Esto asegura a los usuarios finales que el programa proviene de un desarrollador reconocido y que no ha sufrido modificaciones desde su autenticación [12].
- **Certificados para Correo Electrónico (S/MIME):** Estos certificados permiten a los usuarios verificar la identidad del remitente y proteger el contenido de los correos mediante cifrado. La firma digital asegura que el mensaje no haya sido alterado y proviene de una fuente confiable, mientras que el cifrado impide que terceros accedan a la información [13].
- **Certificados de Identificación Personal (o de Cliente):** Su uso principal es la firma electrónica de documentos, dado que permiten unir de manera segura y legal a un individuo con un documento, asegurando la autoría y evitando el repudio [14].

2.4.2 Ciclo de vida de un certificado digital

Un certificado digital tiene un período de validez determinado y debe ser gestionado adecuadamente por la Infraestructura de Clave Pública (PKI) para garantizar que siga siendo confiable y auténtico a lo largo del tiempo. Este proceso incluye cada etapa que experimenta un certificado, desde su emisión hasta que se vuelve inválido, ya sea por caducidad o por revocación. La adecuada gestión de este proceso es crucial para preservar la solidez y la confianza en el sistema de firmas electrónicas [15].

Las etapas que conforman el ciclo de vida de un certificado digital son las siguientes:

- **Solicitud**: Esta fase marca el comienzo del ciclo de vida del certificado. En ella, el solicitante (un estudiante) inicia el proceso pidiendo la emisión de un certificado digital a su nombre. Para iniciar el trámite, el interesado debe presentar una petición formal ante la Autoridad de Registro (RA), junto con la

documentación e información requerida que respalde su identidad de manera verificable.

- **Emisión**: Una vez que la Autoridad de Registro (RA) ha corroborado y dado el visto bueno a la identidad de quien solicita el certificado, la petición se envía a la Autoridad de Certificación (CA) para su correspondiente emisión. Posteriormente, la CA genera el certificado digital y lo firma con su clave privada para garantizar su autenticidad. Finalmente, el certificado se entrega al solicitante.
- **Confirmación**: Tras la emisión del certificado, el titular debe proceder con su aceptación formal para completar el proceso. Esta etapa implica revisar que los datos contenidos en el certificado sean precisos y asumir el compromiso de utilizarlo de forma responsable. Generalmente, se otorga un plazo determinado para que el usuario verifique la información y, en caso de encontrar errores, solicite su revocación inmediata.
- **Renovación**: Un certificado digital tiene un tiempo de vigencia determinado. Antes de que ese tiempo finalice, el poseedor puede pedir una renovación para recibir un nuevo certificado y asegurar la continuidad del servicio. Este procedimiento generalmente requiere la creación de un nuevo par de claves criptográficas para el poseedor.
- **Suspensión**: Esta fase implica la desactivación temporal del certificado. Puede iniciarse a petición del propietario del certificado o en casos donde se sospeche un posible compromiso de la clave privada. Mientras está suspendido, el certificado aparece en la Lista de Certificados Revocados (CRL) y puede ser reactivado si se resuelve la causa que originó la suspensión.
- **Revocación**: Es el proceso de invalidar definitivamente un certificado digital antes de que finalice su fecha de vencimiento. La revocación puede suceder por varias razones, como la pérdida o compromiso irreversible de la clave privada, el uso inapropiado del certificado, la verificación de inexactitudes en los datos suministrados por el poseedor o por el incumplimiento de las políticas establecidas.
- **Expiración**: Si un certificado no se renueva, al alcanzar la fecha final de su plazo de validez, este expira automáticamente y deja de ser operativo para llevar a cabo nuevas firmas o autenticaciones.

2.5 Infraestructura de clave pública (PKI)

Una infraestructura de clave pública se fundamenta en la aplicación de tecnologías informáticas y normas de seguridad, entre otros aspectos, para gestionar y supervisar la emisión de certificados digitales, los cuales tienen múltiples aplicaciones, incluyendo la firma electrónica. La esencia de esta infraestructura está delineada en la recomendación ITU-T X. 509. X. 509 representa un estándar que describe el formato de los certificados digitales que son generados por una infraestructura de clave pública. Este estándar especifica la información que deben contener los certificados digitales en relación con la identidad de un individuo. Adicionalmente, se debe incluir información complementaria como el período de vigencia del certificado y la denominación de la entidad que lo ha emitido.

2.5.1 Componentes de una PKI

Una infraestructura de clave pública se integra por los siguientes componentes:

- **Entidad Certificadora:** Es una organización responsable de expedir los certificados digitales a los usuarios finales.
- **Almacén de Claves Públicas:** Es un repositorio para almacenar las claves públicas de los usuarios.
- **Normativa de Certificación:** Comprende todas las reglas que dicta la Entidad Certificadora para la correcta gestión de los certificados digitales. En esencia, este reglamento define los procedimientos para emitir, renovar y cancelar los certificados, gobernando así todo su ciclo de vida.
- **Certificado Electrónico**: Funciona como un documento de identidad digital. Es un archivo que contiene los datos para identificar a una persona, incluyendo un par de claves criptográficas, y toda esta información está organizada según la normativa del estándar X.509.
- **Sistema de Validación**: Es un grupo de servicios que permiten comprobar y certificar la validez de los certificados digitales, así como supervisar su ciclo de vida.

2.5.2 Escalabilidad y resiliencia en la PKI

La implementación de un sistema de firma electrónica sustentado en una infraestructura de clave pública (PKI) debe considerar no solo su funcionamiento inicial y nivel de seguridad, sino también su capacidad de adaptación frente al crecimiento de

usuarios, nuevas exigencias y posibles contingencias. La escalabilidad resulta esencial para permitir que el sistema soporte un aumento progresivo en el volumen de operaciones sin que ello afecte su desempeño. Una infraestructura robusta debe ser lo suficientemente flexible como para ampliarse y cubrir tanto a toda la comunidad universitaria como a otras instituciones que puedan requerir su uso en el futuro.

En este contexto, la arquitectura del sistema desempeña un papel clave. Aunque en una etapa inicial el servicio podría ser implementado en un único servidor, para lograr alta disponibilidad se recomienda distribuir los servicios críticos de la PKI, como la Autoridad de Registro (RA) y la Autoridad de Certificación (CA), en distintos servidores. Esta segmentación ayuda a prevenir sobrecargas y garantiza la continuidad operativa, lo que resulta indispensable para mantener la fiabilidad del servicio.

Además, la capacidad de recuperación ante fallos forma parte fundamental de la resiliencia del sistema. Por ello, es necesario establecer protocolos que permitan enfrentar incidentes o desastres, asegurar la operación continua en caso de interrupciones eléctricas y proteger los datos mediante copias de seguridad programadas. Un centro de datos adecuado, equipado con sistemas redundantes de alimentación eléctrica, se convierte en un componente clave para asegurar la estabilidad del servicio. Estas consideraciones técnicas no solo fortalecen la confianza en la solución, sino que también son determinantes para alcanzar su certificación oficial y garantizar su sostenibilidad a largo plazo.

2.6 **Estructura PKI**

Una estructura de PKI es un sistema sistematizado de certificados digitales que establece vínculos de confianza entre las entidades que los emiten y los que los utilizan. Una estructura de PKI (Infraestructura de Clave Pública) es, en esencia, una jerarquía de Autoridades de Certificación (CA). Esto significa que está organizada en varios niveles, y cada uno de ellos cuenta con su propia CA. Se sugiere emplear este tipo de estructura para tener un control más efectivo en la emisión de certificados digitales. En este marco, se aconseja implementar una jerarquía de al menos dos niveles, compuesta por una Autoridad Certificadora Raíz (RootCA) y varias Autoridades Certificadoras Subordinadas (SubCA) según las necesidades. De este modo, una RootCA solo emite certificados a SubCA's, y estas son responsables de emitir certificados solo a las entidades finales o de establecer niveles adicionales de SubCA. Esto permitiría que la duración de

la RootCA se mantenga por más tiempo o que tenga una mayor vida útil, mientras que una SubCA podría tener un ciclo de vida más corto e incluso ser eliminada. Gracias a este enfoque, se minimiza la necesidad de renovar o sustituir los certificados de la CA Raíz. En el contexto de una PKI, también se incluyen entidades como la Autoridad de Registro (RA), la Autoridad de Validación (VA), las Entidades Finales (EE) y el Auditor, cuyas funciones se explican a continuación:

- **Autoridad de Registro (RA):** Se puede considerar como un conjunto de servicios diseñados para manejar la duración de los certificados digitales, así como para llevar a cabo el registro de los usuarios, asegurando la validación de su información. En una estructura jerárquica de PKI, puede haber varias RA según sea necesario.
- **Autoridad de Validación (VA):** Esta es la entidad responsable de examinar y certificar los certificados digitales que están en el repositorio de certificados, lo que implica verificar si un certificado todavía es válido o si ha sido revocado, entre otras funciones.
- **Auditor**: Es el encargado de revisar y evaluar los registros del sistema, asegurando el cumplimiento de los procedimientos establecidos.
- **Entidad Final (EE):** Esta entidad puede aludir a una persona o usuario que busca obtener un certificado digital, pero en otros contextos puede referirse también a aparatos como un servidor. La Validación de Autoridad se compone, a su vez, de un conjunto de servicios destinados a confirmar la autenticidad de un certificado digital, los cuales se detallan a continuación.
- **CRL**: Corresponde a las iniciales en inglés de *Certificate Revocation List*, lo que en español significa Lista de Certificados Revocados. Se trata de un documento que incluye los identificativos de todos los certificados que han sido anulados. Para acceder a este documento, se establece un punto final en la Autoridad de Certificación desde el cual se puede descargar. Este punto final es empleado por la Autoridad de Validación. El inconveniente es que este documento puede crecer significativamente a medida que se revocan certificados digitales, por lo que se implementa el siguiente servicio.
- **OCSP**: Se refiere al Online Certificate Status Protocol, que en español es protocolo de estado de certificados en línea. También se trata de un punto final que se configura en la autoridad de certificación para su uso en la autoridad de

validación. A diferencia del CRL, este punto final permite verificar un solo identificador de certificado a la vez, sin requerir la descarga completa de la lista de certificados revocados.

2.7 Arquitecturas de PKI

Cuando se mencionan las arquitecturas de infraestructura de clave pública, se trata de la forma en que se puede establecer y crear una jerarquía de PKI.

- **Estructura simple**: Esto se refiere a una PKI que se ejecuta en un único servidor. Este tipo de configuración es de las más fáciles de poner en práctica, donde toda la jerarquía de PKI reside en un solo servidor. Sin embargo, en cuanto a eficiencia, no suele ser la opción más óptima, ya que puede causar que el servidor se sature.
- **Estructura distribuida:** Esta configuración implica la implementación de una jerarquía de PKI en diversos servidores. Por ejemplo, la Autoridad Certificadora Raíz (RootCA) y una SubCA pueden alojarse en un mismo servidor, mientras que las Autoridades de Registro (RA) y de Validación (VA) se distribuyen en distintos servidores.
- **Estructura híbrida**: Las arquitecturas previamente descritas se consideran privadas, ya que todo su funcionamiento se encuentra alojado dentro de la propia organización. Por otro lado, en una arquitectura híbrida, la infraestructura de clave pública (PKI) se establece utilizando tanto componentes instalados localmente como servicios alojados en la nube. Por ejemplo, las Autoridades Certificadoras principales, como la RootCA, pueden estar instaladas en la infraestructura interna, mientras que otras entidades como las RA pueden operar desde la nube.

2.8 Operatividad de una PKI

El funcionamiento de una PKI requiere la colaboración de todas las partes mencionadas previamente. En primer lugar, un usuario final solicita su certificado digital a la autoridad de registro, proporcionando información personal como su nombre completo, correo electrónico, número de teléfono, entre otros. La autoridad de registro examina la solicitud y verifica los datos entregados por el usuario final. Si la solicitud es adecuada, se envía una notificación a la autoridad certificadora para que emita un nuevo certificado digital para el usuario final.

A continuación, cuando el usuario final utiliza el certificado digital para firmar un documento, la persona que reciba este documento firmado y lo abra con un software

especializado, como Adobe Reader, al abrirlo envía una solicitud a la autoridad de validación para comprobar si el certificado digital usado para la firma sigue siendo válido o ha sido revocado. Esta comprobación se lleva a cabo mediante servicios CRL y OCSP.

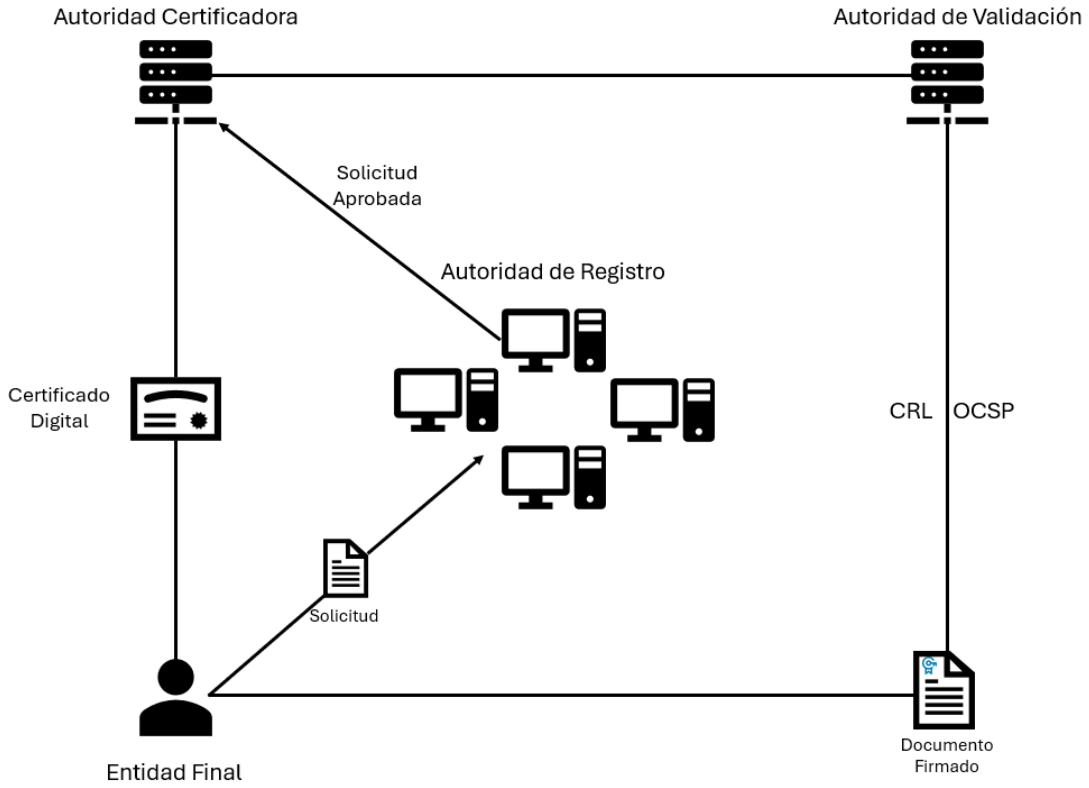


Figura: 8 Funcionamiento de una PKI

2.9 **Tecnologías utilizadas para la instauración de PKI**

Cuando nos referimos a tecnologías para establecer una PKI, hablamos de la utilización de programas de software que nos ayuden a lograr este objetivo. La implementación de estos servicios no exige una gran recopilación de software; hay proyectos o marcos ya existentes que facilitan la creación de este tipo de servicio, como PGP, OPENCA, EJBCA o XCA.

Cada una de estas soluciones presenta sus pros y contras, aunque, según el análisis realizado por (Carrera López & Celi Jiménez, 2022) sobre las características y capacidades de las soluciones evaluadas, OPENCA y EJBCA destacan como las opciones más viables para la implementación del servicio, siendo EJBCA la más recomendada debido a su disponibilidad como software libre y su mayor compatibilidad funcional [15].

A pesar de que esta herramienta proporciona lo necesario para establecer una PKI, hay otras soluciones que pueden ser útiles durante el proceso, como un sistema de gestión de bases de datos que asegure la conservación de la información generada en tiempo real y tecnologías de virtualización que permitan un mejor control del entorno de ejecución. En este contexto, se puede mencionar a MariaDB como sistema de gestión de bases de datos y a Wildfly 32 como servidor de aplicaciones.

2.9.1 EJBCA

La Autoridad Certificadora de Enterprise Java Bean es una de las soluciones de infraestructura de clave pública más reconocidas a nivel mundial. Incluye todos los elementos requeridos de una PKI, como la entidad certificadora, la entidad de registro y la entidad de validación [16].

EJBCA es un proyecto de código abierto respaldado por la empresa Keyfactor, y se distribuye bajo la licencia LGPL versión 2.1, lo que permite su descarga y uso sin ningún costo [16].

EJBCA es compatible con diferentes plataformas, brindando versatilidad y expansión para casi cualquier aplicación de PKI, que abarca DevOps, Internet de las Cosas, IoT Industrial, PKI empresarial y más. Además, permite integraciones fluidas con sistemas externos para lograr una automatización completa y una operación simplificada. Permite múltiples usuarios y puede gestionar varias CA y PKI en una única instalación del servidor [16].

2.9.2 Wildfly 32

Wildfly 32 es un servidor de aplicaciones Java EE y Jakarta EE de código abierto, diseñado para ejecutar aplicaciones empresariales con alto rendimiento, escalabilidad y eficiencia. Su arquitectura modular permite cargar únicamente los componentes necesarios, optimizando el uso de los recursos del sistema y rediciendo los tiempos de inicio.

Además, ofrece servicios integrados como gestión de transacciones, seguridad, mensajería, persistencia y balanceo de carga, lo que facilita el desarrollo y despliegue de aplicaciones robustas y seguras. De esta forma, Wildfly 32 se consolida como una plataforma completa y flexible para el desarrollo de soluciones empresariales basadas en Java [17].

2.9.3 Java JDK 21

Java JDK 21 es la versión más reciente del kit de desarrollo de Java (Java Development Kit), que proporciona las herramientas esenciales para compilar, ejecutar y depurar aplicaciones desarrolladas en el lenguaje Java.

Esta versión se distingue por su escalabilidad a largo plazo (LTS), Ofreciendo mejoras significativas en rendimiento, seguridad y productividad para los desarrolladores

Además, mantiene la compatibilidad con versiones anteriores, asegurando que las aplicaciones existentes puedan ejecutarse sin modificaciones. En conjunto, Java JDK 21 consolida la evolución de la plataforma Java, proporcionando un entorno moderno, eficiente y seguro para el desarrollo de software empresarial y de propósito general [18].

2.9.4 Apache ANT

Apache ANT Es una herramienta de automatización de compilación desarrollada en Java, hola utilizada principalmente para compilar, ensamblar, probar y desplegar aplicaciones basadas en este lenguaje. Se fundamenta en el uso de archivos XML denominados build.xml, donde se definen las tareas y dependencias necesarias para la construcción de un proyecto.

A diferencia de los sistemas de compilación tradicionales, ANT ofrece un enfoque flexible y extensible, permitiendo personalizar el proceso de construcción mediante la creación de tareas específicas y el uso de propiedades configurables. Su independencia de plataforma y su integración con diversas herramientas de desarrollo lo convierten en un componente esencial dentro del ciclo de vida del software en entornos Java.

En esencia, Apache ANT proporciona una manera estructurada, automatizada y reproducible de gestionar los procesos de compilación y despliegue, hp garantizando coherencia y eficiencia en el desarrollo de aplicaciones empresariales [19].

2.9.5 MariaDB

Se trata de una base de datos relacional derivada de MySQL, impulsada por la comunidad y distribuida como software libre bajo la licencia GPL v2, lo que garantiza su disponibilidad abierta y gratuita para diversos entornos. Se considera que es una alternativa optimizada de MySQL, proporcionando más características que potencian la escalabilidad y eficacia de las bases de datos durante la ejecución de consultas SQL [20].

2.10 **Marco legal y normativo en Ecuador**

En relación con las regulaciones y directrices que gobiernan el comercio digital, las firmas electrónicas y los certificados digitales, es fundamental conocer y adherirse a un conjunto de leyes y normativas. En la legislación de Ecuador, hay múltiples iniciativas que subrayan la relevancia de las políticas y procesos en las operaciones realizadas de manera electrónica.

2.10.1 Ley de comercio electrónico, firmas y mensajes de datos

La legislación ecuatoriana sobre Comercio Electrónico, Firmas y Mensajes de Datos (LEC), que fue aprobada el 10 de abril del año 2002 y posteriormente actualizada, regula las transacciones comerciales que se efectúan mediante plataformas electrónicas en el país. Su propósito primordial es proporcionar un marco legal que favorezca y controle el uso del comercio a través de internet, así como las firmas digitales y los mensajes electrónicos, con el fin de simplificar las transacciones en línea y ofrecer seguridad y confianza a todos los involucrados.

Desde 2002, esta normativa reconoce legalmente a los mensajes electrónicos, otorgándoles el mismo peso que los documentos impresos. Además, estos mensajes cuentan con protección en aspectos como la propiedad intelectual, la privacidad y la confidencialidad. Por lo tanto, la legislación prohíbe las intromisiones electrónicas, la transferencia no autorizada de mensajes y la infracción de la confidencialidad profesional.

Además, los mensajes electrónicos deben ser guardados bajo ciertas condiciones y requieren el permiso del propietario para ser generados. Por último, la LEC establece que las bases de datos pueden ser transmitidas o empleadas solo con el consentimiento del propietario o de la autoridad correspondiente. Cada mensaje electrónico es único y se puede solicitar su confirmación y la verificación técnica de su autenticidad [21].

2.10.2 Interoperabilidad y reconocimiento de certificados

La efectividad de un servicio de firma electrónica, especialmente uno basado en una Infraestructura de Clave Pública (PKI) universitaria, no solo reside en su robustez interna, sino también en su capacidad para interactuar y ser reconocido por otras infraestructuras y sistemas tanto a nivel nacional como internacional. La interoperabilidad garantiza que los certificados digitales emitidos por la PKI de la FICA-UTN puedan ser validados y aceptados por terceros, mientras que el reconocimiento legal asegura su validez jurídica en diversos contextos.

En el contexto ecuatoriano, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (LEC) es el marco normativo fundamental que establece la equiparación y validez de la firma manuscrita con la firma digital para actos judiciales y transacciones comerciales electrónicas. La ley concede validez legal a los mensajes de datos, siempre que cumplan con condiciones relacionadas con la protección de la información, tales como derechos de autor, privacidad y confidencialidad, considerándolos equivalentes a los documentos en papel. Específicamente, el Artículo 14 de la LEC detalla que la firma electrónica posee la misma validez y efectos jurídicos que la firma manuscrita, siendo aceptada como prueba en juicios [22].

Para que un certificado digital tenga validez legal, debe ajustarse a lo establecido en el Artículo 22 de la LEC. Esto implica incluir datos como la identificación de la entidad emisora, su domicilio jurídico, la información del titular, el método utilizado para la verificación, incluyendo detalles como cuándo fue emitido y hasta cuándo es válido, un identificador exclusivo del certificado, y la firma digital emitida por la entidad que lo certifica. Además, el Artículo 28 de la misma ley aborda el reconocimiento internacional, indicando que las entidades de certificación extranjeras que cumplan los requisitos de la ley ecuatoriana y demuestren un nivel equivalente de garantía tendrán el mismo valor legal que los certificados acreditados en Ecuador.

Sin embargo, es crucial distinguir entre entidades de certificación acreditadas y no acreditadas. En Ecuador, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es el organismo de control gubernamental encargado de otorgar la acreditación a entidades de certificación de la información. Entidades como el Banco Central del Ecuador, el Consejo de la Judicatura, Security Data y ANFAC Autoridad de Certificación del Ecuador, entre otras, están acreditadas para la emisión de certificados digitales y servicios relacionados, cumpliendo con normas y estándares nacionales e internacionales. Estas entidades acreditadas gozan de privilegios, como la obligatoriedad de que el sector público acceda a sus servicios de certificación.

En contraste, los certificados emitidos por entidades de certificación no acreditadas, aunque estén registradas y presten sus servicios, no han sido acreditados por el CONATEL (ahora ARCOTEL). Esto implica que la responsabilidad de probar la fiabilidad, seguridad y eficiencia técnica de los procesos de vida de los certificados recae en el usuario. Un ejemplo de esto es la "Implementación de una PKI no acreditada" en la ESPE, donde si bien se logró una PKI operativa para generar certificados digitales, estos

carecen del mismo reconocimiento legal que aquellos de organizaciones acreditadas, lo que significa que los usuarios necesitan validar su autenticidad si es preciso, y su uso está restringido en el ámbito público.

El estándar ITU-T X.509 proporciona un formato estructurado para certificados digitales, facilitando su compatibilidad en entornos diversos, lo que mejora la interoperabilidad entre sistemas.

. Este formato garantiza que se incluya la información esencial para identificar al titular, definir su periodo de validez y especificar la autoridad certificadora responsable de su emisión. El aprovechamiento de tecnologías libres como EJBCA que se ajustan a los lineamientos de X.509 e IETF.PKIX permite construir infraestructuras adaptables, con la capacidad de conectarse a plataformas externas y soportar procesos automatizados con eficiencia. No obstante, la ausencia de una acreditación oficial podría representar una limitación para su escalamiento dentro del ámbito universitario o al colaborar con instituciones gubernamentales [23].

Por lo tanto, la interoperabilidad y el reconocimiento de los certificados emitidos por la PKI de la FICA-UTN dependerán en gran medida de la alineación con los requisitos de ARCOTEL para una futura certificación. De este modo, se garantiza que las firmas electrónicas sean reconocidas no solo dentro de la institución, sino también en procesos externos, brindándoles validez legal y aumentando la credibilidad en la digitalización y administración de documentos estudiantiles.

2.11 **Trabajos similares**

Ampuero Herrera (2021) implementó una plataforma de firma electrónica con la intención de mejorar la generación de documentos académicos en la Universidad Nacional de Barranca, lo que, a su vez, busca aumentar la satisfacción de los alumnos y la administración documental. La investigación utilizó un enfoque cuantitativo con una estructura preexperimental y se fundamentó en el marco ágil SCRUM para su realización, empleando métodos como entrevistas y encuestas para recopilar información. El hallazgo más significativo indicó una variación considerable tras la implementación, con un p-valor de $0.000 (< 0.05)$, concluyendo que el sistema mejoró la producción de documentos y fue satisfactorio para los estudiantes, logrando que el 92% de los documentos se emitieran en un día laboral. Como limitación, la investigación se centró en la producción de ciertos documentos académicos y no se extendió al uso de la firma digital en otros

trámites administrativos o educativos, como la firma de actas finales por parte de los docentes, ni a la compra de tokens criptográficos o la creación de un repositorio institucional central para certificados digitales [24].

Vela Gonzales y Macedo Rojas (2019) crearon y pusieron en marcha una plataforma en línea con firma digital y certificado electrónico en el SENATI Zonal Loreto, buscando optimizar la administración de calificaciones al permitir a los profesores confirmar y proteger la información ingresada en el sistema ERP. La metodología utilizada fue de carácter tecnológico, utilizando un diseño cuasiexperimental con un solo grupo, que abarcó la recopilación de datos a través de encuestas antes y después de la implementación con una muestra de 15 docentes. El hallazgo más significativo mostró una relación directa y relevante ($r=0.562$, $p<0.05$) entre la puesta en marcha de la aplicación y la mejora en la administración de calificaciones, con un 60% de los profesores considerando el proceso seguro y un 27% como muy seguro tras la implementación, evidenciando un notable incremento en la percepción de confianza. No obstante, una limitación es que el estudio se enfocó en la validación y seguridad de las calificaciones sin abordar la optimización de los procedimientos administrativos de gestión de calificaciones en términos de eficiencia o reducción de tiempos. Además, la sugerencia de obtener certificados digitales de entidades reconocidas y la ausencia de un análisis sobre la implementación a gran escala de una infraestructura de clave pública o los costos y desafíos relacionados con la adquisición masiva de certificados externos, indican una carencia en la solución integral para una institución más grande como SENATI [25].

Carrera López y Celi Jiménez (2022) establecieron un sistema de clave pública no verificado en el Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, con el objetivo de asegurar la integridad y la autoría de documentos digitales debido a la creciente desconfianza en el intercambio de información. Se utilizó la metodología de Investigación Científica del Diseño, centrada en la creación de un artefacto, empleando software libre como EJBCA para gestionar el ciclo de vida de los certificados digitales, junto con Apache Ant y MySQL Server para la implementación de la infraestructura. El principal logro fue la exitosa creación e implementación de una PKI operativa que genera certificados digitales, lo que permite a los usuarios realizar firmas electrónicas, mejorando la seguridad y la confianza en el intercambio de información digital. Sin embargo, una de las limitaciones más importantes

es que, al ser una PKI "no verificada", los certificados otorgados no tienen el mismo reconocimiento legal que aquellos de organizaciones acreditadas, lo que significa que los usuarios necesitan validar su autenticidad si es preciso, y su uso está restringido en el ámbito público. Esto implica que, a pesar de la implementación técnica, la solución carece del respaldo legal completo necesario para una adopción amplia en instituciones o para la interoperabilidad con otras entidades gubernamentales [15].

Vermejo Ruiz (2020) sugirió la creación y puesta en marcha de la estructura oficial del Sistema Nacional de Firma Electrónica y Certificados Digitales en Perú, con el objetivo de facilitar intercambios electrónicos seguros y ayudar en la modernización y descentralización del gobierno. Esta iniciativa, de alcance nacional y a nivel estatal, se fundamentó en el análisis de viabilidad del Sistema Nacional de Inversión Pública (SNIP) y en la legislación vigente sobre Firmas y Certificados Digitales. La propuesta técnica abarcó la determinación de las necesidades de hardware y software (incluyendo servidores, cortafuegos y dispositivos de almacenamiento), un diseño exhaustivo de la infraestructura física con áreas de seguridad, así como la creación de una Autoridad Administrativa Competente (AAC) para la acreditación y supervisión, así como de una Autoridad de Emisión y Registro de Certificados del Estado (AERC). La implementación más significativa fue la formación de la AAC en INDECOPI y la AERC en RENIEC, lo que facilitó la creación de empresas de forma digital y la firma de más de un millón de documentos en el sistema de gestión documental, generando importantes ahorros y acelerando procesos. No obstante, el autor menciona como una limitación la inestabilidad política y el enfoque en intereses institucionales en lugar de atender las necesidades del ciudadano, lo que ha dificultado que estas iniciativas alcancen los beneficios previstos dentro de los plazos establecidos, además de la confusión técnica provocada por la inclusión de la tecnología de microformas en la legislación de firma digital y la exigencia de certificaciones CMMI innecesarias que restringen la interoperabilidad [26].

Arcos Poma y Espín Flores (2022) llevaron a cabo el funcionamiento y optimización del sistema de firma electrónica del ESPE-CERT en el área de Ciencias de la Computación de la ESPE, siguiendo las pautas de ITIL V4, con el objetivo de validar digitalmente documentos para la comunidad educativa. La metodología Design Science Research dirigió esta labor, que abarcó la creación de una PKI (implementando EJBCA, Docker y MySQL), la gestión del servicio para estudiantes, docentes y personal administrativo, junto con una evaluación de la usabilidad y funcionalidad mediante

encuestas. El hallazgo más significativo fue el alto grado de satisfacción entre los usuarios, quienes consideraron que la firma digital era accesible (64. 4%), muy útil (80%), y no encontraron ninguna complejidad superflua en el sistema (48. 9%), logrando avances notables en el manejo de certificados y documentos. No obstante, el análisis no cubre cómo se manejaría la certificación externa con ARCOTEL para dar validez legal a la firma más allá de la institución, ni ofrece un esquema para la recuperación ante desastres, lo cual limita la capacidad de expansión y la robustez del servicio en un contexto universitario más extenso [27].

Otavalo Arrayan (2020) llevó a cabo la implementación de un módulo para firmas digitales en el Sistema Integrado de Actividad Docente (SIAD) de la Carrera de Software en la UTN, con la intención de automatizar la entrega de documentos mediante un token criptográfico y aplicando el estándar X. 509 de la Infraestructura de Clave Pública. Este desarrollo se realizó dentro del marco de trabajo ágil SCRUM y se utilizó la API del Registro Civil de Ecuador como parte del proceso, además de emplear bibliotecas como iText-Pdf y Rúbrica para la firma y verificación de documentos. Como consecuencia, la aplicación facilita la firma y validación de documentos, así como la confirmación de la validez de certificados digitales, adhiriéndose al estándar X. 509 y aportando beneficios ecológicos al disminuir la utilización de papel. No obstante, una limitación significativa es que la biblioteca Bouncy Castle y la misma Rúbrica no fueron compatibles con el sistema SIAD creado en Eclipse, lo que sugiere posibles dificultades en la integración y mantenimiento en el futuro si el entorno de desarrollo de la UTN cambia o si se necesitan personalizaciones adicionales para estas funciones, además de no examinar las repercusiones de una PKI interna o la gestión de certificados a gran escala [28].

Galarza-Pauta y Criollo-Bonilla (2024) presentaron un enfoque para validar firmas y certificados digitales incorporados en documentos electrónicos creados por alumnos de la Universidad Católica de Cuenca, con el objetivo de garantizar la autenticidad, integridad y no repudio de la documentación frente a falsificaciones y errores en trámites en persona. El estudio se llevó a cabo en tres etapas metodológicas: una revisión del contexto actual, un análisis situacional para detectar problemas y variables, y la aplicación de métodos hipotéticos y experimentales para desarrollar una solución innovadora. El enfoque se fundamentó en la encriptación asimétrica (RSA, ECDSA) y subrayó la relevancia de contar con una infraestructura de clave pública (PKI) sólida, delineando un procedimiento de verificación en seis etapas para garantizar la

validez de las firmas. El principal resultado es la creación de un marco robusto para implementar este modelo, que mejora la gestión documental y promueve la confianza, además de demostrar una alta fiabilidad en las variables evaluadas mediante el coeficiente Alfa de Cronbach. No obstante, el artículo no aborda en profundidad las repercusiones legales y normativas relacionadas con la ejecución del modelo, ni presenta un plan específico para la inversión necesaria en la infraestructura tecnológica sólida que dicha ejecución demanda, dejando sin respuesta la cuestión de la sostenibilidad y el ámbito formal de la validación [29].

CAPÍTULO III

DESARROLLO

En el siguiente capítulo se describe el proceso de implantación del servicio de firma electrónica en la FICA-UTN, detallando los objetivos, alcance, recursos, indicadores de cumplimiento y actividades realizadas. Se explica la configuración de la jerarquía PKI, la instalación y personalización de EJBCA Community, la arquitectura del sistema, la capacitación de usuarios y las pruebas de funcionamiento. Asimismo, se incluye el análisis de amenazas, la investigación sobre requisitos de certificación legal y la estimación presupuestaria para una posible acreditación formal.

3.1 Implantación del servicio de firma electrónica.

3.1.1 Objetivos

- Implantar el servicio de firma electrónica en la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

3.1.2 Alcance

Realizar una implementación del servicio de Firma Electrónica en la Facultad de Ingeniería en Ciencias Aplicadas (FICA), con un plazo estimado de un mes a partir del inicio de la implantación. La fase inicial estará orientada a los estudiantes de la carrera de Ingeniería en Software, quienes serán los primeros en disponer del sistema, lo que permitirá validar su funcionamiento en un entorno controlado. Posteriormente, se prevé la ampliación progresiva del servicio hacia los estudiantes de las demás carreras que conforman la facultad FICA, garantizando así una cobertura integral dentro de la misma. La implementación se considerará culminada cuando los estudiantes de las distintas carreras de la facultad FICA cuenten con el servicio plenamente operativo.

3.1.3 Indicadores de cumplimiento

- Disponibilidad del sistema.
- Plazo de entrega.
- Incidencias y defectos.

3.1.4 Recursos

Todo lo concerniente con el hardware y la infraestructura física es provisto por la Universidad Técnica del Norte, específicamente a través de la Facultad de Ingeniería en Ciencias Aplicadas, mediante el Laboratorio de Sistemas. Este laboratorio se ocupa de ofrecer los recursos tecnológicos requeridos para la implementación exitosa del proyecto. Además de asegurar la accesibilidad a los equipos y a la infraestructura necesaria, que se necesita para la etapa de implementación y operación del sistema, garantizando de esta manera un entorno propicio para su rendimiento eficaz.

RECURSOS**:**	
Humanos	Se dispone de un alumno que está a cargo del proyecto de titulación, con la ayuda y supervisión del director de tesis de este.
Financieros	Para esta implantación no se requieren recursos financieros.
Hardware	Un servidor disponible en el Laboratorio de Sistemas.
Software	EJBCA Community, MariaDB, Wildfly32, Java JDK, Apache ANT, Visual Code, Alma Linux.
Conocimientos	Investigación previa.

Tabla 2 Descripción de recursos utilizados para la fase de implantación.

3.1.5 Actividades a realizar

La siguiente tabla explica el cronograma con todas las actividades a realizar, que son necesarias para la fase de implementación del sistema.

Tarea	Responsable	Duración	Comienzo	Fin
Diseño de una jerarquía PKI.	Tesista	2 días	08 sep.	09 sep.
Diseño de la arquitectura del servicio de firma electrónica.	Tesista	2 días	10 sep.	11 sep.
Descarga y personalización del software EJBCA Community.	Tesista	8 días	12 sep.	23 sep.
Descarga, instalación y configuración de herramientas necesarias.	Tesista	1 días	24 sep.	24 sep.

Instalación del software EJBCA Community.	Tesista	2 día	25 sep.	26 sep.
Configuración del servicio de firma electrónica.	Tesista	5 días	29 sep.	03 oct.
Capacitación de usuarios.	Tesista	10 días	06 sep.	17 oct.
Operación y pruebas del servicio.	Tesista	10 días	20 oct.	31 oct.

Tabla 3 Actividades para la implantación del servicio de firma electrónica.

3.1.6 Ejecución de actividades

En esta sección se describe de manera detallada el proceso de instalación y configuración general de la herramienta EJBCA, así como todos los pasos necesarios para asegurar el correcto funcionamiento de la infraestructura de clave pública (PKI). Es importante mencionar que, antes de este proceso, se llevó a cabo la instalación del sistema operativo AlmaLinux, cuyo manual completo se encuentra en la sección de anexos (**Anexo D**).

3.1.6.1 Diseño de una jerarquía PKI

Durante la etapa de investigación sobre la firma digital, se descubrió que es esencial poseer o crear certificados digitales para su uso, los cuales se generan mediante un sistema de clave pública. Por lo tanto, la creación de un servicio para la firma electrónica inicia con el establecimiento de una PKI con todos los componentes y estándares necesarios. Una jerarquía de clave pública forma una estructura organizada que refuerza la confianza y regula el proceso de emisión de certificados digitales. Esta jerarquía se compone de diferentes niveles de certificación, donde las entidades de mayor rango se encargan de autorizar o certificar a aquellas de menor rango. Con base en ello, se ha elaborado la siguiente jerarquía de clave pública.

Jerarquía PKI

Componente	Descripción	Funciones principales	Ejemplo en el proyecto
RootCA (Autoridad Certificadora Raíz)	Nodo principal de la jerarquía PKI, entidad de mayor nivel que se autofirma.	- Autorizar y firmar a las Autoridades Certificadoras Subordinadas.	Universidad Técnica del Norte.

		-Emitir certificados digitales a niveles inferiores. - Mantener la máxima confianza en la jerarquía.	
SubCA (Autoridad Certificadora Subordinada)	Entidad ubicada en un nivel jerárquico inferior al RootCA, firmada por esta.	- Emitir certificados digitales únicamente a las Entidades Finales. - No está autorizada para certificar a otras autoridades. - Permite segmentar y descentralizar la gestión de certificados.	Facultad de Ingeniería en Ciencias Aplicadas (FICA).
EE (End Entities / Entidades Finales)	Usuarios finales que reciben y utilizan los certificados digitales.	- Representar a los estudiantes. - Permitir la autenticación y uso de la firma electrónica. - Incluir roles administrativos como Autoridades de Registro y Superadministrador.	Estudiantes de la facultad FICA, autoridades de registro y superadministrador de la PKI.

Tabla 4 Jerarquía PKI.

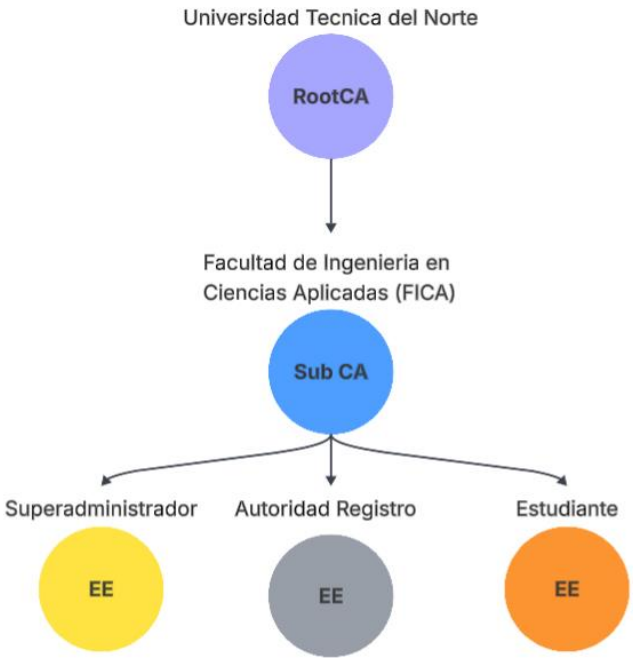


Figura: 9 Diseño de la jerarquía PKI.

Como se aprecia en el diagrama, se encuentran representados los componentes principales de la jerarquía PKI definida para este proyecto. En la parte superior se establece el nodo raíz, correspondiente a la Universidad Técnica del Norte, el cual cumple la función de autoridad certificadora raíz (RootCA) y constituye a la máxima entidad de confianza dentro de la infraestructura. Este nodo otorga validez al siguiente nivel jerárquico, representado por la Facultad de Ingeniería en Ciencias Aplicadas (FICA), que actúa como autoridad certificadora subordinada (SubCA). A su vez, la SubCA es responsable de emitir certificados digitales a las entidades finales (EE), entre las que se incluyen el superadministrador, la autoridad de registro y los estudiantes de la facultad, quienes serán los principales usuarios del servicio de firma electrónica.

3.1.6.2 Diseño de la arquitectura del servicio de firma electrónica.

A continuación, se describe la estructura de la implementación del servicio de firma digital.

Para la implementación del servicio de firma electrónica en la Universidad Técnica del Norte, se dispuso de un servidor que cumple funciones específicas: se instauró el software necesario para la creación de la infraestructura de clave pública (PKI), además de configurar el motor de base de datos MariaDB, destinado a almacenar certificados digitales, claves criptográficas y demás información relacionada (ver Figura 2).

Una vez finalizada la instalación tanto del servicio de la base de datos como del sistema PKI, se procedió con la configuración del entorno, lo cual incluyó la habilitación de la emisión de certificados digitales, la definición de roles y la aplicación de reglas de acceso, de acuerdo con la jerarquía PKI diseñada previamente.

En cuanto a la gestión del sistema, se establecieron dos perfiles principales de administración: el Superadministrador, con acceso total a todas las funciones del sistema, y la Autoridad de Registro, cuya responsabilidad se limita al manejo del ciclo de vida de los certificados digitales. Ambos perfiles realizan su autenticación mediante certificados digitales propios, lo que garantiza un nivel adecuado de seguridad en la administración.

Adicionalmente, se definió un perfil de Estudiante, considerado de acceso público, que no requiere de certificados digitales para autenticarse en el sistema. Este rol está diseñado exclusivamente para permitir a los estudiantes llenar el formulario de

solicitud de certificado digital, consultar el estado de su trámite y, posteriormente, descargar su certificado una vez aprobado.

Finalmente, se configuraron los servicios CRL y OCSP bajo la Autoridad de Validación, los cuales son de carácter público y no requieren autenticación para su uso.

Funcionamiento del servicio de firma electrónica.

El proceso para la emisión de certificados digitales en la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte se desarrolla de la siguiente manera:

1. El estudiante accede al sistema, ingresa sus datos personales y registra una nueva solicitud de emisión de certificado digital.
2. El sistema confirma el registro de la solicitud y notifica al estudiante.
3. La autoridad de registro revisa la solicitud, valida la información proporcionada y aprueba el trámite si es correcto; en caso contrario lo rechaza.
4. El sistema informa al estudiante sobre la aprobación de su solicitud e indica que puede proceder con la descarga de su certificado digital.
5. Finalmente, el estudiante accede nuevamente al sistema y descarga su certificado digital para su uso en los procesos requeridos.

3.1.6.3 Descarga y personalización del software EJBCA community

1. Se ingresa al sitio web de EJBCA y hacemos clic en la opción de “Download”.

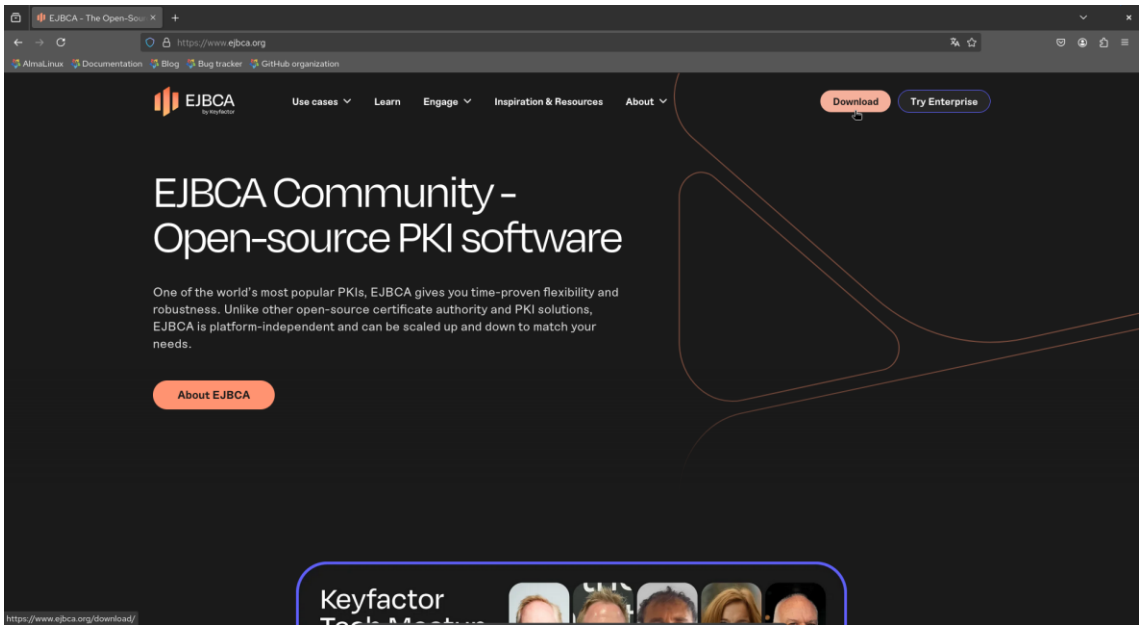


Figura: 10 Página oficial de EJBCA.

2. En la siguiente página, nos dirigimos al vínculo de “Download from SourceForge”.

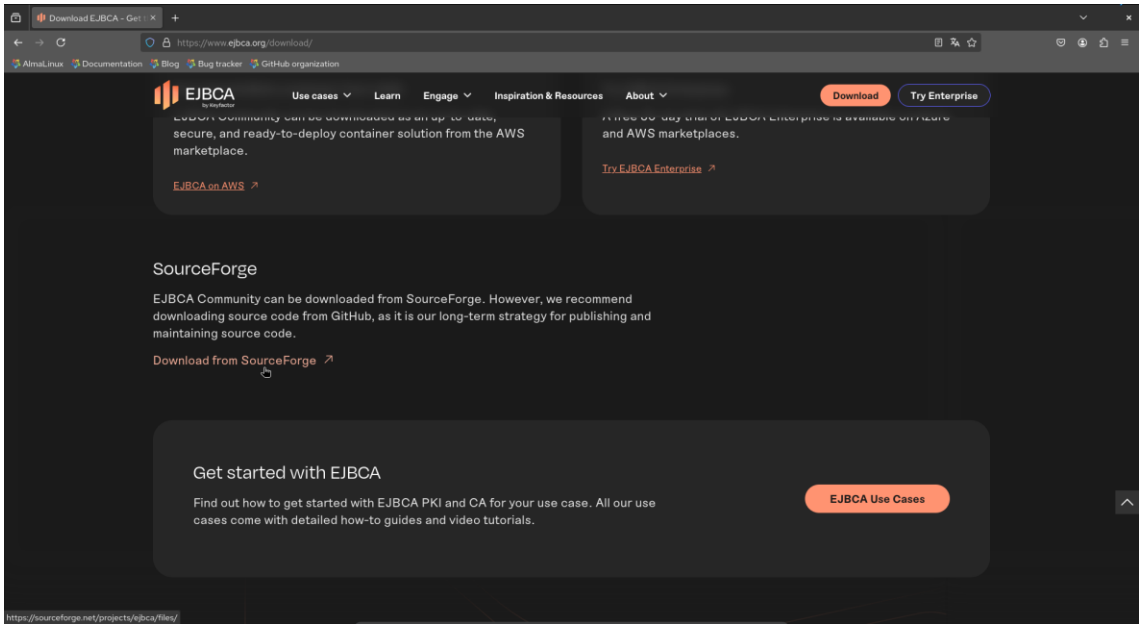


Figura: 11 Página de alternativas de descarga EJBCA.

3. En la siguiente página, escogemos la versión más reciente de EJBCA y la descarga empezará automáticamente.

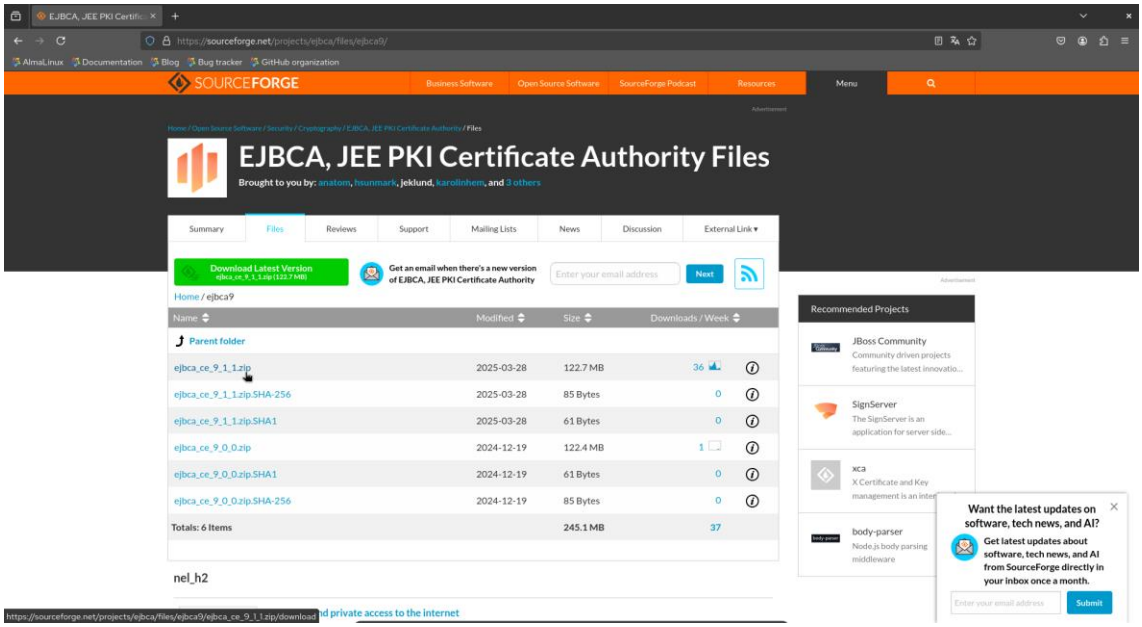


Figura: 12 Página de descarga de versiones de EJBCA.

4. Descomprimimos el archivo de EJBCA descargado.

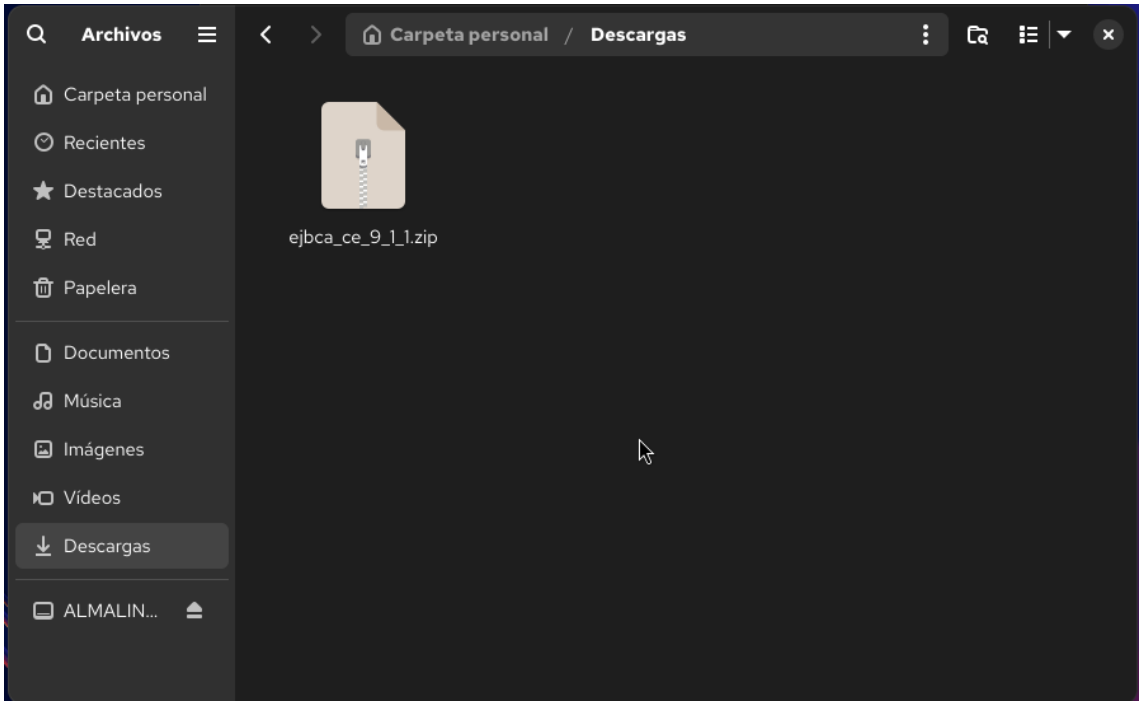


Figura: 13 Descompresión de código fuente de EJBCA.

5. Colocamos la carpeta de EJBCA en una dirección conveniente, para este caso en /opt.

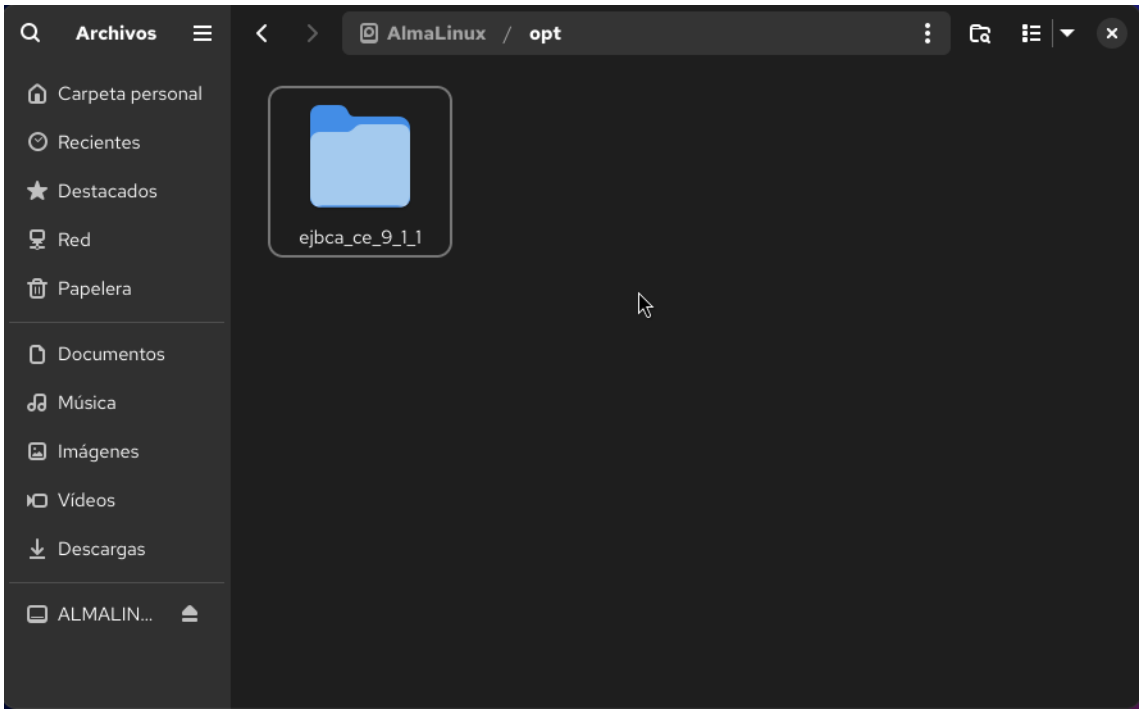


Figura: 14 Ubicación de código fuente de EJBCA.

6. Ingresamos en el directorio /conf de la carpeta de EJBCA.

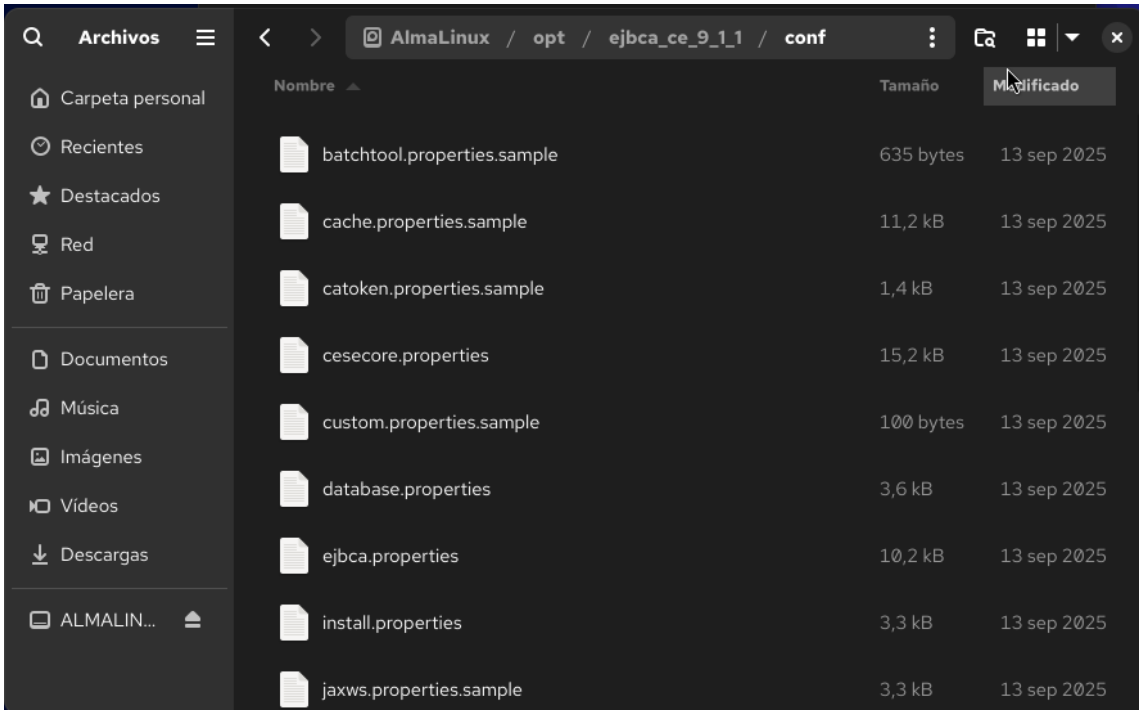


Figura: 15 Directorio /conf de EJBCA.

7. Buscamos el archivo install.properties.sample y lo renombramos a install.properties

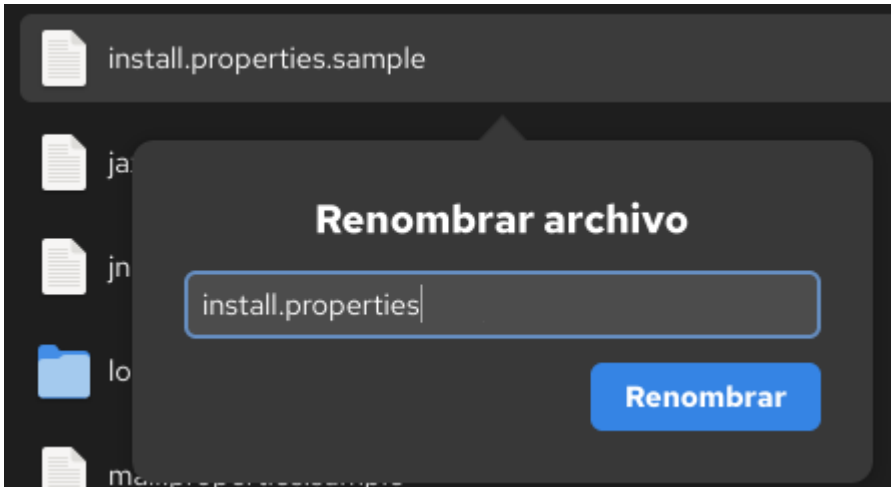


Figura: 16 Cambio de nombre al archivo install.

8. Abrimos con el bloc de notas el archivo renombrado anteriormente.

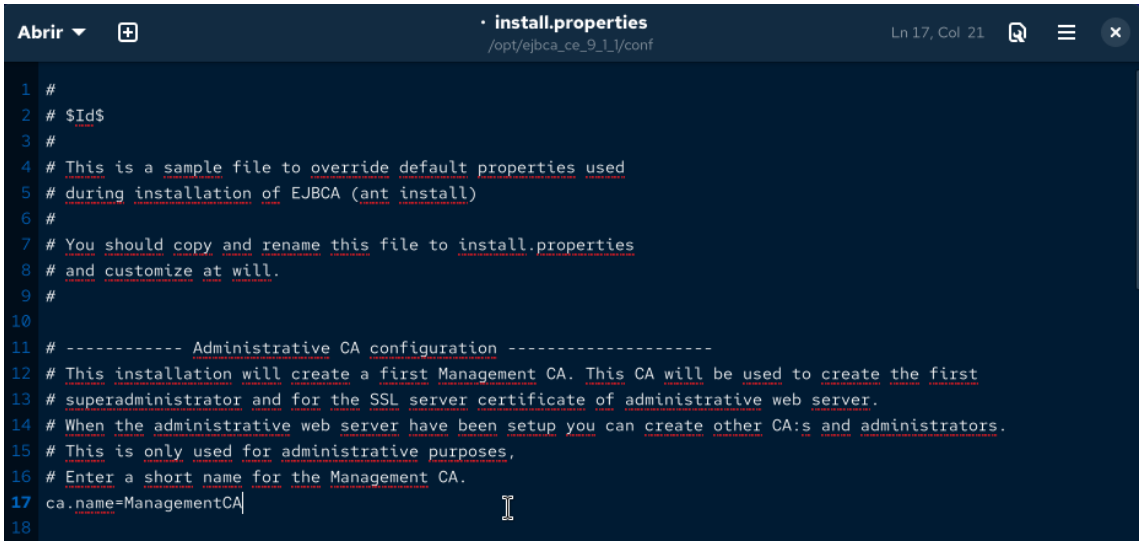


Figura: 17 Configuración de archivo install.properties.

8.1 Cambiamos el nombre de la CA de gestión.

Figura: 18 Cambio de nombre de la CA.

8.2 Cambiamos el nombre de distinción de la CA de gestión y guardamos los cambios.

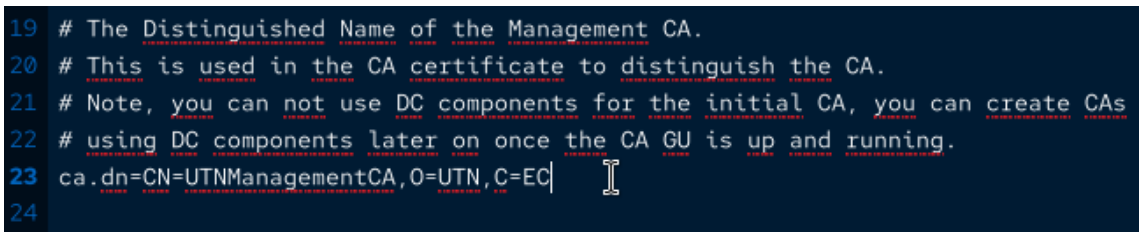


Figura: 19 Cambio de nombre de distinción de la CA.

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

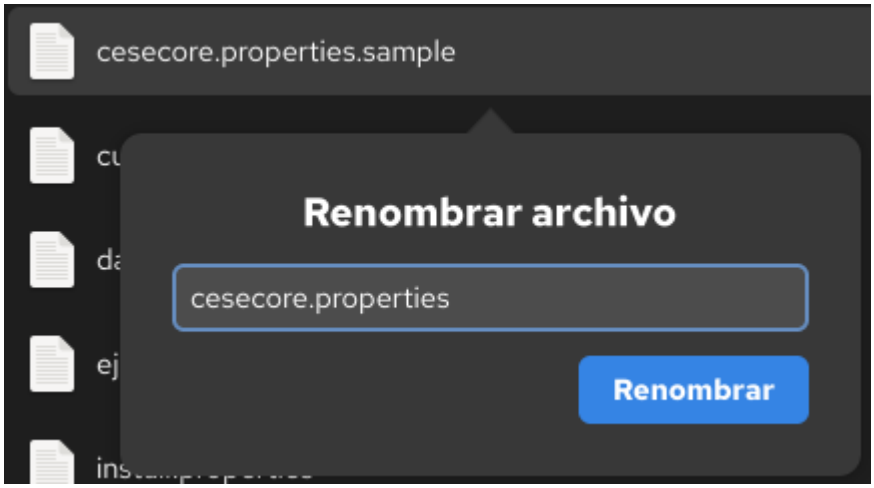


Figura: 20 Cambio de nombre al archivo cesecore.

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

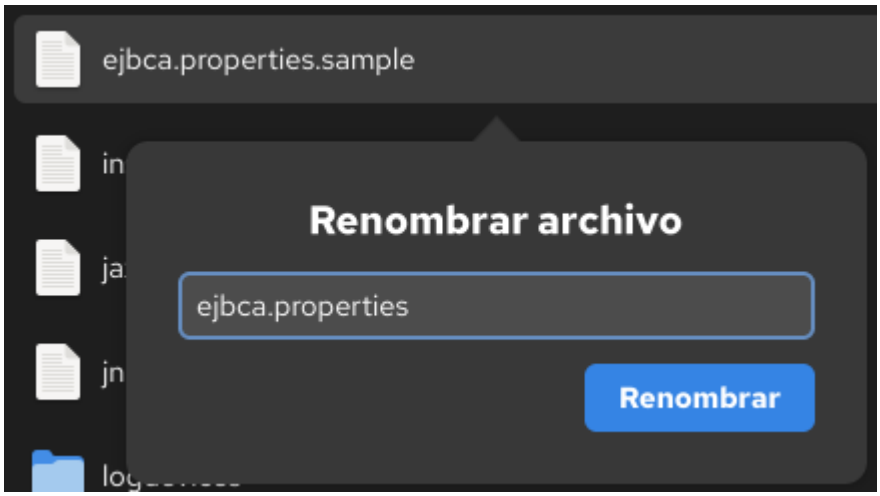


Figura: 21 Cambio de nombre al archivo ejbca.

11. Se renombra el archivo web.properties.sample a web.properties.

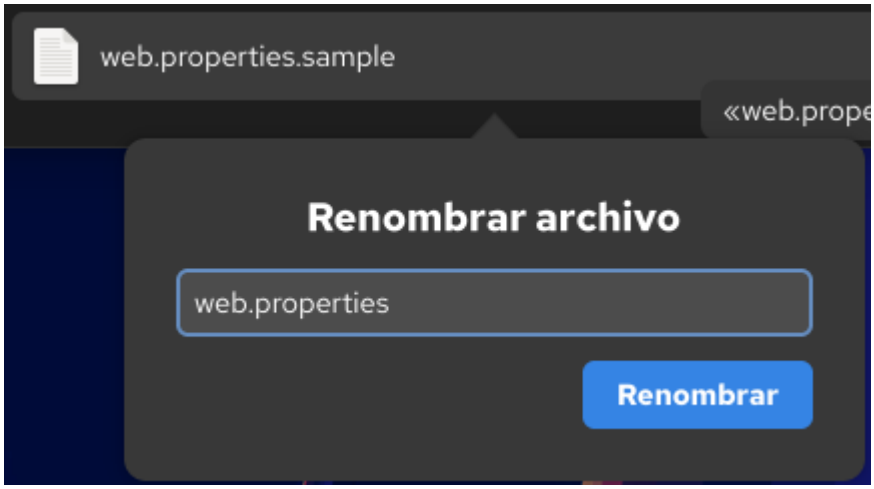


Figura: 22 Cambio de nombre al archivo web.

12. Abrimos con el bloc de notas el archivo renombrado en el paso anterior.

12.1 Se cambia la contraseña para el almacén de claves de confianza de Java.

```
# Password for java trust keystore (p12/truststore.jks). Default is changeit
# This truststore will contain the CA-certificate after running 'ant javatruststore'
# Run 'ant -Dca.name=FooCA javatruststore' to install the CA-certificate for FooCA instead of the default ManagementCA
# Note: avoid special characters that need escaping, such as $, in the password. These may not be properly handled by ant.
java.trustpassword=********************
```

Figura: 23 Cambio de contraseña para el almacén de claves de confianza de Java.

12.2 Se cambia el nombre del superadmin.

Figura: 24 Cambio de nombre del superadmin.

12.3 Se cambia el nombre de distinción del superadmin.

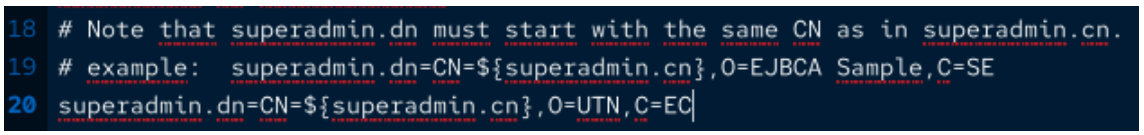


Figura: 25 Cambio de nombre de distinción del superadmin.

12.4 Se cambia la contraseña de superadmin.

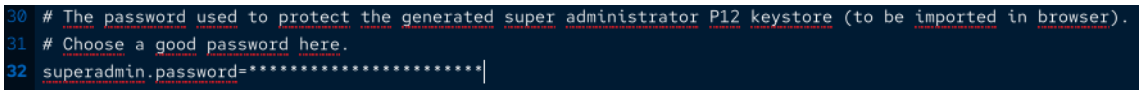


Figura: 26 Cambio de contraseña de superadmin.

12.5 Se cambia la contraseña para el almacén de claves del servidor de aplicaciones.

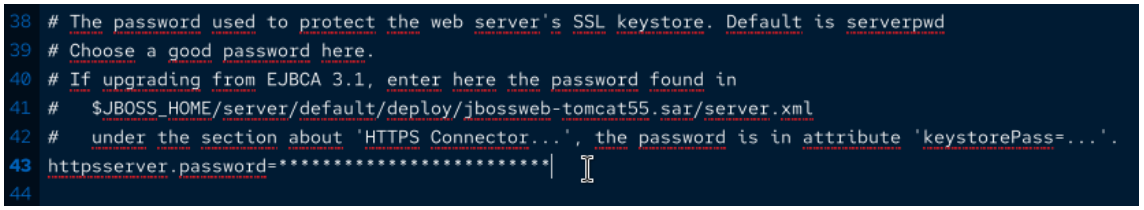


Figura: 27 Cambio de contraseña para el almacén de claves del servidor de aplicaciones.

12.6 Se cambia el nombre del host de esta instancia.

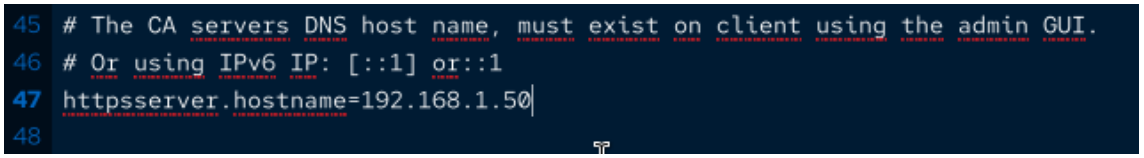


Figura: 28 Cambio de nombre del host.

12.7 Se cambia el nombre de distinción del sujeto del certificado TLS utilizado por la interfaz de usuario de EJBCA y guardamos los cambios.

Figura: 29 Cambio del nombre de distinción del sujeto del certificado TLS.

13. Se renombra el archivo database.properties.sample a database.properties.

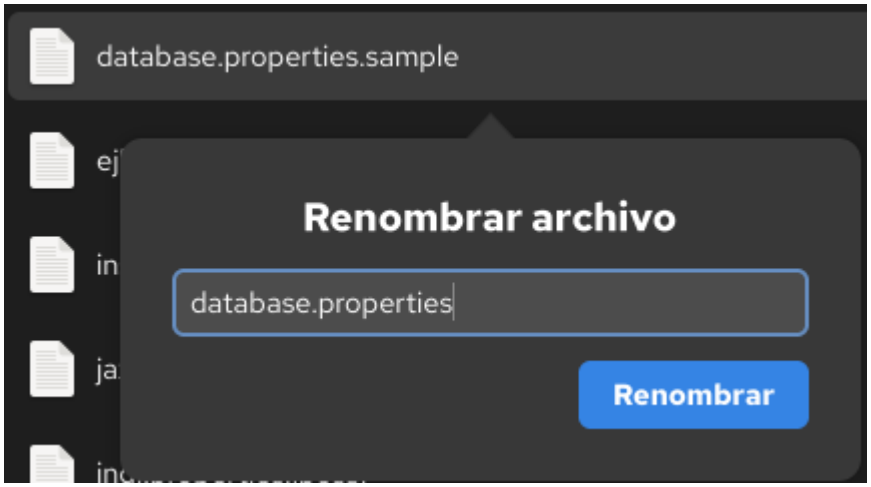


Figura: 30 Cambio del nombre al archivo database.

14. Abrimos con el bloc de notas el archivo renombrado anteriormente.

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

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

Figura: 31 Cambio de nombre de la fuente de datos.

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

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

Figura: 32 Cambio de nombre de la base de datos utilizada.

14.3 Se modifica la URL de la base de datos.

```
# Database connection URL.
# This is the URL used to connect to the database, used to configure a new datasource in JBoss.
# Default: jdbc:h2:~/ejbcadb;DB_CLOSE_DELAY=-1;NON_KEYWORDS=VALUE
database.url=jdbc:mariadb://127.0.0.1:3306/ejbca
#database.url=jdbc:mysql://127.0.0.1:3306/ejbca?characterEncoding=UTF-8
#database.url=jdbc:postgresql://127.0.0.1/ejbca
```

Figura: 33 Cambio de la URL de la base de datos.

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

```
62 # JDBC driver classname.
63 # The JEE server needs to be configured with the appropriate JDBC driver for the selected database
64 # The Default h2 works (as test database) on JBoss 7, on JBoss 5 use org.hsqldb.jdbcDriver
65 # Default: h2
66 database.driver=org.mariadb.jdbc.Driver
67 #database.driver=com.mysql.jdbc.Driver
68 #database.driver=org.postgresql.Driver
```

Figura: 34 Cambio de nombre del controlador de la base de datos.

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

```
78 # Database username.
79 # Default: sa (works with H2 on JBoss 7)
80 database.username=ejbca
81
```

Figura: 35 Cambio de nombre del usuario establecido para la base de datos.

14.6 Se cambia la contraseña del usuario establecido para la base de datos EJBCA y se guarda los cambios.

```
82 # Database password.
83 # Default: sa (works with H2 on JBoss 7)
84 database.password=********************
```

Figura: 36 Cambio de contraseña del usuario establecido para la base de datos.

15. Nos dirigimos nuevamente al navegador y buscamos “Visual Studio Code”.

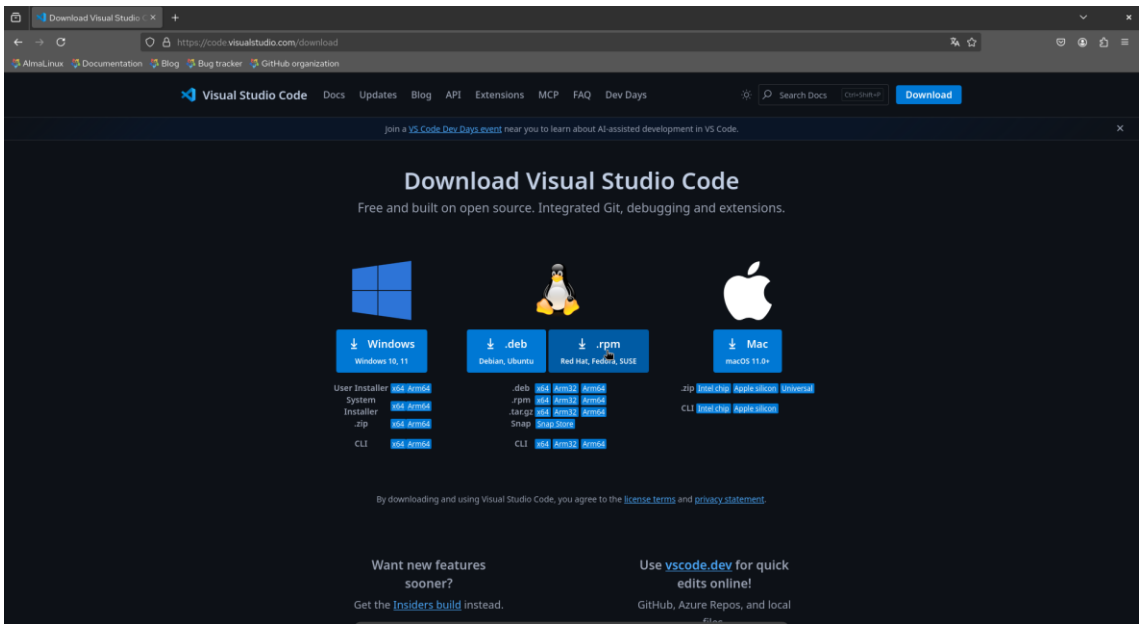


Figura: 37 Página de descarga de Visual Studio Code.

16. Una vez descargado el instalador de VS Code, hacemos doble clic e instalamos la aplicación.
17. Desde el explorador de archivos, nos dirigimos al directorio de la carpeta de ejbca, hacemos clic derecho y seleccionamos “Abrir en consola”.

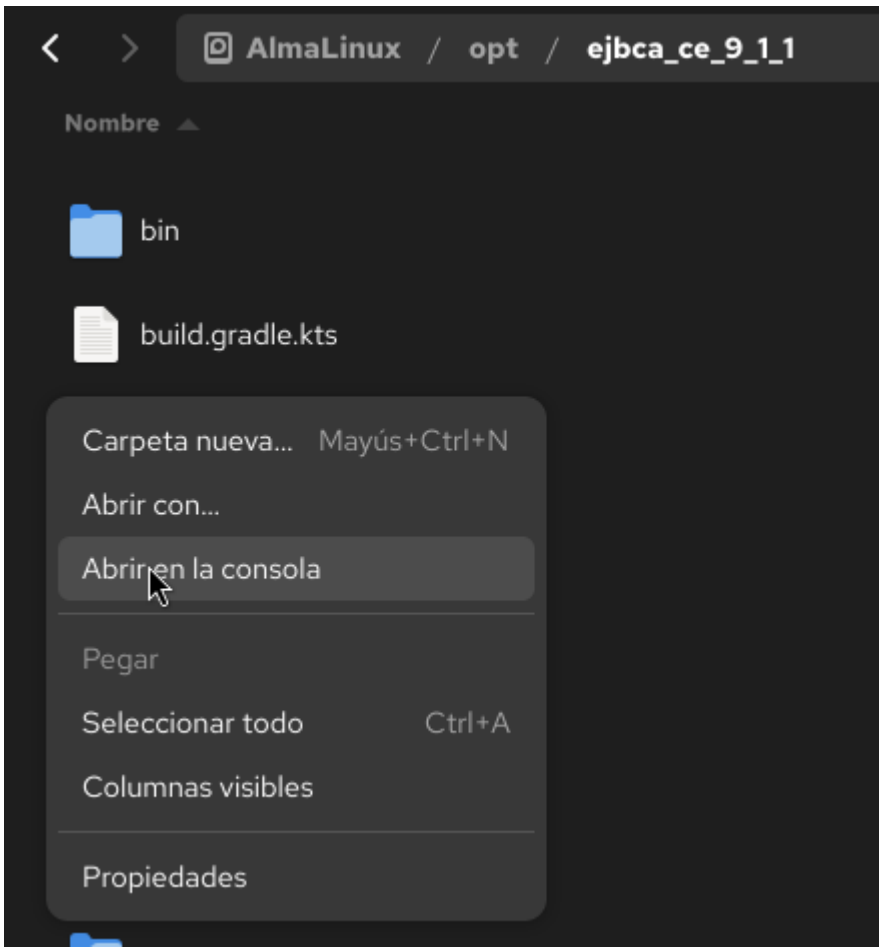


Figura: 38 Directorio de ejbca.

18. Se nos abre la terminal y escribimos el siguiente comando.

Figura: 39 Comando para abrir VS Code.

19. Se nos abrirá el IDE de VS Code y seleccionamos la opción de “Confiar en los autores”.

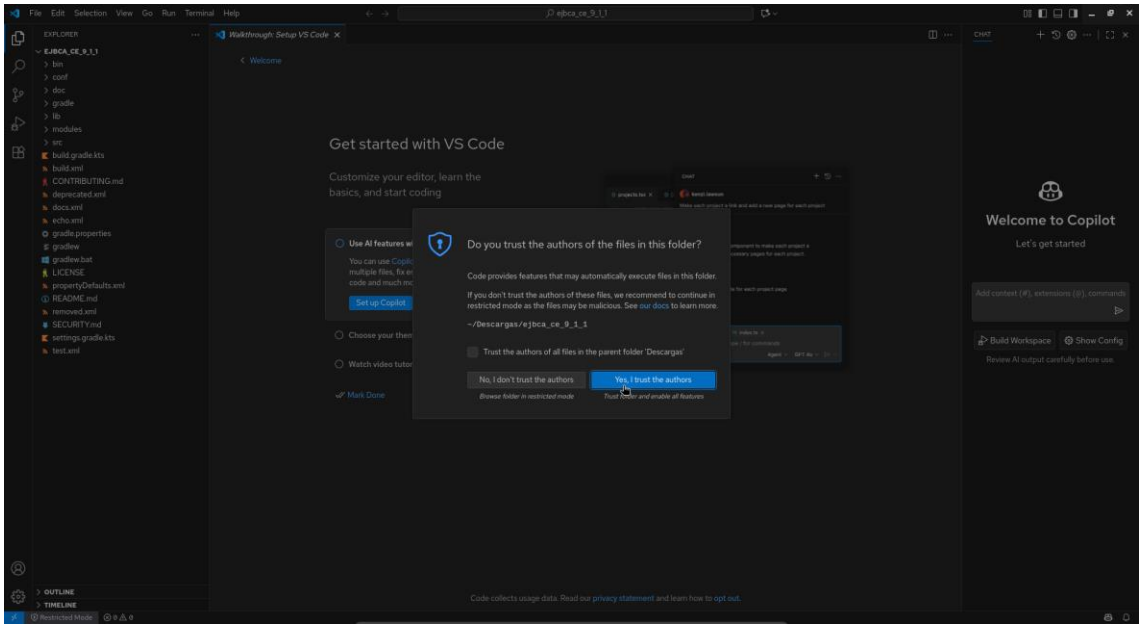


Figura: 40 Presentación de VS Code.

20. En esta área de trabajo, podremos ver en la parte izquierda de la aplicación un árbol jerárquico con todos los archivos correspondientes a EJBCA. Aquí podemos modificar todo el código fuente del sistema EJBCA según lo que necesitemos; las secciones de vistas, estilos y lógica del sistema se encuentran dentro de la carpeta modules.

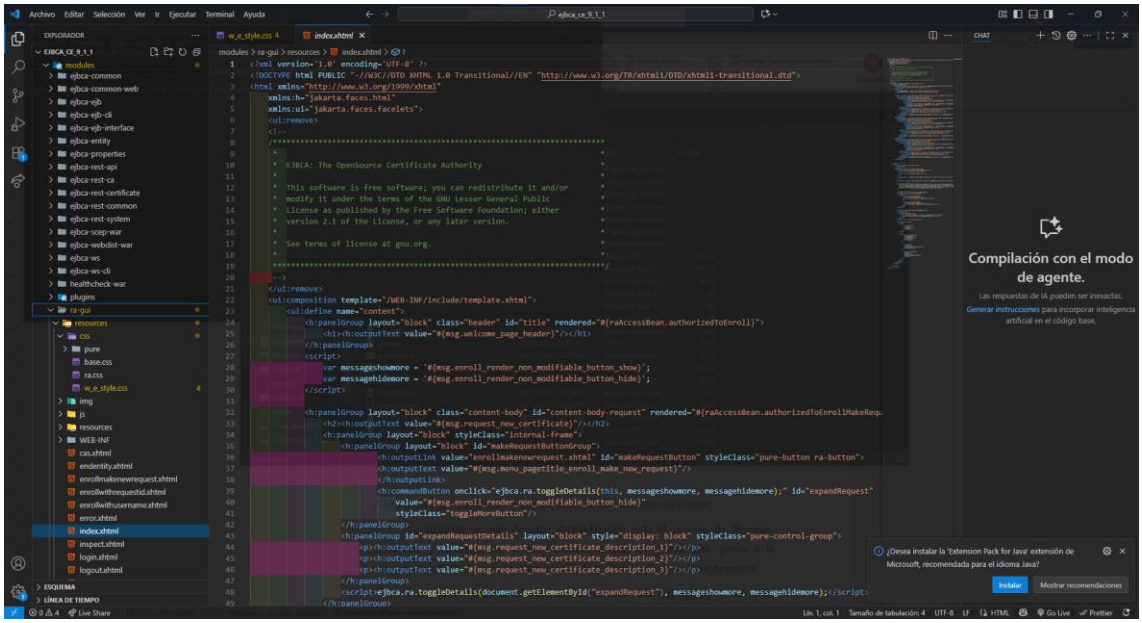


Figura: 41 Visual Studio Code.

3.1.6.4 Descarga, instalación y configuración de herramientas necesarias.

La siguiente sección describe detalladamente todo el proceso de descarga, instalación y configuración de las diferentes herramientas necesarias, previo a la instalación de EJBCA, que se realiza a través de la "Terminal" del sistema operativo.

Como primer paso, se debe ejecutar el comando **sudo dnf update -y**, con el fin de actualizar todos los paquetes del sistema operativo y asegurar que se encuentre con las versiones más recientes antes de proceder con la instalación de las herramientas necesarias.

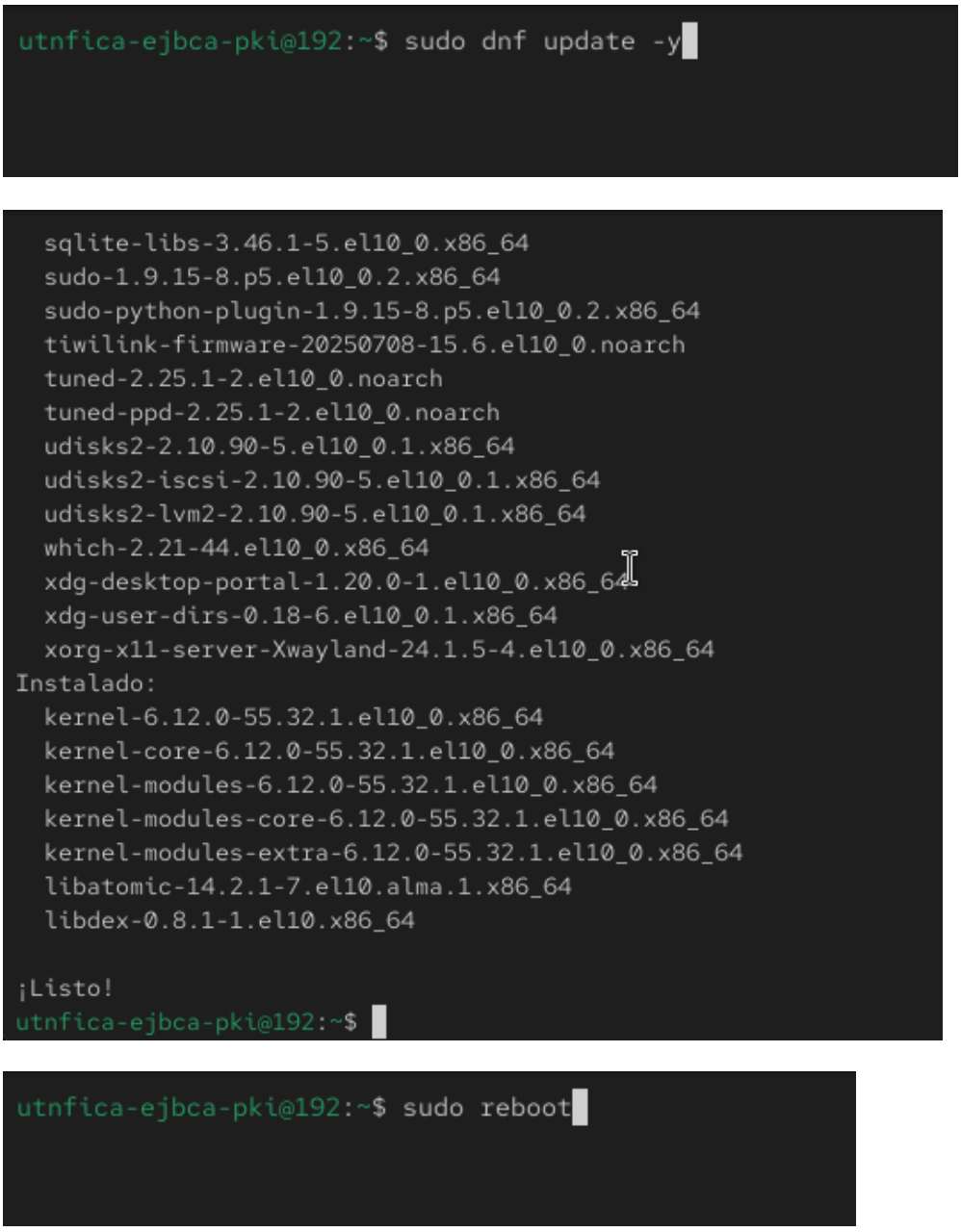


Figura: 42 Actualización de paquetes del sistema

1. Instalación Java JDK 21

1.1 Desde la terminal ejecutamos el comando para revisar la versión disponible de Java.

```
utnfica-ejbca-pki@192:~$ sudo dnf search openjdk
```

```
java-21-openjdk-javadoc.x86_64 : OpenJDK 21 API documentation
java-21-openjdk-javadoc-zip.x86_64 : OpenJDK 21 API documentation compressed in a single archive
java-21-openjdk-jmods.x86_64 : JMods for OpenJDK 21
java-21-openjdk-jmods-fastdebug.x86_64 : JMods for OpenJDK 21 optimised with full debugging on
java-21-openjdk-jmods-slowdebug.x86_64 : JMods for OpenJDK 21 unoptimised with full debugging on
java-21-openjdk-slowdebug.x86_64 : OpenJDK 21 Runtime Environment unoptimised with full debugging
                                 : on
java-21-openjdk-src.x86_64 : OpenJDK 21 Source Bundle
java-21-openjdk-src-fastdebug.x86_64 : OpenJDK 21 Source Bundle for packages with debugging on and
                                     : optimisation
java-21-openjdk-src-slowdebug.x86_64 : OpenJDK 21 Source Bundle for packages with debugging on and
                                     : no optimisation
java-21-openjdk-static-libs.x86_64 : OpenJDK 21 libraries for static linking
java-21-openjdk-static-libs-fastdebug.x86_64 : OpenJDK 21 libraries for static linking optimised
                                             : with full debugging on
java-21-openjdk-static-libs-slowdebug.x86_64 : OpenJDK 21 libraries for static linking unoptimised
                                             : with full debugging on
maven-openjdk21.noarch : maven binding for openjdk21
xmvn-toolchain-openjdk21.noarch : xmvn-minimal binding for openjdk21
================================ Coincidencia en Nombre: openjdk ================================
javapackages-local-openjdk21.noarch : Non-essential macros and scripts for Java packaging support
maven-local-openjdk21.noarch : Macros and scripts for Maven packaging support
utnfica-ejbca-pki@192:~$
```

Figura: 43 Versión de paquetes de Java disponibles.

1.2 Ejecutamos el comando para instalar Java 21 o la versión disponible.

```
utnfica-ejbca-pki@192:~$ sudo dnf install -y java-21-openjdk java-21-openjdk-devel
```

```
  Ejecutando scriptlet: xorg-x11-fonts-Type1-7.5-40.el10.noarch                                5/9
  Instalando          : javapackages-filesystem-6.4.0-1.el10.noarch                            6/9
  Instalando          : java-21-openjdk-headless-1:21.0.8.0.9-1.el10.alma.1.x86_64             7/9
  Ejecutando scriptlet: java-21-openjdk-headless-1:21.0.8.0.9-1.el10.alma.1.x86_64             7/9
  Instalando          : java-21-openjdk-1:21.0.8.0.9-1.el10.alma.1.x86_64                      8/9
  Ejecutando scriptlet: java-21-openjdk-1:21.0.8.0.9-1.el10.alma.1.x86_64                      8/9
  Instalando          : java-21-openjdk-devel-1:21.0.8.0.9-1.el10.alma.1.x86_64                9/9
  Ejecutando scriptlet: java-21-openjdk-devel-1:21.0.8.0.9-1.el10.alma.1.x86_64                9/9
  Ejecutando scriptlet: java-21-openjdk-1:21.0.8.0.9-1.el10.alma.1.x86_64                      9/9
  Ejecutando scriptlet: java-21-openjdk-devel-1:21.0.8.0.9-1.el10.alma.1.x86_64                9/9

Instalado:
  java-21-openjdk-1:21.0.8.0.9-1.el10.alma.1.x86_64
  java-21-openjdk-devel-1:21.0.8.0.9-1.el10.alma.1.x86_64
  java-21-openjdk-headless-1:21.0.8.0.9-1.el10.alma.1.x86_64
  javapackages-filesystem-6.4.0-1.el10.noarch
  lksctp-tools-1.0.21-1.el10.x86_64
  mkfontscale-1.2.2-8.el10.x86_64
  ttmkfdir-3.0.9-72.el10.x86_64
  tzdata-java-2025b-1.el10.noarch
  xorg-x11-fonts-Type1-7.5-40.el10.noarch

¡Listo!
utnfica-ejbca-pki@192:~$
```

Figura: 44 Instalación de paquetes Java 21.

1.3 Revisamos la instalación con los siguientes comandos.

```
utnfica-ejbca-pki@192:~$ sudo java -version
openjdk version "21.0.8" 2025-07-15 LTS
OpenJDK Runtime Environment (Red_Hat-21.0.8.0.9-1) (build 21.0.8+9-LTS)
OpenJDK 64-Bit Server VM (Red_Hat-21.0.8.0.9-1) (build 21.0.8+9-LTS, mixed mode, sharing)
```

```
utnfica-ejbca-pki@192:~$ sudo javac -version
javac 21.0.8
```

Figura: 45 Verificación de versiones de instaladas Java.

2. Instalación de Apache ANT

2.1 Ejecutamos el siguiente comando para la instalación de Apache ANT.

```
utnfica-ejbca-pki@192:~$ sudo dnf install -y ant
```

Figura: 46 Instalación de Apache ANT.

2.2 Revisamos la instalación con el siguiente comando.

```
utnfica-ejbca-pki@192:~$ sudo ant -version
Apache Ant(TM) version 1.10.15 compiled on December 17 2024
```

Figura: 47 Verificación de versión instalada Apache ANT.

3. Instalación y configuración de MariaDB

3.1 Se ejecuta el siguiente comando para la instalación de MariaDB.

```
utnfica-ejbca-pki@192:~$ sudo dnf install -y mariadb-server
```

Figura: 48 Instalación de MariaDB.

3.2 Se ejecuta el siguiente comando para iniciar el servicio de MariaDB.

```
utnfica-ejbca-pki@192:~$ sudo systemctl start mariadb
```

Figura: 49 Iniciar el servicio de MariaDB.

3.3 Se ejecuta el siguiente comando para realizar la configuración de seguridad de MariaDB.

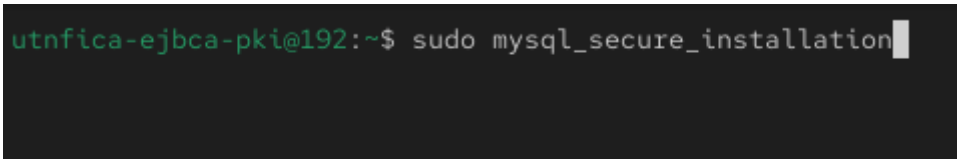


Figura: 50 Configuración de seguridad MariaDB.

3.3.1 En la siguiente configuración de contraseña para usuario root, presionamos la tecla enter ya que aún no hemos colocado una.

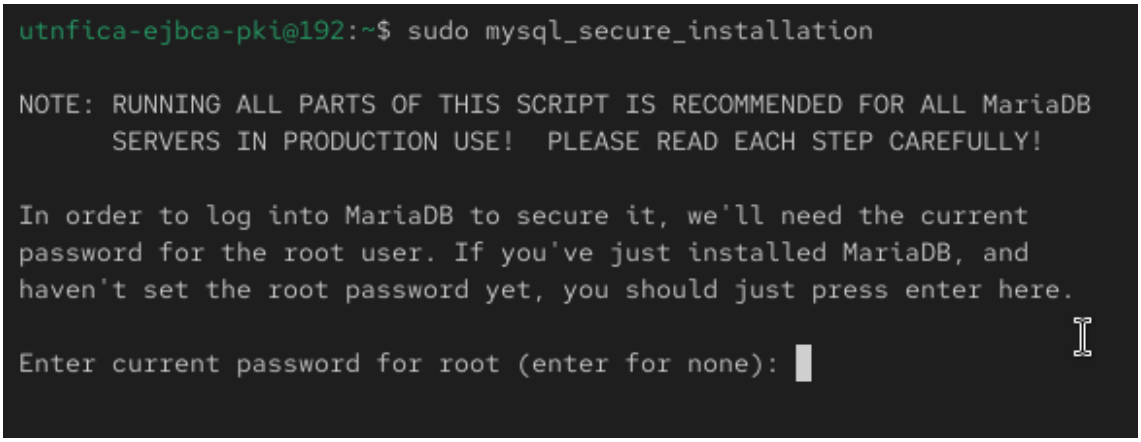


Figura: 51 Salto de contraseña root.

3.3.2 Colocamos la letra “n” en el switch to unix_socket authentication.

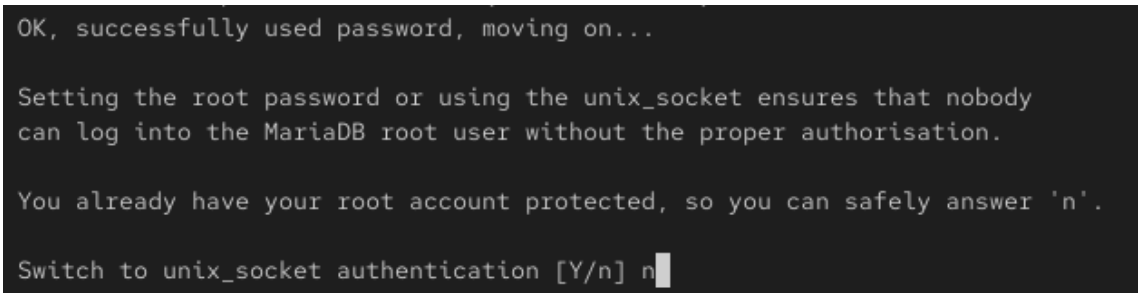


Figura: 52 Configuración de switch unix_socket.

3.3.3 Colocamos la letra “n” en el cambio de contraseña para el usuario root.

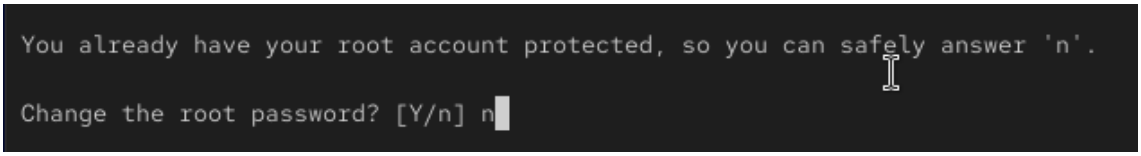


Figura: 53 Configuración de cambio de contraseña root.

3.3.4 Colocamos la letra “y” para remover los usuarios anónimos.

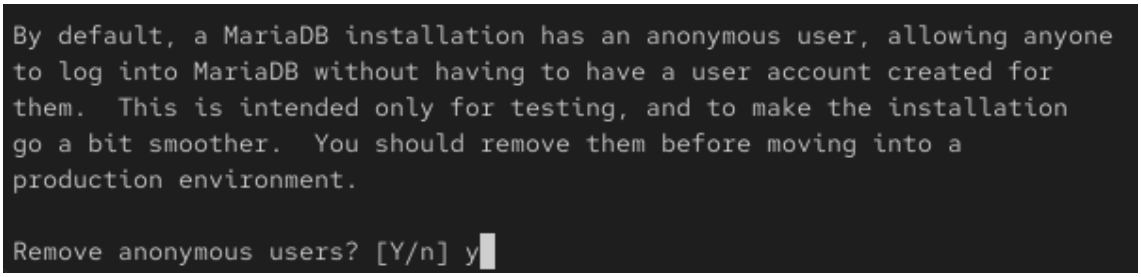


Figura: 54 Configuración de eliminación de usuarios anónimos.

3.3.5 Colocamos la letra "y" para deshabilitar el acceso remoto root.

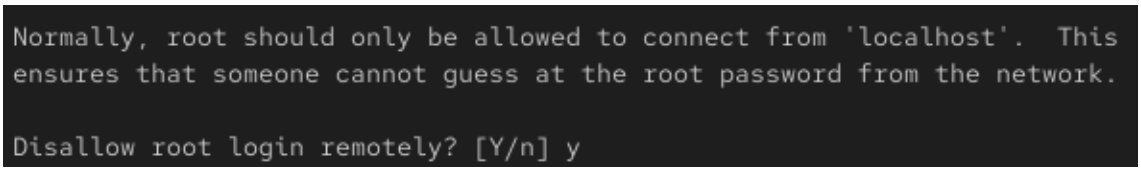


Figura: 55 Configuración de acceso root remoto MariaDB.

3.3.6 Colocamos la letra "y" para remover las bases de datos de pruebas que incluye la instalación de MariaDB.

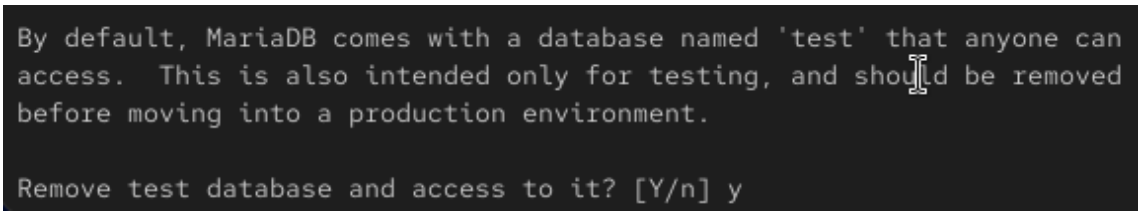


Figura: 56 Configuración de eliminación de bases de datos de prueba.

3.3.7 Colocamos la letra "y" para recargar los privilegios de las tablas.

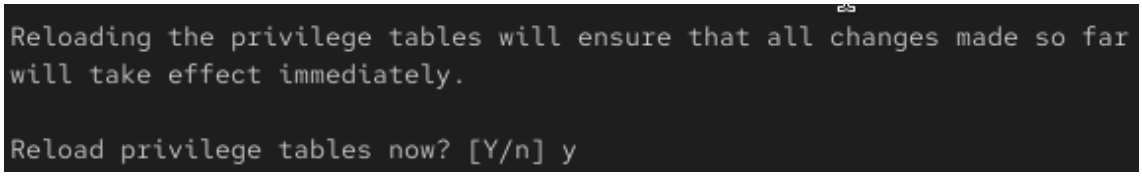


Figura: 57 Configuración de recarga de privilegios de las tablas.

3.4 Se ejecuta el siguiente comando para acceder a MariaDB como usuario root y presionamos enter ya que no hemos configurado ninguna contraseña para este usuario.

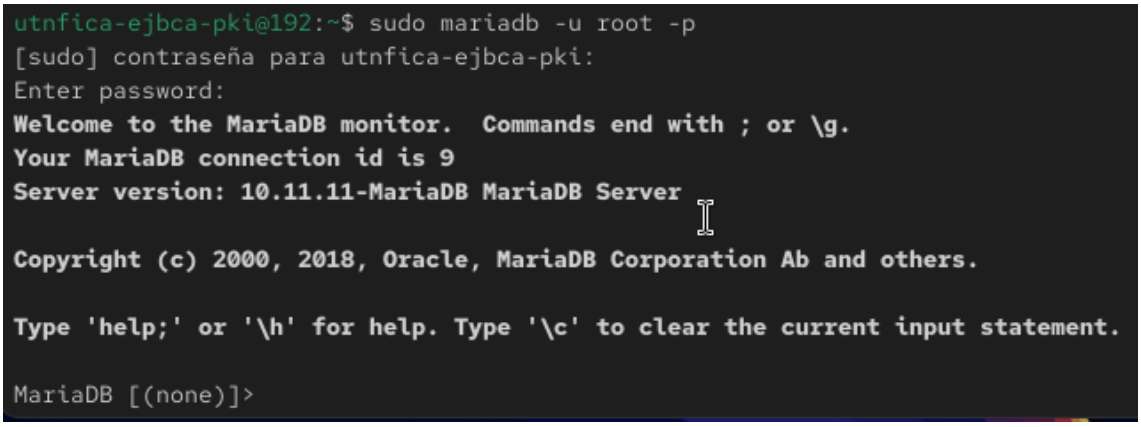


Figura: 58 Acceso a MariaDB como usuario root.

3.4.1 Una vez dentro de la consola de MariaDB, ingresamos el siguiente comando para colocar una contraseña segura al usuario root.

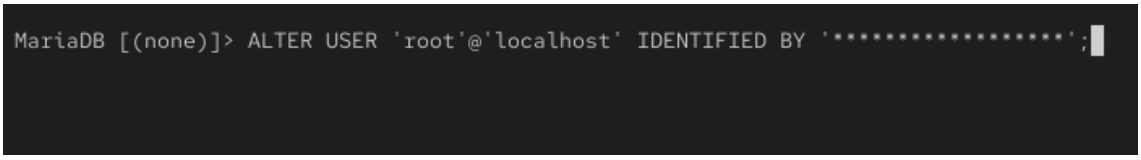


Figura: 59 Asignación de contraseña a usuario root.

3.4.2 Colocamos el siguiente comando para refrescar los privilegios.

Figura: 60 Refrescar privilegios.

3.4.3 Colocamos el siguiente comando para crear el usuario ejbca con su respectiva contraseña segura.

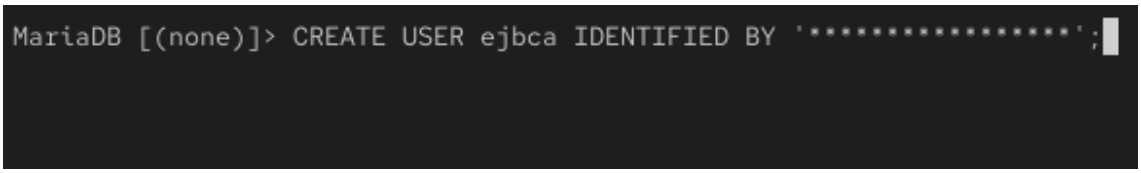


Figura: 61 Creación de usuario ejbca.

3.4.4 Colocamos el siguiente comando para crear la base de datos ejbca.

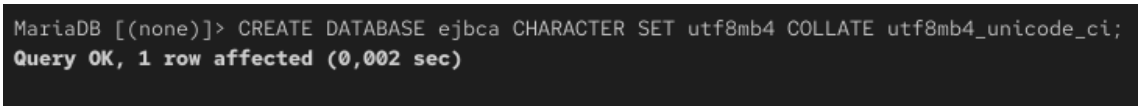


Figura: 62 Creación de base de datos ejbca.

3.4.5 Colocamos el siguiente comando para otorgarle todos los privilegios al usuario ejbca sobre la base de datos ejbca.

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON ejbca.* TO ejbca;
Query OK, 0 rows affected (0,006 sec)
```

Figura: 63 Otorgar privilegios al usuario ejbca.

3.4.6 Colocamos el siguiente comando para refrescar los privilegios.

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)
```

Figura: 64 Refrescar privilegios.

3.4.7 Colocamos el siguiente comando para ubicarnos y usar la base de datos ejbca.

```
MariaDB [(none)]> USE ejbca;
Database changed
MariaDB [ejbca]>
```

Figura: 65 Uso de base de datos ejbca.

4. Instalación y configuración del servidor de aplicaciones Wildfly32

4.1 Se ejecuta el siguiente comando para descargar Wildfly32.

```
utnfica-ejbca-pki@192:~$ wget https://github.com/wildfly/wildfly/releases/download/32.0.0.Final/wil
dfly-32.0.0.Final.zip -O /tmp/wildfly-32.0.0.Final.zip
```

Figura: 66 Descarga de Wildfly32.

4.2 Se ejecuta el siguiente comando para descomprimir en una carpeta a escoger, en este caso la carpeta /opt.

```
utnfica-ejbca-pki@192:~$ unzip -q /tmp/wildfly-32.0.0.Final.zip -d /
opt/
```

Figura: 67 Extracción de Wildfly32.

4.3 Se crea enlaces entre ficheros.

```
utnfica-ejbca-pki@192:~$ ln -snf /opt/wildfly-32.0.0.Final /opt/wildfly
```

Figura: 68 Creación de enlaces entre ficheros Wildfly32.

4.4 Se elimina RESTEasy-Crypto.

El servidor de aplicaciones a veces puede cargar su propia versión de Bouncy Castle, lo que genera problemas de incompatibilidad y/o conflicto, para el cual ejecutamos los siguientes comandos para eliminar RESTEasy-Crypto.

```
utnfica-ejbca-pki@192:~$ sed -i 's|.*org.jboss.resteasy.resteasy-crypto.*||' /opt/wildfly/module
s/system/layers/base/org/jboss/as/jaxrs/main/module.xml
```

```
utnfica-ejbca-pki@192:~$ rm -rf /opt/wildfly/modules/system/layers/base/org/jboss/resteasy/reste
asy-crypto
```

Figura: 69 Eliminación de RESTEasy-Crypto.

4.5 Se crea una configuración personalizada de Wildfly.

4.5.1 Ingresamos al directorio /bin de la carpeta donde ubicamos el servidor de aplicaciones Wildfly32.

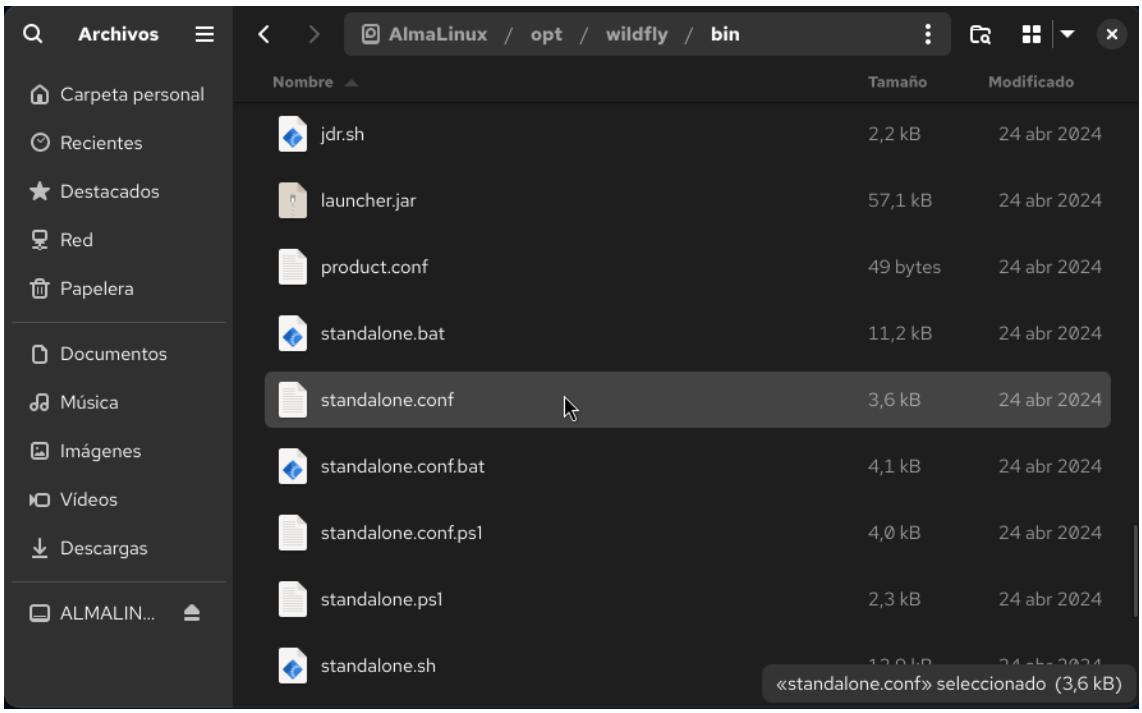


Figura: 70 Directorio /bin de Wildfly32.

4.5.2 Buscamos y abrimos el archivo standalone.conf y se borra su contenido.

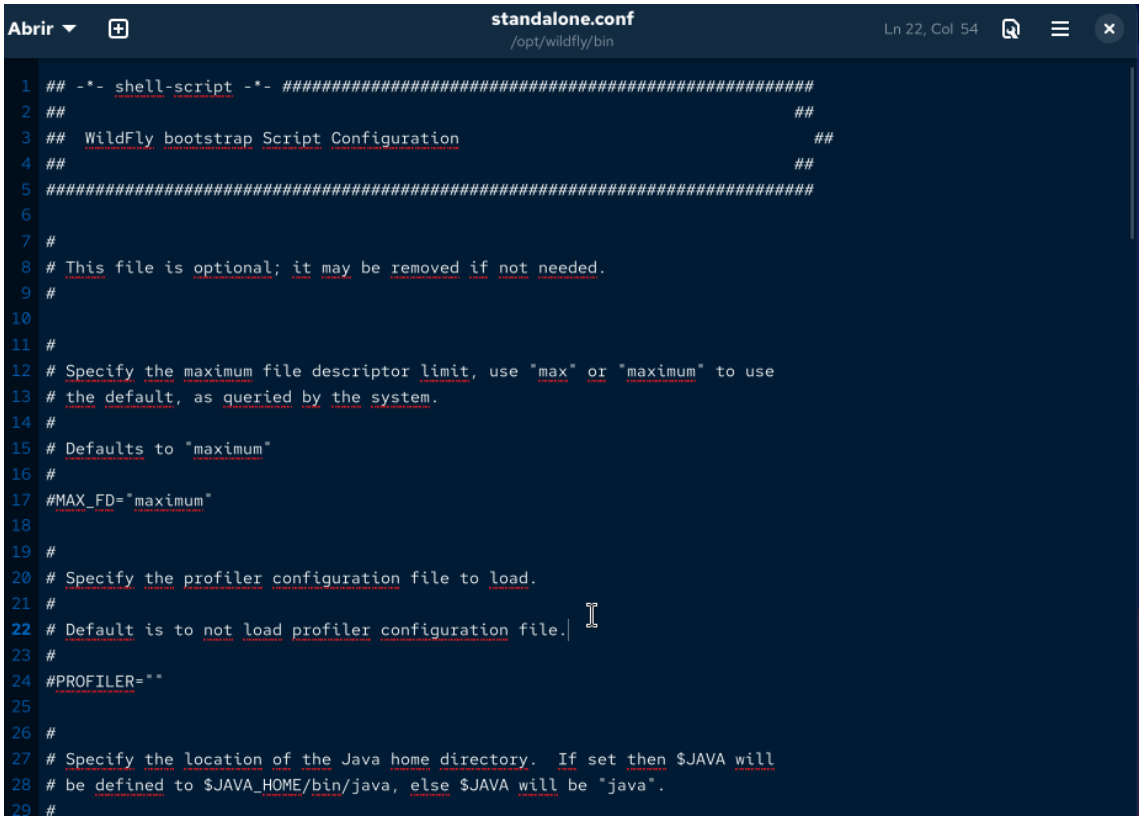


Figura: 71 Archivo standalone.conf

4.5.3 Se escribe el contenido que se necesita para ejecutar EJBCA.

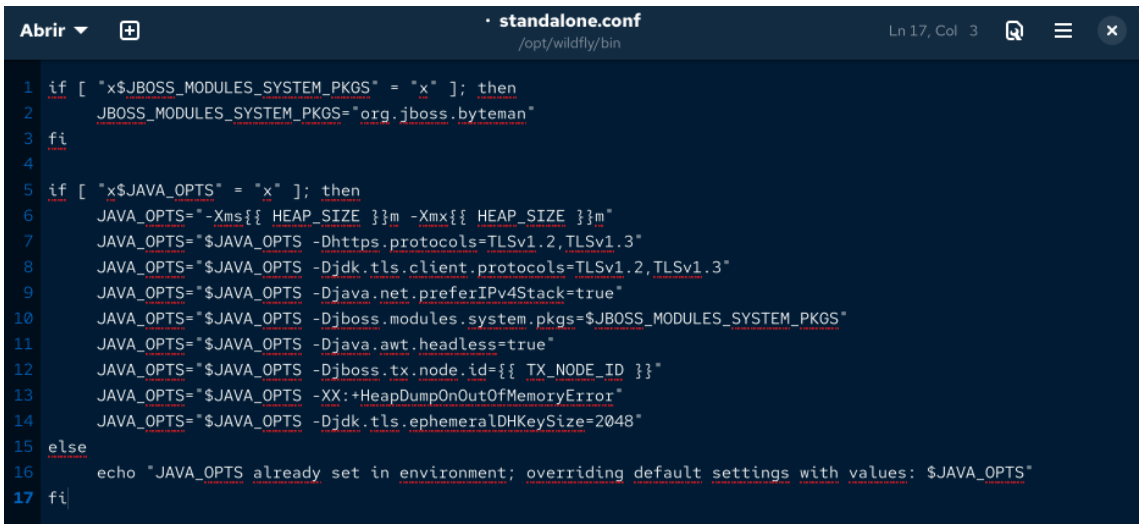


Figura: 72 Configuración de archivo standalone.conf

4.6 Establecer el uso de memoria permitido.

De forma predeterminada, el servidor de aplicaciones permite utilizar 512 MB de montón (RAM). Esto no es suficiente para ejecutar EJBCA. Recomendamos asignar al menos 2048 MB de RAM. Para aumentar el valor predeterminado, ejecute el siguiente comando:

```
utnfica-ejbca-pki@192:~$ sed -i -e 's/{{ HEAP_SIZE }}/2048/g' /opt/wildfly/bin/standalone.conf
```

Figura: 73 Asignación de uso de memoria permitido por Wildfly.

4.7 Establecer el ID del nodo de transacción.

Establezca el ID del nodo de transacción en un número único. El ID del nodo es utilizado por el transactions subsystems y garantiza que el administrador de transacciones solo recupere sucursales que coincidan con el identificador especificado. Es imperativo que este identificador sea único entre las instancias de WildFly que comparten un almacén de objetos o acceden a administradores de recursos comunes (es decir, cuando EJBCA opera en un clúster).

```
utnfica-ejbca-pki@192:~$ sed -i -e "s/{{ TX_NODE_ID }}/$(od -A n -t d -N 1 /dev/urandom | tr -d
' ')/g" /opt/wildfly/bin/standalone.conf
```

Figura: 74 Asignación de nodo de transacción para Wildfly.

4.8 Configurar Wildfly como servicio.

Los sistemas Linux modernos utilizan systemd para iniciar y detener servicios. El paquete zip WildFly ya contiene los archivos necesarios para ejecutarse como servicio, pero deben instalarse manualmente. Una vez iniciado como servicio, WildFly funcionará como wildfly usuario, y necesitamos agregar este usuario también.

```
utnfica-ejbca-pki@192:~$ cp /opt/wildfly/docs/contrib/scripts/systemd/launch.sh /opt/wildfly/bin

sudo cp /opt/wildfly/docs/contrib/scripts/systemd/wildfly.service /etc/systemd/system
sudo mkdir /etc/wildfly
sudo cp /opt/wildfly/docs/contrib/scripts/systemd/wildfly.conf /etc/wildfly
sudo systemctl daemon-reload
sudo useradd -r -s /bin/false wildfly
sudo chown -R wildfly:wildfly /opt/wildfly-32.0.0.Final/
```

Figura: 75 Configuración de Wildfly como servicio.

4.9 Se ejecuta el siguiente comando para iniciar el servicio de Wildfly.

```
utnfica-ejbca-pki@192:~$ sudo systemctl start wildfly
utnfica-ejbca-pki@192:~$
```

Figura: 76 Iniciar Wildfly como servicio.

4.10 Se ejecuta el siguiente comando para comprobar si está activo el servicio de Wildfly.

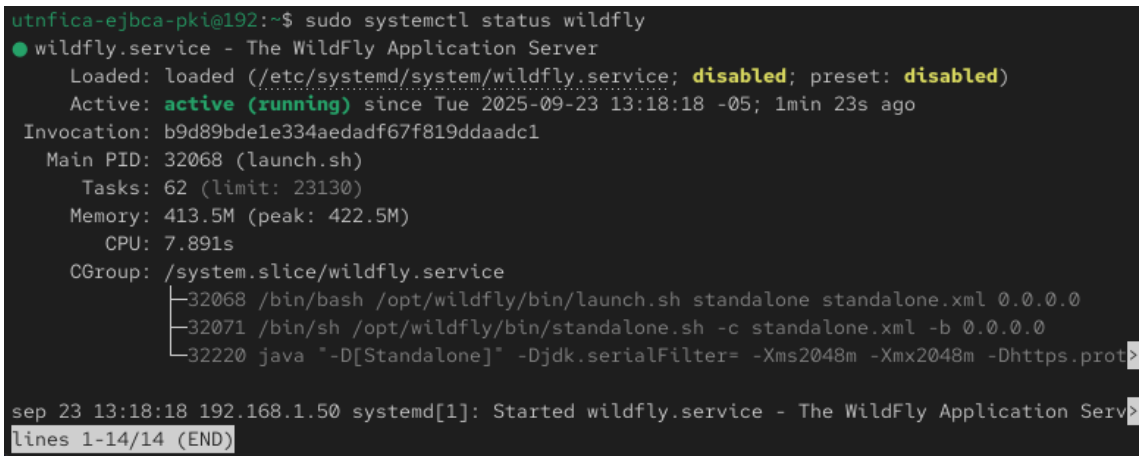


Figura: 77 Comprobación de estado del servicio de Wildfly.

4.11 Crear una tienda de credenciales de Elytron.

Se debe proteger las contraseñas almacenándolas en un almacén de credenciales. La credencial está cifrada con una contraseña maestra que WildFly obtiene al iniciarse.

4.11.1 Crea una contraseña maestra.

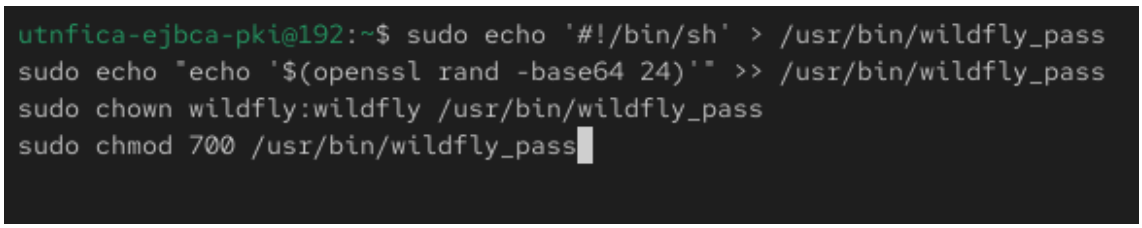


Figura: 78 Creación de una contraseña maestra.

4.11.2 Crear el almacén de credenciales

Figura: 79 Creación de almacén de credenciales.

4.12 Agregar controlador de base de datos

4.12.1 Desde el navegador, nos dirigimos al siguiente enlace, para que inicie la descarga del controlador.

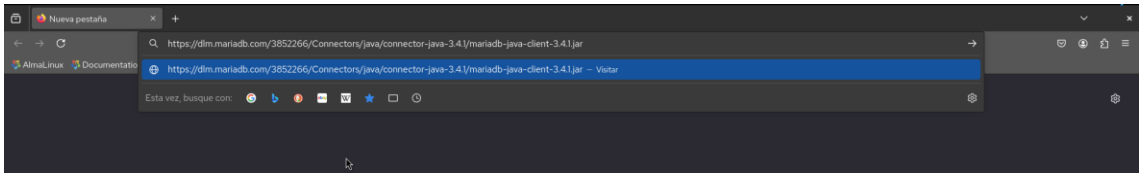


Figura: 80 Enlace de descarga para controlador de base de datos MariaDB.

4.12.2 Una vez descargado el controlador, lo renombramos de la siguiente manera.

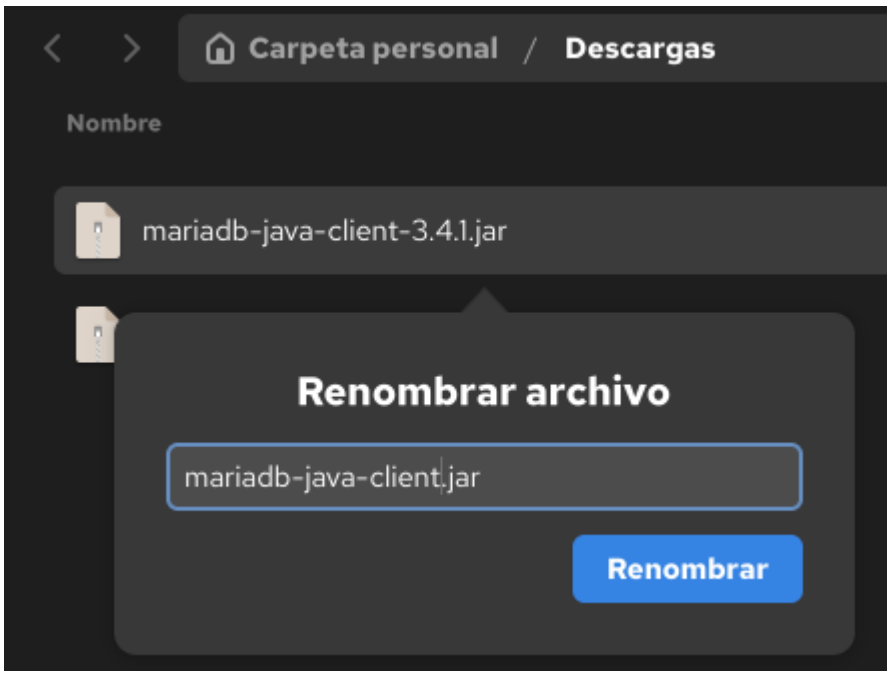


Figura: 81 Cambio de nombre del controlador de base de datos.

4.12.3 Desde la terminal, ejecutamos el siguiente código, para mover el controlador a la carpeta de Wildfly.

```
root@192:/home/utnfica-ejbca-pki# sudo mv /home/utnfica-ejbca-pki/Descargas/mariadb-java-client.
jar /opt/wildfly/standalone/deployments/
```

Figura: 82 Reubicación del controlador de base de datos.

4.13 Agregar fuente de datos.

Se ejecuta los comandos para las siguientes acciones.

- Agregar 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.

- Crear la fuente de datos al servidor de aplicaciones para lo cual se coloca la URL de la base de datos, el controlador de base de datos, el nombre usuario establecido en la base de datos y la referencia a la credencial del paso *4.11.2*.
- Recarga el servicio.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/credential-store=defaultCS:add-alias(alias=dbPassword, secret-value="******************")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect 'data-source add --name=utnejbcads --connection-url="jdbc:mariadb://127.0.0.1:3306/ejbca" --jndi-name="java:/UtnEjbcaDS" --use-ccm=true --driver-name="mariadb-java-client.jar" --driver-class="org.mariadb.jdbc.Driver" --user-name="ejbca" --credential-reference={store=defaultCS, alias=dbPassword} --validate-on-match=true --background-validation=false --prepared-statements-cache-size=50 --share-prepared-statements=true --min-pool-size=5 --max-pool-size=150 --pool-prefill=true --transaction-isolation=TRANSACTION_READ_COMMITTED --check-valid-connection-sql="select 1;"'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'
```

Figura: 83 Agregación de fuente de datos en Wildfly.

4.14 Configurar WildFly remotamente.

EJBCA necesita utilizar JBoss Remoting para que la CLI de EJBCA funcione. Configúrelo para usar un puerto separado 4447 y elimine cualquier otra dependencia del control remoto excepto lo que EJBCA necesita.

```
root@192:/home/utnfica-ejbca-pki — sudo su
file://192.168.1.50/home/utnfica-ejbca-pki

root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=remoting/http-connector=http-remoting-connector:write-attribute(name=connector-ref,value=remoting)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/socket-binding-group=standard-sockets/socket-binding=remoting:add(port=4447,interface=management)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server/http-listener=remoting:add(socket-binding=remoting,enable-http2=true)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
{
    "outcome" => "success",
    "response-headers" => {"process-state" => "reload-required"}
}
{
    "outcome" => "success",
    "response-headers" => {"process-state" => "reload-required"}
```

Figura: 84 Configurar WildFly remotamente.

4.15 Configurar registro de Wildfly.

4.15.1 Ejecutamos los siguientes comandos para configurar que WildFly registre mensajes de auditoría, advertencias y errores.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=loggi
ng/logger=org.ejbca:add(level=INFO)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.cesecore:add(level=I
NFO)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=com.keyfactor:add(level=
INFO)'
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 85 Configuración de registro de mensajes.

4.15.2 Ejecutamos los siguientes comandos para la configuración de logs adicional.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.jboss.as.config:write-attribute(name=level, value=WARN)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.jboss:add(level=WARN)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.wildfly:add(level=WARN)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.xnio:add(level=WARN)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.hibernate:add(level=WARN)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.apache.cxf:add(level=WARN)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=org.cesecore.config.ConfigurationHolder:add(level=WARN)'
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 86 Configuración de registro de mensajes adicional.

4.15.3 Ejecutamos los siguientes comandos para agregar registros de acceso.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-serve
r/host=default-host/setting=access-log:add(pattern="%h %t \"%r\" %s \"%{i,User-Agent}\"", relative-to=jboss.server.log.d
ir, directory=access-logs)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/logger=io.undertow.accesslog:add(level=INFO)'
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 87 Configuración de registros de acceso.

4.15.4 Ejecutamos los siguientes comandos para retirar el controlador de la consola.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/root-logger=ROOT:remo
ve-handler(name=CONSOLE)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=logging/console-handler=CONSOLE:remove()'
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 88 Eliminación del controlador de la consola.

4.15.5 Eliminar archivos de log pasado los 7 días.

- Se crea un archivo llamado “remove-old-wildfly-logs.sh” en el directorio etc/cron.daily.

```
root@192:/home/utnfica-ejbca-pki# sudo nano /etc/cron.daily/remove-old-wildfly-logs.sh
```

Figura: 89 Creación del archivo remove-old-wildfly-logs.sh

- Se coloca el script para la ejecución

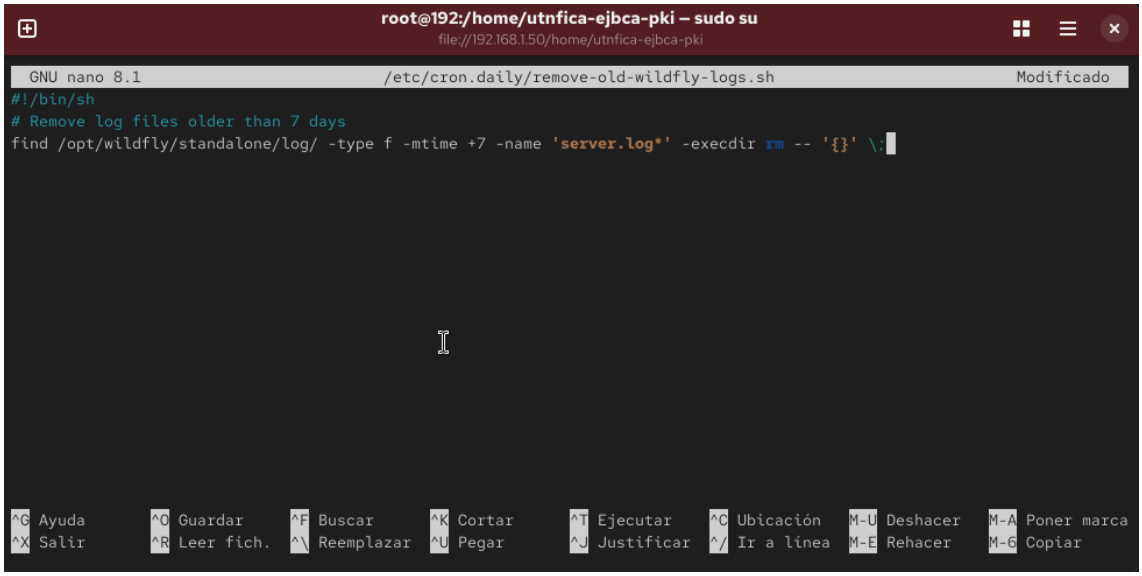


Figura: 90 Contenido del archivo remove-old-wildfly-logs.sh

- Se ejecuta el comando para hacer el archivo ejecutable.

```
root@192:/home/utnfica-ejbca-pki# sudo chmod +x /etc/cron.daily/remove-old-wildfly-logs.sh
```

Figura: 91 Permisos de ejecución sobre el archivo remove-old-wildfly-logs.sh

4.16 Configuración HTTP(S) con separación de 2 puertos.

4.16.1 Se ejecuta el comando para eliminar la configuración TLS y HTTP existente.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server
r/http-listener=default:remove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/socket-binding-group=standard-sockets/socket-binding=http:remove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server/https-listener=https:remove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/socket-binding-group=standard-sockets/socket-binding=https:remove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':read-attribute(name=server-state)'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
```

Figura: 92 Eliminación de configuración TLS y HTTP existente.

4.16.2 Se ejecutan los siguientes comandos para agregar nuevas interfaces y sockets.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/interface=http:add(inet-address="0.0.0.
0")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/interface=https:add(inet-address="0.0.0.0")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/socket-binding-group=standard-sockets/socket-binding=http:add(port="8080"
,interface="http")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/socket-binding-group=standard-sockets/socket-binding=https:add(port="8443
",interface="https")'
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 93 Agregación de nuevas interfaces y sockets.

4.16.3 Se ejecutan los siguientes comandos para configurar TLS, para lo cual es necesario colocar la contraseña del almacén de claves para keystore.jks, la contraseña del almacén de confianza para truststore.jks que definimos anteriormente en el archivo web.properties de la carpeta donde se encuentra EJBCA y el nombre de la tienda de credenciales definida anteriormente.

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/credential-store=defaultCS:add-alias(alias=httpsKeystorePassword, secret-value="******
**********")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/credential-store=defaultCS:add-alias(alias=httpsTruststorePassword, secret-value="******************")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/key-store=httpsKS:add(path="keystore/keystore.p12",relative-to=jboss.server.config.dir,credential-reference={store=defa
ultCS, alias=httpsKeystorePassword},type=PKCS12)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/key-store=httpsTS:add(path="keystore/truststore.p12",relative-to=jboss.server.config.dir,credential-reference={store=de
faultCS, alias=httpsTruststorePassword},type=PKCS12)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/key-manager=httpsKM:add(key-store=httpsKS,algorithm="SunX509",credential-reference={store=defaultCS, alias=httpsKeystor
ePassword})'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/trust-manager=httpsTM:add(key-store=httpsTS)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/server-ssl-context=https:add(key-manager=httpsKM,protocols=["TLSv1.3","TLSv1.2"],use-cipher-suites-order=false,cipher-s
uite-filter="TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_ECD
SA_WITH_CHACHA20_POLY1305_SHA256",cipher-suite-names="TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256",trust-manager=httpsTM,want-client-auth=true,authentica
tion-optional=true)'
```

Figura: 94 Configuración TLS.

4.16.4 Se ejecutan los siguientes comandos para agregar los oyentes de HTTP(S).

```
root@192:/home/utnfica-ejbca-pki# sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=def
ault-server/http-listener=http:add(socket-binding="http", redirect-socket="https")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server/https-listener=https:a
dd(socket-binding="https", ssl-context="https", max-parameters=2048)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':read-attribute(name=server-state)'
{"outcome" => "success"}
{"outcome" => "success"}
{
    "outcome" => "success",
    "result" => undefined
}
{
    "outcome" => "success",
    "result" => "running"
}
```

Figura: 95 Agregación de oyentes HTTP(S).

4.16.5 Se ejecutan los siguientes comandos para configurar el firewall.

```
root@192:/home/utnfica-ejbca-pki# systemctl enable firewalld --now

firewall-cmd --set-default-zone=dmz

firewall-cmd --zone=dmz --permanent --add-port 8080/tcp

firewall-cmd --zone=dmz --permanent --add-port 8443/tcp

firewall-cmd --reload
success
success
success
success
```

Figura: 96 Configuración de comportamiento del firewall.

4.17 Se ejecutan los siguientes comandos para la configuración del comportamiento del protocolo HTTP.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/system-property=org.apache.catalina.co
nnector.URI_ENCODING:add(value="UTF-8")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/system-property=org.apache.catalina.connector.USE_BODY_ENCODING
_FOR_QUERY_STRING:add(value=true)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/system-property=org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCOD
ED_SLASH:add(value=true)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/system-property=org.apache.tomcat.util.http.Parameters.MAX_COUN
T:add(value=2048)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/system-property=org.apache.catalina.connector.CoyoteAdapter.ALL
OW_BACKSLASH:add(value=true)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=webservices:write-attribute(name=wsdl-host, value=jbo
ssws.undefined.host)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=webservices:write-attribute(name=modify-wsdl-address,
 value=true)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':read-attribute(name=server-state)'
[sudo] contraseña para utnfica-ejbca-pki:
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{"outcome" => "success"}
{
    "outcome" => "success",
    "result" => undefined
}
{
    "outcome" => "success",
    "result" => "running"
}
```

Figura: 97 Configuración del comportamiento del protocolo HTTP.

4.18 Configuración opcional.

4.18.1 Se ejecutan los siguientes comandos para eliminar el contenido de bienvenida de Wildfly.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-serv
er/host=default-host/location="\/":remove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/configuration=handler/file=welcome-content:r
emove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':read-attribute(name=server-state)'

sudo rm -rf /opt/wildfly/welcome-content/
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
{
    "outcome" => "success",
    "result" => undefined
}
{
    "outcome" => "success",
    "result" => "running"
}
```

Figura: 98 Eliminación del contenido de bienvenida de Wildfly.

4.18.2 Se ejecutan los siguientes comandos para redirigir a la aplicación para URL desconocidas.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/configuration=filte
r/rewrite=redirect-to-app:add(redirect=true,target="/ejbca/adminweb/")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server/host=default-host/filt
er-ref=redirect-to-app:add(priority=1,predicate="method(GET) and not path-prefix(/ejbca,/crls,/certificates,/.
well-known) and not equals({\%{LOCAL_PORT}, 4447})")'
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 99 Redirección a la aplicación para URL's desconocidas.

4.18.3 Se ejecutan los siguientes comandos para habilitar la seguridad estricta de la capa de transporte HTTP.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/configuration=filte
r/response-header=hsts:add(header-name="Strict-Transport-Security",header-value="max-age=31536000")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server/host=default-host/filt
er-ref=hsts:add()'
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 100 Activación de la seguridad estricta de la capa de transporte HTTP.

4.18.4 Se ejecutan los siguientes comandos para eliminar la fuente de datos ExampleDS.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=ee/service=default-bindings:
remove()'

sudo /opt/wildfly/bin/jboss-cli.sh --connect 'data-source remove --name=ExampleDS'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':read-attribute(name=server-state)'
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
operation-requires-reload: true
process-state:             reload-required
{
    "outcome" => "success",
    "result" => undefined
}
{
    "outcome" => "success",
    "result" => "running"
}
```

Figura: 101 Eliminación de la fuente de datos ExampleDS.

4.18.5 Se ejecutan los siguientes comandos para agregar un limitador de solicitud.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/configuration=filte
r/request-limit=ejbca-request-limiter:add(max-concurrent-requests=100,queue-size=300)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=undertow/server=default-server/host=default-host/filt
er-ref=ejbca-request-limiter:add(predicate=path-prefix(/ejbca)'
{"outcome" => "success"}
{"outcome" => "success"}
```

Figura: 102 Agregación de un limitador de solicitud.

4.18.6 Se ejecutan los siguientes comandos para agregar soporte para enviar correos electrónicos.

```
utnfica-ejbca-pki@192:~$ sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=elytron/credential-store=def
aultCS:add-alias(alias=smtpPassword, secret-value="****************")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/socket-binding-group=standard-sockets/remote-destination-outbou
nd-socket-binding=ejbca-mail-smtp:add(port="587", host="smtp.office365.com")'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=mail/mail-session="java:/EjbcaMail":add(jndi-name=jav
a:/EjbcaMail, from=certificadodigital@utn.edu.ec)'

sudo /opt/wildfly/bin/jboss-cli.sh --connect '/subsystem=mail/mail-session="java:/EjbcaMail"/server=smtp:add(o
utbound-socket-binding-ref=ejbca-mail-smtp, tls=true, username=certificadodigital@utn.edu.ec, credential-refer
ence={store=defaultCS, alias=smtpPassword})'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':reload'

sudo /opt/wildfly/bin/jboss-cli.sh --connect ':read-attribute(name=server-state)'
```

Figura: 103 Agregación de soporte para enviar correos electrónicos.

4.19 Se ejecuta el siguiente comando para que Wildfly se configure e inicie como servicio.

```
utnfica-ejbca-pki@192:~$ sudo systemctl enable wildfly
Created symlink '/etc/systemd/system/multi-user.target.wants/wildfly.service' → '/etc/systemd/system/wildfly.s
ervice'.
```

Figura: 104 Iniciar Wildfly como servicio.

3.1.6.5 Instalación del software EJBCA community

Antes de continuar con la instalación de EJBCA, debemos realizar la creación de las tablas de la base de datos de ejbca, para lo cual seguimos los siguientes pasos.

1. Desde el explorador de archivos, nos dirigimos al directorio doc/sql-scripts de la carpeta donde se encuentra EJBCA.

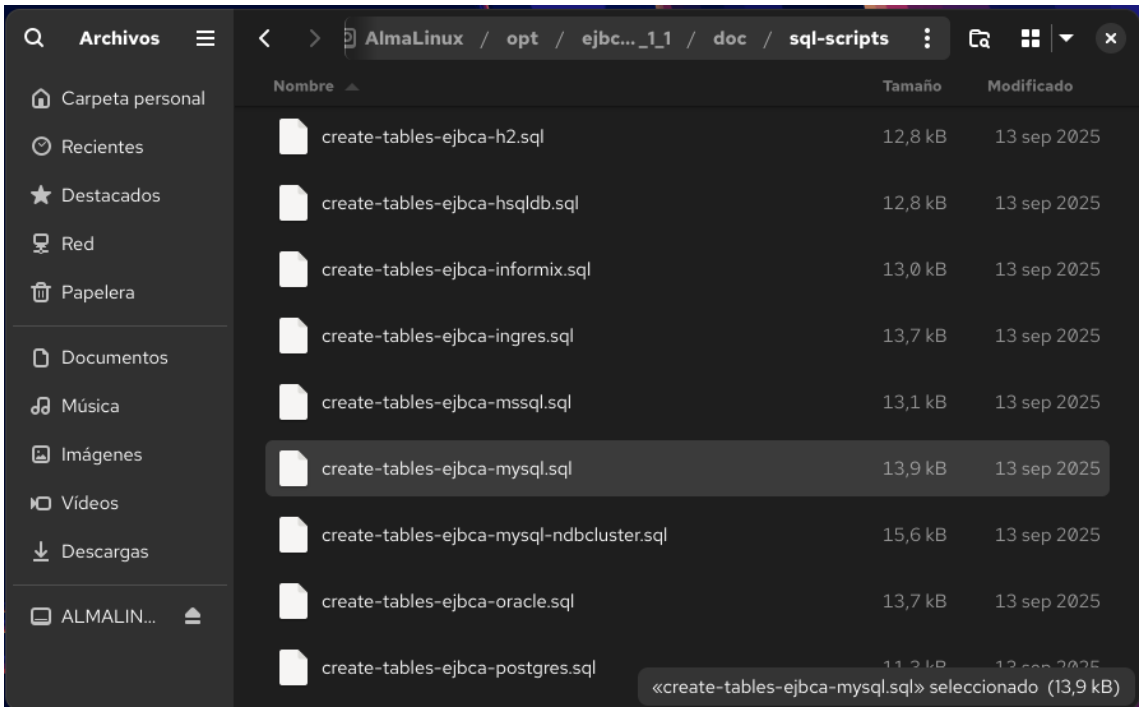


Figura: 105 Directorio de scripts para crear las tablas de la base de datos.

2. Abrimos el archivo create-tables-ejbca-mysql.sql y se copia su contenido.

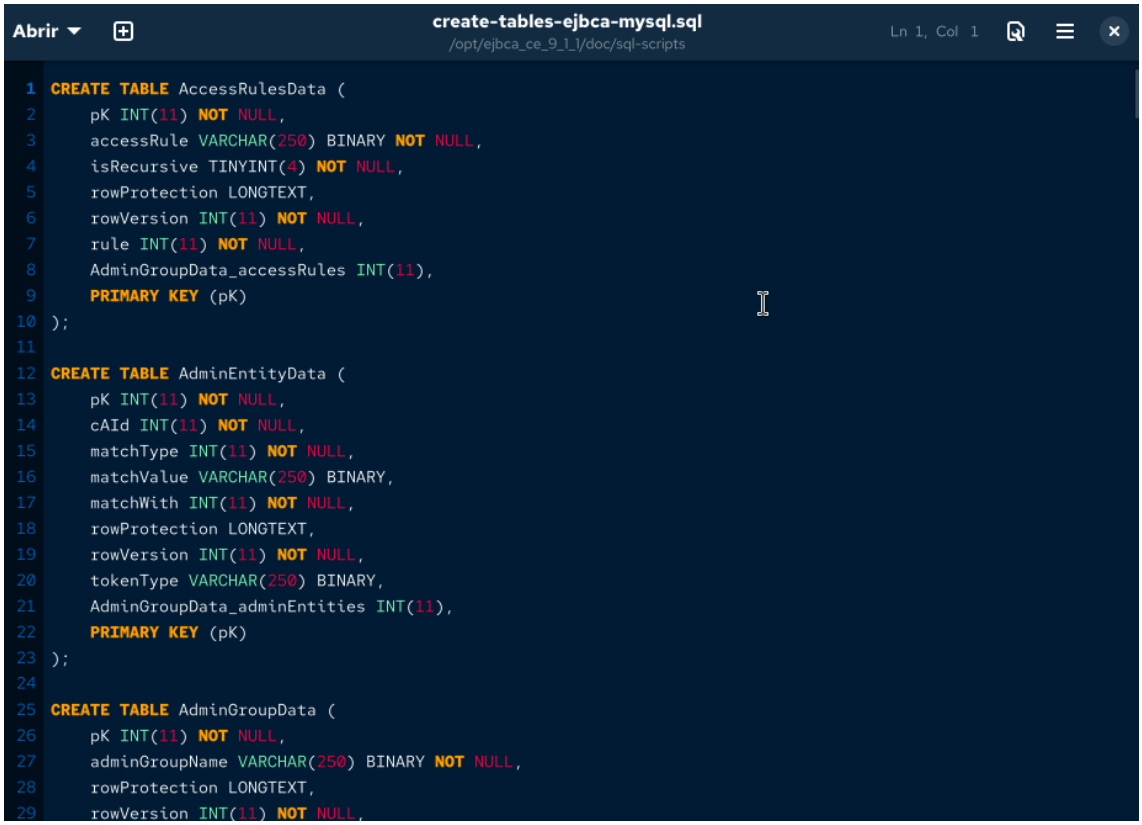


Figura: 106 Archivo create-tables-ejbca-mysql.sql.

3. Se pega en la consola de MariaDB el contenido y se deja que se ejecute.

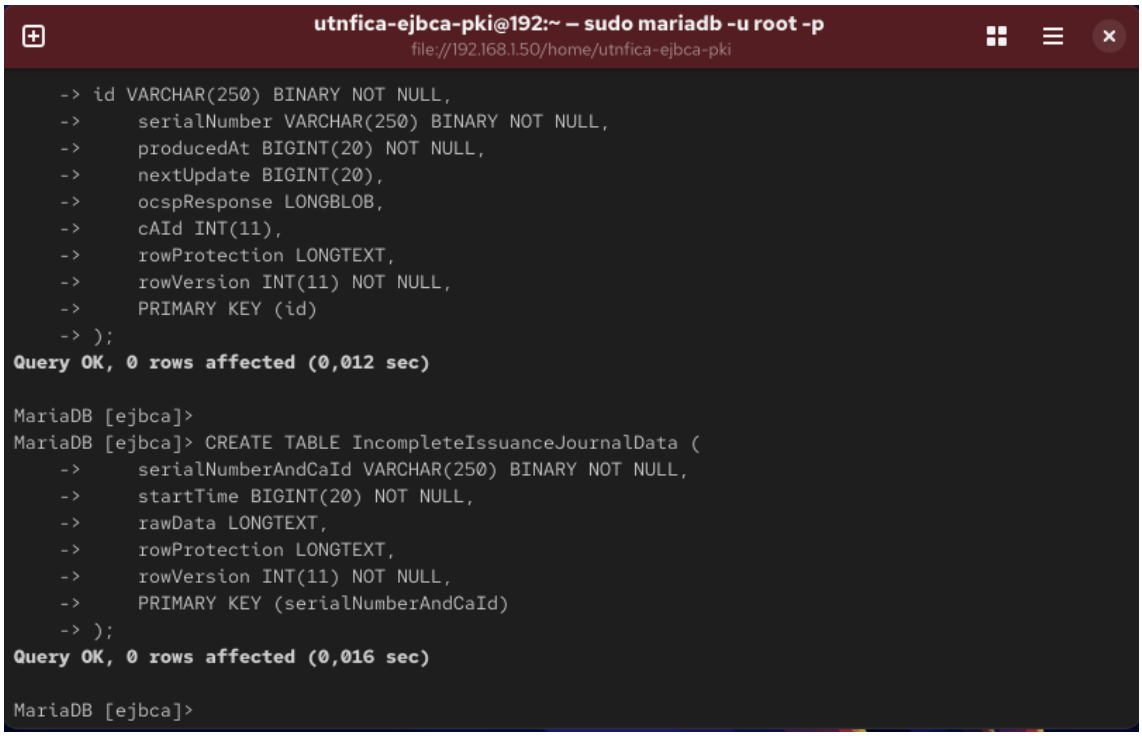


Figura: 107 Creación de tablas de la base de datos ejbca.

4. Abrimos el archivo create-index-ejbca.sql y se copia su contenido.

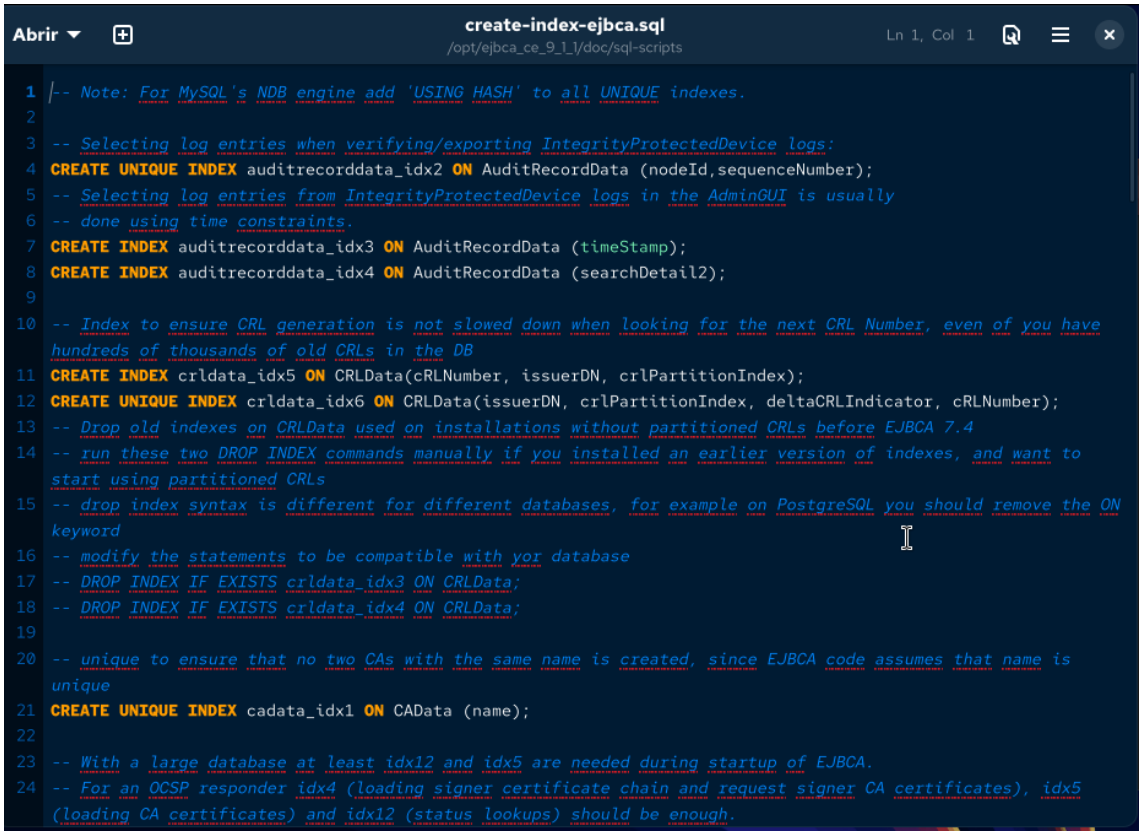


Figura: 108 Archivo create-index-ejbca.sql.

5. Se pega en la consola de MariaDB y se deja que se ejecute.

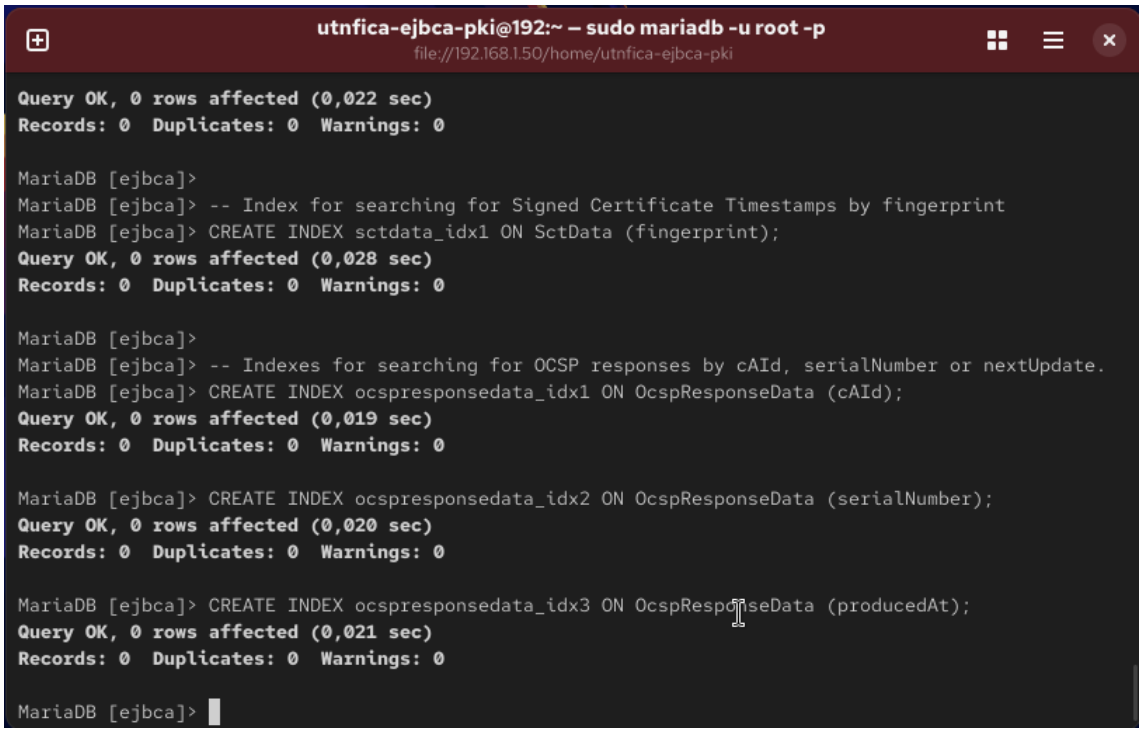


Figura: 109 Creación del índex de la base de datos ejbca.

Una vez realizada la creación de tablas e índex de la base de datos ejbca, realizamos la instalación del sistema mediante Apache ANT.

1. Desde la terminal, nos dirigimos al directorio donde se encuentra ejbca.

```
root@192:/home/utnfica-ejbca-pki# cd /opt/ejbca_ce_9_1_1/
```

Figura: 110 Directorio de ejbca.

2. Ejecutamos el siguiente comando para limpiar la construcción previa del proyecto y luego ejecutar el despliegue de la aplicación EJBCA.

```
root@192:/opt/ejbca_ce_9_1_1# ant -q clean deployear
```

```
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
     [echo] Local documentation is now available in file:///opt/ejbca_ce_9_1_1/tmp/htdocs/docs/index.html
     [echo] in-test-mode: false
     [echo] Enabled module doc.war
     [echo] Enabled module ejbca-ws-ejb.jar
     [echo] Disabled module systemtests-ejb.jar
     [echo] Disabled module statedump-ejb.jar
     [echo] Disabled module configdump-ejb.jar
     [echo] Disabled module peerconnector-ejb.jar
     [echo] Disabled module cesecore-cvcca.jar
     [echo] Enabled module cesecore-x509ca.jar
     [echo] Disabled module proxy-ca.jar
     [echo] Disabled module unidfnr-ejb.jar
     [echo] Disabled module peerconnector.rar
     [echo] Disabled module peerconnector.war
     [echo] Enabled module ra-gui.war
     [echo] Disabled module acme.war
     [echo] Disabled module msae.war
     [echo] Disabled module cits.war
     [echo] Disabled module est.war
     [echo] Enabled module ejbca-rest-api.war
     [echo] Disabled module swagger-ui.war
     [echo] Disabled module ssh.war
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
     [echo] Enabled module status.war
     [echo] Enabled module certstore.war
     [echo] Enabled module crlstore.war
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
     [echo] Specify -Dsignjar.keystore=/path/keystore.jks if you want to sign the release.
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
     [echo] Using appserver.home : /opt/wildfly
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.
     [echo] Task completed 2025-09-23 14:02:48 -0500.

BUILD SUCCESSFUL
Total time: 34 seconds
root@192:/opt/ejbca_ce_9_1_1#
```

Figura: 111 Construcción de la aplicación de EJBCA.

3. Ejecutamos el siguiente comando para verificar el estado de la construcción de EJBCA.

```
root@192:/opt/ejbca_ce_9_1_1# /opt/wildfly/bin/jboss-cli.sh --connect --commands="deployment-info"
NAME                    RUNTIME-NAME            PERSISTENT ENABLED STATUS
ejbca.ear               ejbca.ear               false      true    OK
mariadb-java-client.jar mariadb-java-client.jar false      true    OK
root@192:/opt/ejbca_ce_9_1_1#
```

Figura: 112 Estado de la aplicación de EJBCA.

4. Ejecutamos el siguiente comando que generará la Autoridad Certificadora (CA) de gestión, los almacenes de claves TLS necesarios para manejar HTTPS firmados por la CA de administración, así como el almacén de claves del superadministrador inicial. Además, añadirá ciertos valores de control de acceso iniciales en la base de datos e información de roles para el usuario superadministrador.

```
root@192:/opt/ejbca_ce_9_1_1# ant runinstall
```

```
     [echo] appserver.home         : /opt/wildfly
     [echo]

ejbca:install:

ejbca:initCA:
     [echo] Initializing CA with 'UTNManagementCA' 'CN=UTNManagementCA,O=UTN,C=EC' 'soft' '<ca.tokenpassword h
idden>' '2048' 'RSA' '3650' 'null' 'SHA256WithRSA'   -superadmincn 'SuperAdminUTN'...

ejbca:adminweb:
     [echo] batch tomcat

ejbca:setclearpwd:

ejbca:batchsuperadmin:
     [echo] batch superadmin

ejbca:deploytrustprompt:
    [input] skipping input as property java.trustpassword has already been set.

ejbca:javatruststore:
    [input] skipping input as property ca.name has already been set.
     [echo] Getting root certificate in DER format...
     [echo] ca getcacert "UTNManagementCA" /tmp/rootca.der -der
     [echo] Adding to or creating keystore: /opt/ejbca_ce_9_1_1/p12/truststore.p12

ejbca:javatruststore-removeold:
     [exec] Se ha agregado el certificado al almacén de claves
     [exec] [Almacenando /opt/ejbca_ce_9_1_1/p12/truststore.p12]
   [delete] Deleting: /tmp/rootca.der

BUILD SUCCESSFUL
Total time: 32 seconds
root@192:/opt/ejbca_ce_9_1_1#
```

Figura: 113 Instalación de la aplicación EJBCA.

5. Ejecutamos el siguiente comando para reiniciar Wildfly y que inicie con las nuevas configuraciones de la instalación de EJBCA.

```
root@192:/opt/ejbca_ce_9_1_1# systemctl restart wildfly
```

Figura: 114 Reinicio del servidor de aplicaciones Wildfly.

6. Revisamos nuevamente el estado de la aplicación de EJBCA.

```
root@192:/opt/ejbca_ce_9_1_1# /opt/wildfly/bin/jboss-cli.sh --connect --commands="deployment-info"
NAME                    RUNTIME-NAME            PERSISTENT ENABLED STATUS
ejbca.ear               ejbca.ear               false      true    OK
mariadb-java-client.jar mariadb-java-client.jar false      true    OK
```

Figura: 115 Estado de la aplicación de EJBCA.

7. Realizado los pasos anteriores, ya se han creado los almacenes de claves TLS y se ejecuta el siguiente comando para copiarlos dentro de Wildfly.

```
root@192:/opt/ejbca_ce_9_1_1# ant deploy-keystore
```

```
set-paths-jboss7:

set-paths:

jee:check:
     [echo] Using appserver.home : /opt/wildfly

jee:keystore:
     [echo] Using JBoss deploy directory /opt/wildfly/standalone/deployments
     [copy] Copying 1 file to /opt/wildfly/standalone/configuration/keystore

customejbca.message:
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.

set-paths-jboss7:

set-paths:

jee:deploytruststore:
     [copy] Copying 1 file to /opt/wildfly/standalone/configuration/keystore

BUILD SUCCESSFUL
Total time: 0 seconds
root@192:/opt/ejbca_ce_9_1_1#
```

Figura: 116 Copia de claves TLS.

8. Ejecutamos los siguientes comandos para dar los permisos de la carpeta keystore de wildfly al usuario wildfly.

```
root@192:/opt/ejbca_ce_9_1_1# chown -R wildfly:wildfly /opt/wildfly/standalone/configuration/keystore/

chmod 600 /opt/wildfly/standalone/configuration/keystore/*.p12
```

Figura: 117 Asignación de permisos del usuario wildlfy a la carpeta wildfly.

9. Reiniciamos nuevamente el servidor de aplicaciones.

```
root@192:/opt/ejbca_ce_9_1_1# systemctl restart wildfly
```

Figura: 118 Reinicio del servidor de aplicaciones Wildfly.

10. Revisamos el estado de la aplicación EJBCA.

```
root@192:/opt/ejbca_ce_9_1_1# /opt/wildfly/bin/jboss-cli.sh --connect --commands="deployment-info"
NAME                    RUNTIME-NAME            PERSISTENT ENABLED STATUS
ejbca.ear               ejbca.ear               false      true    OK
mariadb-java-client.jar mariadb-java-client.jar false      true    OK
```

Figura: 119 Estado de la aplicación de EJBCA.

11. Desde el explorador de archivos, nos dirigimos al directorio de p12, dentro de la capeta de ejbca y copiamos el archivo superadmin.p12, que nos servirá como credencial de acceso para el sistema de EJBCA.

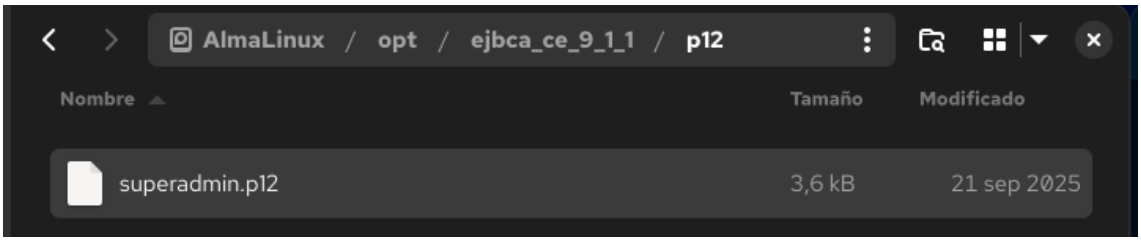


Figura: 120 Archivo de certificado superadmin.p12.

12. Abrimos nuestro navegador de preferencia, en este caso Firefox.
13. Entramos en los ajustes del navegador.
14. Nos dirigimos a la sección de “Privacidad y seguridad”.
15. Nos dirigimos a la sección de Certificados y hacemos clic en “Ver certificados”.
16. En la siguiente ventana, nos ubicamos en la sección de “Sus certificados” y hacemos clic en importar.
17. El navegador nos pedirá la contraseña para este certificado y colocamos la contraseña configurada anteriormente en el archivo web.properties.
18. Vemos que se nos agrega el certificado para poder autenticarnos en el sistema de EJBCA.
19. Colocamos la URL para acceder al sistema de administración de EJBCA y nos pedirá el certificado para autenticarse; seleccionamos el certificado instalado anteriormente.
20. Nos dará el acceso inicial al sistema de EJBCA.

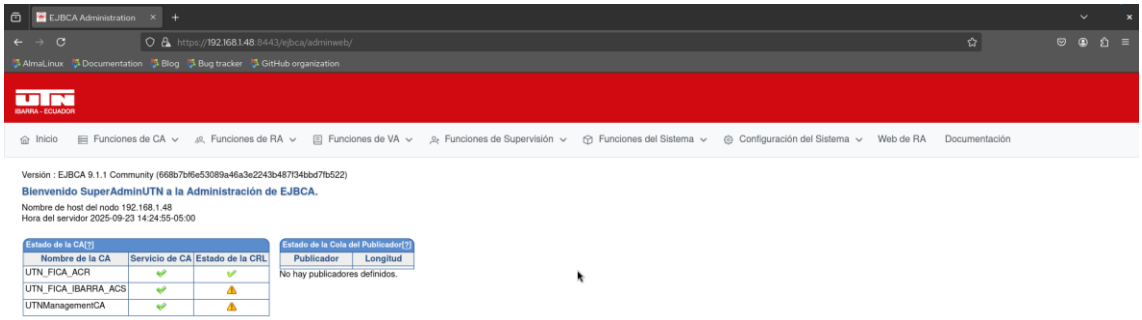


Figura: 121 Página principal de administración EJBCA.

3.1.6.6 Configuración del servicio de firma electrónica

Configuración de la jerarquía PKI

Una vez completada la instalación del software requerido para el servicio de firma electrónica en la Universidad Técnica del Norte, Facultad FICA, se procede con la configuración de la jerarquía PKI anteriormente definida. Este proceso se lleva a cabo mediante la consola de administración de EJBCA Community, donde se establecen los perfiles de certificados, se crean las autoridades de certificación correspondientes, se configuran los tokens criptográficos y se definen los perfiles de entidades finales, garantizando así la correcta implementación de la estructura jerárquica planteada.

1. Creación de la Autoridad Certificadora Raíz (RootCA)

1.1 Definición del perfil de certificado

El primer paso consiste en la creación de un perfil de certificado, el cual corresponde a una plantilla en la que se establecen las propiedades y parámetros que tendrán los certificados emitidos por esta Autoridad Certificadora. Dentro de los atributos más relevantes definidos en este perfil se encuentra el algoritmo criptográfico que será utilizado y el periodo de validez asignado al certificado.

1.1.1 A través de las funciones de la Autoridad Certificadora (CA) en la consola de administración, se accede a la sección de Perfiles de Certificados, donde se clona el perfil preexistente denominado ROOTCA y le asignamos la identificación de UTN_FICA_ARC_PERFIL.

Figura: 122 Creación de perfil de certificado para autoridad certificadora raíz.

1.1.2 Una vez generado el perfil de certificado, se procede a su edición, seleccionando el algoritmo ECDSA para la creación de las llaves criptográficas.

1.1.3 A continuación, se establece el periodo de validez del certificado, que en este caso corresponde a 30 años, y se asigna una descripción que identifique al perfil de certificado configurado.

1.1.4 Finalmente, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

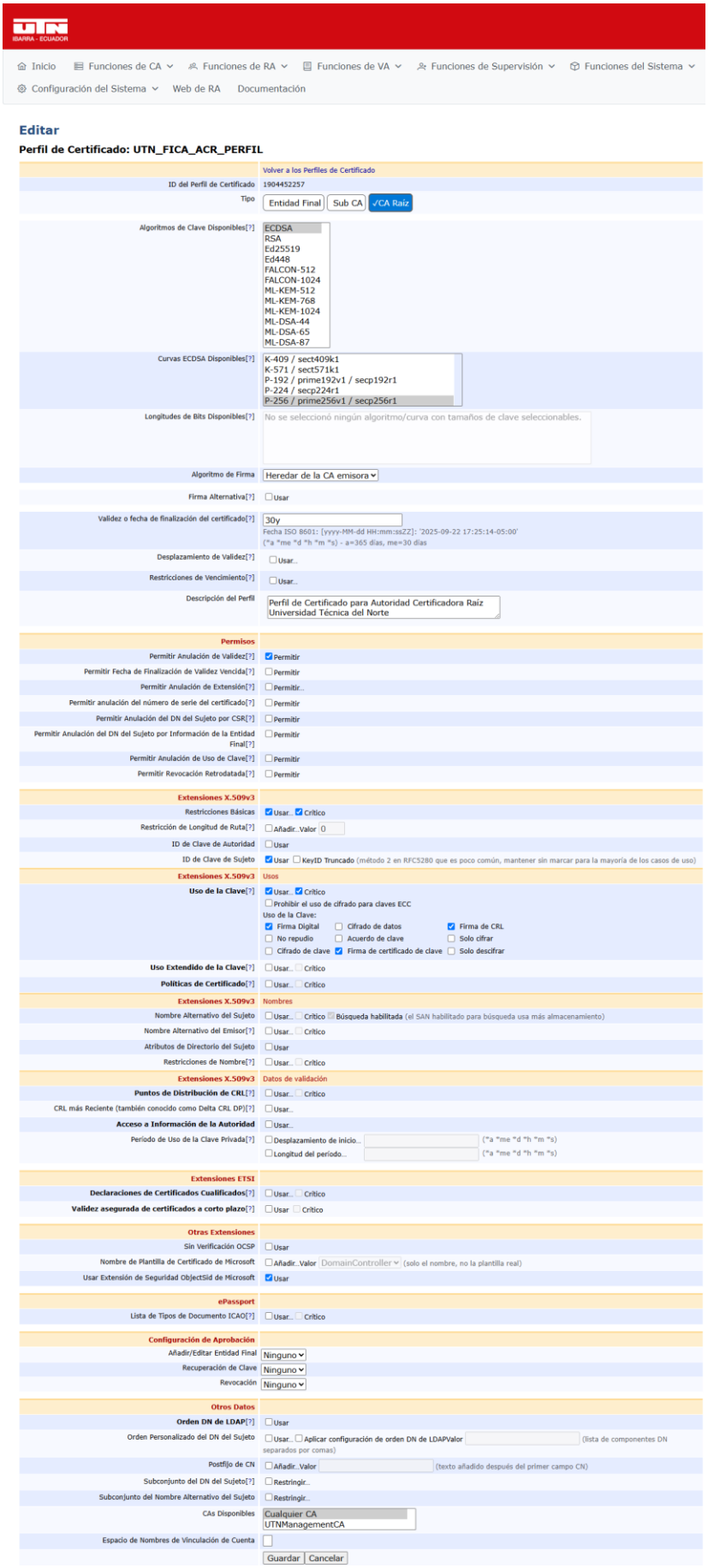

UTN
IBARRA - ECUADOR
Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar
Perfil de Certificado: UTN_FICA_ACR_PERFIL
Volver a los Perfiles de Certificado
ID del Perfil de Certificado
1904452257
Tipo
Entidad Final
Sub CA
√CA Raíz
Algoritmos de Clave Disponibles[?]
ECDSA
RSA
Ed25519
Ed448
FALCON-512
FALCON-1024
ML-KEM-512
ML-KEM-768
ML-KEM-1024
ML-DSA-44
ML-DSA-65
ML-DSA-87
Curvas ECDSA Disponibles[?]
K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1
Longitudes de Bits Disponibles[?]
No se seleccionó ningún algoritmo/curva con tamaños de clave seleccionables.
Algoritmo de Firma
Heredar de la CA emisora
Firma Alternativa[?]
Usar
Validez o fecha de finalización del certificado[?]
30y
Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 17:25:14-05:00'
("a "me "d "h "m "s) - a=365 días, me=30 días
Desplazamiento de Validez[?]
Usar..
Restricciones de Vencimiento[?]
Usar..
Descripción del Perfil
Perfil de Certificado para Autoridad Certificadora Raíz
Universidad Técnica del Norte
Permisos
Permitir Anulación de Validez[?]
Permitir
Permitir Fecha de Finalización de Validez Vencida[?]
Permitir
Permitir Anulación de Extensión[?]
Permitir..
Permitir anulación del número de serie del certificado[?]
Permitir
Permitir Anulación del DN del Sujeto por CSR[?]
Permitir
Permitir Anulación del DN del Sujeto por Información de la Entidad Final[?]
Permitir
Permitir Anulación de Uso de Clave[?]
Permitir
Permitir Revocación Retrodatada[?]
Permitir
Extensiones X.509v3
Restricciones Básicas
Usar.. Crítico
Restricción de Longitud de Ruta[?]
Añadir..Valor 0
ID de Clave de Autoridad
Usar
ID de Clave de Sujeto
Usar KeyID Truncado (método 2 en RFC5280 que es poco común, mantener sin marcar para la mayoría de los casos de uso)
Extensiones X.509v3
Usos
Uso de la Clave[?]
Usar.. Crítico
Prohibir el uso de cifrado para claves ECC
Uso de la Clave:
Firma Digital
Cifrado de datos
Firma de CRL
No repudio
Acuerdo de clave
Solo cifrar
Cifrado de clave
Firma de certificado de clave
Solo descifrar
Uso Extendido de la Clave[?]
Usar.. Crítico
Políticas de Certificado[?]
Usar.. Crítico
Extensiones X.509v3
Nombres
Nombre Alternativo del Sujeto
Usar.. Crítico Búsqueda habilitada (el SAN habilitado para búsqueda usa más almacenamiento)
Nombre Alternativo del Emisor[?]
Usar.. Crítico
Atributos de Directorio del Sujeto
Usar
Restricciones de Nombre[?]
Usar.. Crítico
Extensiones X.509v3
Datos de validación
Puntos de Distribución de CRL[?]
Usar.. Crítico
CRL más Reciente (también conocido como Delta CRL DP)[?]
Usar..
Acceso a Información de la Autoridad
Usar..
Período de Uso de la Clave Privada[?]
Desplazamiento de inicio..
("a "me "d "h "m "s)
Longitud del período..
("a "me "d "h "m "s)
Extensiones ETSI
Declaraciones de Certificados Cualificados[?]
Usar.. Crítico
Validez asegurada de certificados a corto plazo[?]
Usar Crítico
Otras Extensiones
Sin Verificación OCSP
Usar
Nombre de Plantilla de Certificado de Microsoft
Añadir..Valor DomainController (solo el nombre, no la plantilla real)
Usar Extensión de Seguridad ObjectSid de Microsoft
Usar
ePassport
Lista de Tipos de Documento ICAO[?]
Usar.. Crítico
Configuración de Aprobación
Añadir/Editar Entidad Final
Ninguno
Recuperación de Clave
Ninguno
Revocación
Ninguno
Otros Datos
Orden DN de LDAP[?]
Usar
Orden Personalizado del DN del Sujeto
Usar.. Aplicar configuración de orden DN de LDAPValor
(lista de componentes DN separados por comas)
Postfijo de CN
Añadir..Valor
(texto añadido después del primer campo CN)
Subconjunto del DN del Sujeto[?]
Restringir..
Subconjunto del Nombre Alternativo del Sujeto
Restringir..
CAs Disponibles
Cualquier CA
UTNManagementCA
Espacio de Nombres de Vinculación de Cuenta
Guardar
Cancelar

Figura: 123 Configuración de perfil de certificado para autoridad certificadora raíz.

1.2 Crear token criptográfico.

El siguiente paso consiste en la creación de un token criptográfico, el cual será utilizado por la Autoridad Certificadora Raíz para la firma de los certificados digitales emitidos. Es recomendable definir un token criptográfico independiente para cada Autoridad Certificadora.

1.2.1 Desde las funciones de la Autoridad Certificadora (CA), se accede a la opción Tokens Criptográficos, donde se procede a generar un nuevo token identificado como UTN_FICA_CRYPTO_TOKEN. Durante su configuración se habilita la opción de auto activación, lo que permite que, en caso de reinicio del servicio, el token se active automáticamente. Finalmente, se establece una contraseña asociada al token para garantizar su seguridad.

Figura: 124 Creación token criptográfico para autoridad certificadora raíz.

1.2.2 Una vez creado el token criptográfico para la Autoridad Certificadora Raíz, se procede a la generación de tres llaves criptográficas.

1.2.2.1 Se define una llave de firma, utilizando el algoritmo de ECDSA, la cual se identifica con el nombre UTN_FICA_SIGN.

1.2.2.2 A continuación, se crea una llave de cifrado, implementando el algoritmo RSA, con la denominación UTN_FICA_ENCRYPT_KEY.

1.2.2.3 Finalmente, se genera una llave de pruebas, también con el algoritmo ECDSA, asignándole el identificador UTN_FICA_TEST_KEY.

Figura: 125 Configuración token criptográfico para la autoridad certificadora raíz.

1.3 Creación de la Autoridad Certificadora Raíz

1.3.1 Desde las funciones de la Autoridad Certificadora (CA), se accede a la opción Autoridades Certificadoras, donde se procede a crear una nueva entidad con la denominación UTN_FICA_ACR.

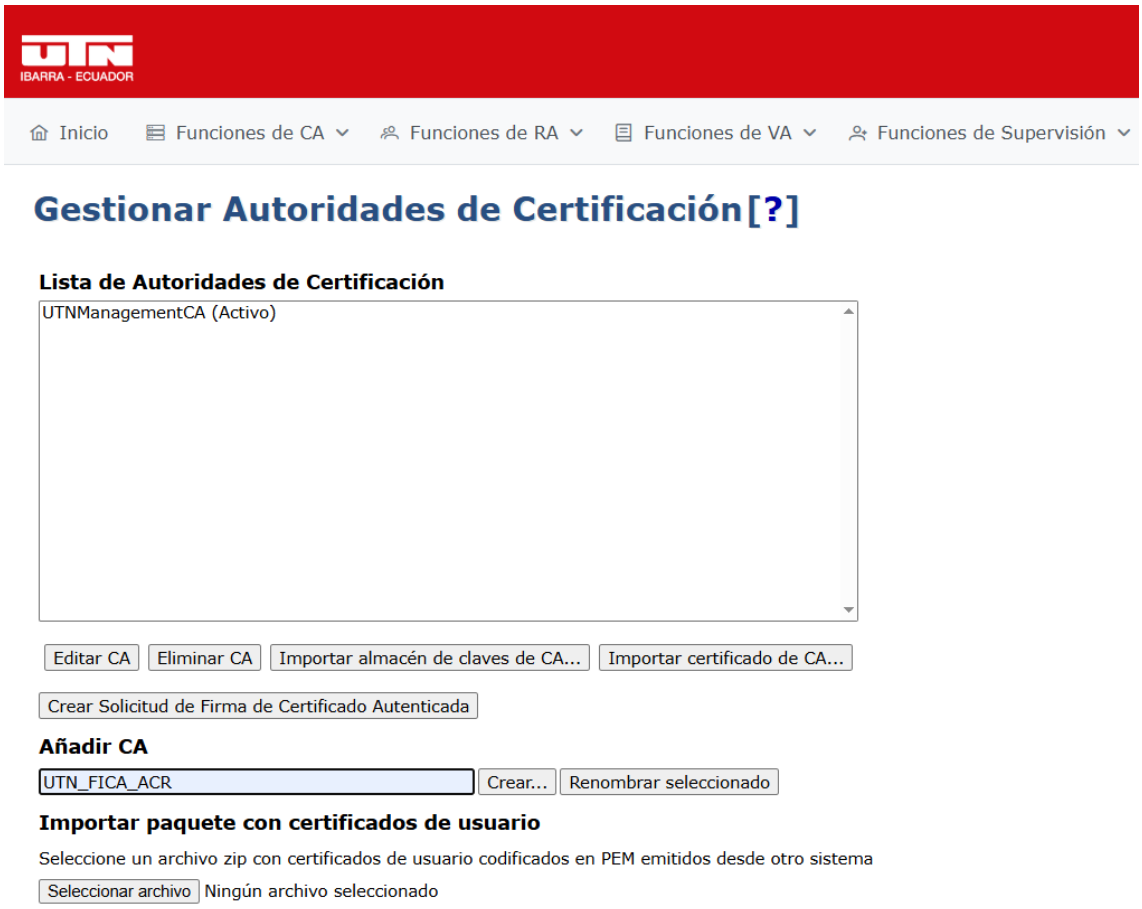


Figura: 126 Creación autoridad certificadora raíz.

1.3.2 Realizamos la configuración de la autoridad creada como en la siguiente figura.

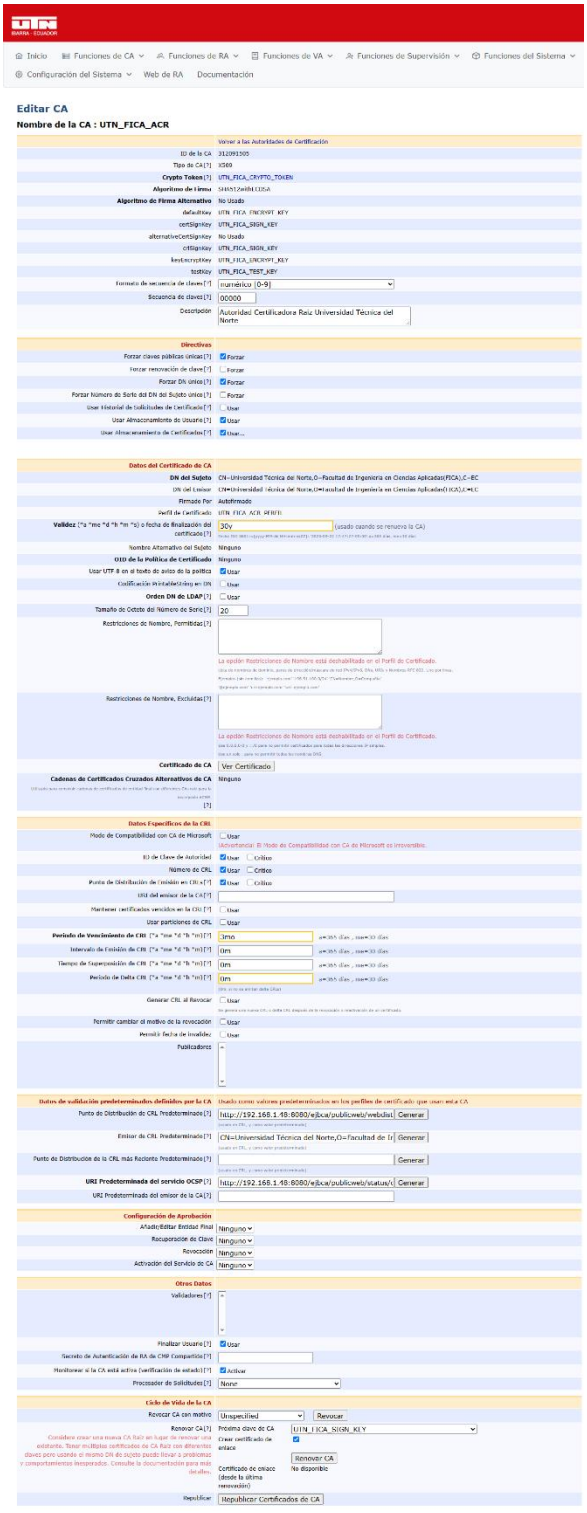


Figura: 127 Configuración autoridad certificadora raíz.

2. Creación de la autoridad certificadora subdelegada (SubCA)

2.1 Definición del perfil de certificado

2.1.1 Desde las funciones de la autoridad certificadora (CA) en la consola de administración, se accede a la sección perfiles de certificados, donde se clona

el perfil preexistente denominado SUBCA. Al nuevo perfil generado se le asigna la identificación UTN_FICA_ACS_PERFIL.

Figura: 128 Creación perfil de certificado para autoridad certificadora subdelegada.

2.1.2 Una vez definido el perfil de certificado para la autoridad certificadora subdelegada, se procede a su edición seleccionando el algoritmo de ECDSA para la generación de las llaves criptográficas.

2.1.3 Posteriormente, se establece un periodo de validez de 30 años para dicho certificado y se incorpora una descripción que identifique claramente al perfil configurado.

2.1.4 Finalmente, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

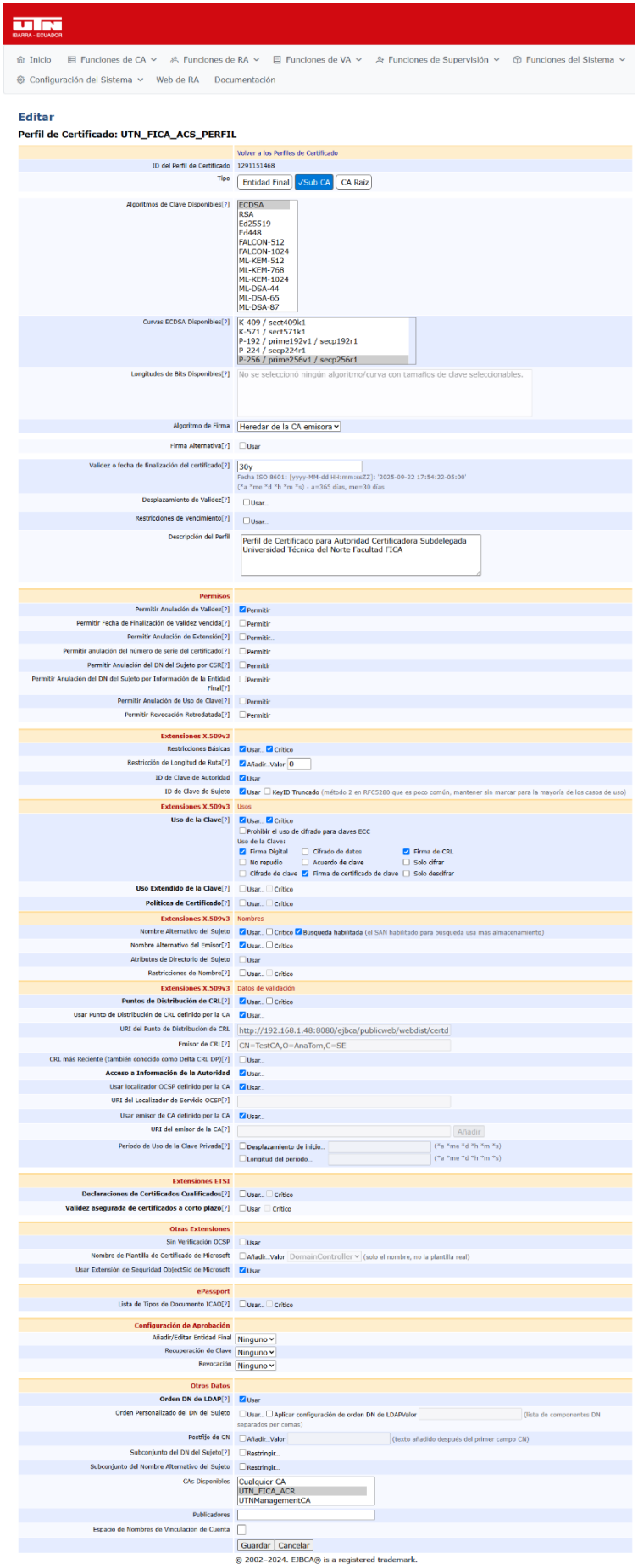

Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar
Perfil de Certificado: UTN_FICA_ACS_PERFIL
Volver a los Perfiles de Certificado
ID del Perfil de Certificado
1291151468
Tipo
Entidad Final
√Sub CA
CA Raíz
Algoritmos de Clave Disponibles[?]
ECDSA
RSA
Ed25519
Ed448
FALCON-512
FALCON-1024
ML-KEM-512
ML-KEM-768
ML-KEM-1024
ML-DSA-44
ML-DSA-65
ML-DSA-87
Curvas ECDSA Disponibles[?]
K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1
Longitudes de Bits Disponibles[?]
No se seleccionó ningún algoritmo/curva con tamaños de clave seleccionables.
Algoritmo de Firma
Heredar de la CA emisora
Firma Alternativa[?]
Usar
Validez o fecha de finalización del certificado[?]
30y
Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 17:54:22-05:00'
('a "me "d "h "m "s) - a=365 días, me=30 días
Desplazamiento de Validez[?]
Usar..
Restricciones de Vencimiento[?]
Usar..
Descripción del Perfil
Perfil de Certificado para Autoridad Certificadora Subdelegada
Universidad Técnica del Norte Facultad FICA
Permisos
Permitir Anulación de Validez[?]
Permitir
Permitir Fecha de Finalización de Validez Vencida[?]
Permitir
Permitir Anulación de Extensión[?]
Permitir..
Permitir anulación del número de serie del certificado[?]
Permitir
Permitir Anulación del DN del Sujeto por CSR[?]
Permitir
Permitir Anulación del DN del Sujeto por Información de la Entidad Final[?]
Permitir
Permitir Anulación de Uso de Clave[?]
Permitir
Permitir Revocación Retrodatada[?]
Permitir
Extensiones X.509v3
Restricciones Básicas
Usar.. Crítico
Restricción de Longitud de Ruta[?]
Añadir..Valor 0
ID de Clave de Autoridad
Usar
ID de Clave de Sujeto
Usar KeyID Truncado (método 2 en RFC5280 que es poco común, mantener sin marcar para la mayoría de los casos de uso)
Extensiones X.509v3
Usos
Uso de la Clave[?]
Usar.. Crítico
Prohibir el uso de cifrado para claves ECC
Uso de la Clave:
Firma Digital
Cifrado de datos
Firma de CRL
No repudio
Acuerdo de clave
Solo cifrar
Cifrado de clave
Firma de certificado de clave
Solo descifrar
Uso Extendido de la Clave[?]
Usar.. Crítico
Políticas de Certificado[?]
Usar.. Crítico
Extensiones X.509v3
Nombres
Nombre Alternativo del Sujeto
Usar.. Crítico Búsqueda habilitada (el SAN habilitado para búsqueda usa más almacenamiento)
Nombre Alternativo del Emisor[?]
Usar.. Crítico
Atributos de Directorio del Sujeto
Usar
Restricciones de Nombre[?]
Usar.. Crítico
Extensiones X.509v3
Datos de validación
Puntos de Distribución de CRL[?]
Usar.. Crítico
Usar Punto de Distribución de CRL definido por la CA
Usar..
URI del Punto de Distribución de CRL
http://192.168.1.48:8080/ejbca/publicweb/webdist/certd
Emisor de CRL[?]
CN=TestCA,O=AnaTom,C=SE
CRL más Reciente (también conocido como Delta CRL DP)[?]
Usar..
Acceso a Información de la Autoridad
Usar..
Usar localizador OCSP definido por la CA
Usar..
URI del Localizador de Servicio OCSP[?]
Usar emisor de CA definido por la CA
Usar..
URI del emisor de la CA[?]
Añadir
Periodo de Uso de la Clave Privada[?]
Desplazamiento de Inicio..
('a "me "d "h "m "s)
Longitud del periodo..
('a "me "d "h "m "s)
Extensiones ETSI
Declaraciones de Certificados Cualificados[?]
Usar.. Crítico
Validez asegurada de certificados a corto plazo[?]
Usar Crítico
Otras Extensiones
Sin Verificación OCSP
Usar
Nombre de Plantilla de Certificado de Microsoft
Añadir..Valor DomainController (solo el nombre, no la plantilla real)
Usar Extensión de Seguridad ObjectSid de Microsoft
Usar
ePassport
Lista de Tipos de Documento ICAO[?]
Usar.. Crítico
Configuración de Aprobación
Añadir/Editar Entidad Final
Ninguno
Recuperación de Clave
Ninguno
Revocación
Ninguno
Otros Datos
Orden DN de LDAP[?]
Usar
Orden Personalizado del DN del Sujeto
Usar.. Aplicar configuración de orden DN de LDAPValor
(lista de componentes DN separados por comas)
Postfijo de CN
Añadir..Valor
(texto añadido después del primer campo CN)
Subconjunto del DN del Sujeto[?]
Restringir..
Subconjunto del Nombre Alternativo del Sujeto
Restringir..
CAs Disponibles
Cualquier CA
UTN_FICA_ACR..
UTNManagementCA
Publicadores
Espacio de Nombres de Vinculación de Cuenta
Guardar
Cancelar
© 2002-2024. EJBCA® is a registered trademark.

Figura: 129 Configuración perfil de certificado para autoridad certificadora subdelegada.

2.2 Crear token criptográfico

2.2.1 Desde las funciones de la autoridad certificadora (CA), se accede a la opción tokens criptográficos, donde se procede a generar un nuevo token identificado como UTN_FICA_ACS_CRYPTO_TOKEN. Durante su configuración se habilita la opción de auto activación, lo que permite que, en caso de reinicio del servicio, el token se active automáticamente. Finalmente, se establece una contraseña asociada al token para garantizar su seguridad.

Figura: 130 Creación token criptográfico para autoridad certificadora subdelegada.

2.2.2 Una vez creado el token criptográfico para la autoridad certificadora subdelegada, se procede a la generación de tres llaves criptográficas.

2.2.2.1 Se define una llave de firma, utilizando el algoritmo de ECDSA, la cual se identifica con el nombre UTN_FICA_ACS_SIGN.

2.2.2.2 A continuación, se crea una llave de cifrado, implementando el algoritmo RSA, con la denominación UTN_FICA_ACS_ENCRYPT_KEY.

2.2.2.3 Finalmente, se genera una llave de pruebas, también con el algoritmo ECDSA, asignándole el identificador UTN_FICA_ACS_TEST_KEY.

Figura: 131 Configuración token criptográfico para la autoridad certificadora subdelegada.

2.3 Creación de la autoridad certificadora subdelegada

2.3.1 Desde las funciones de la autoridad certificadora (CA), se accede a la opción autoridades certificadoras, donde se procede a crear una nueva entidad con la denominación UTN_FICA_IBARRA_ACS.

Figura: 132 Creación autoridad certificadora subdelegada.

2.3.2 Realizamos la configuración de la autoridad creada como en la siguiente figura.

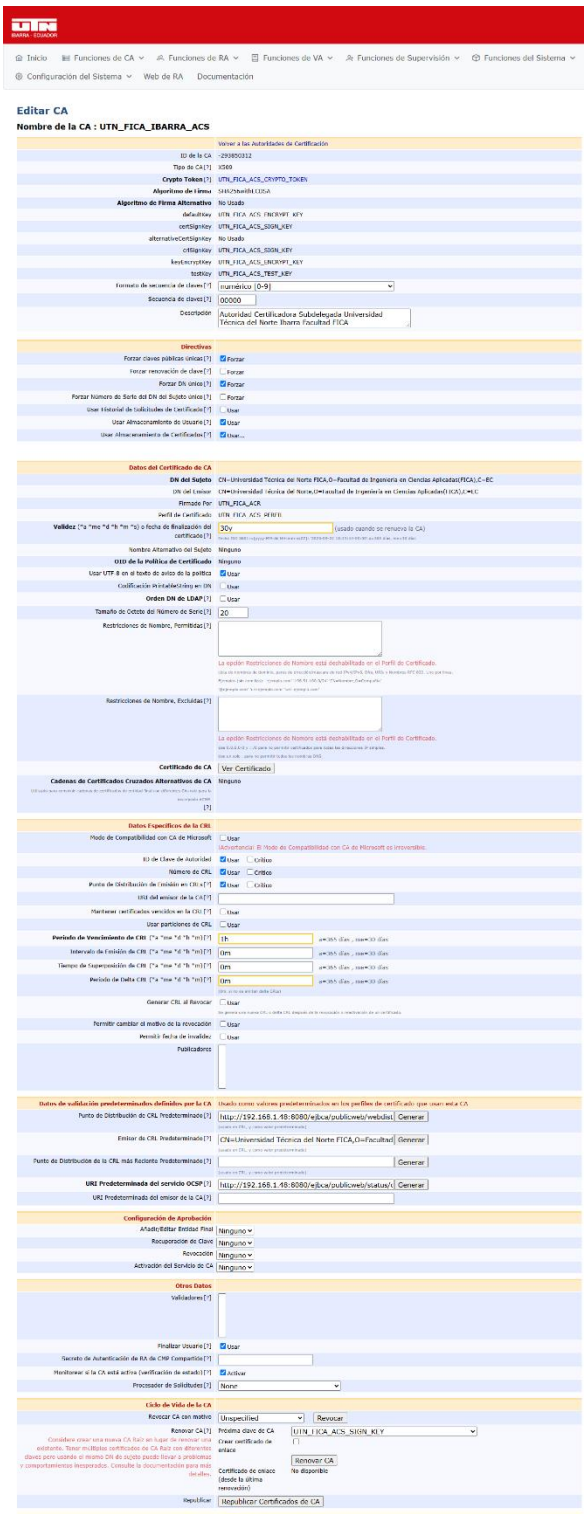


Figura: 133 Configuración autoridad certificadora subdelegada.

3. Creación de entidad final superadministrador

3.1 Definición del perfil de certificado

3.1.1 Desde las funciones de la autoridad certificadora (CA) en la consola de administración, se accede a la sección perfiles de certificados, donde se clona el perfil preexistente denominado ENDUSER. Al nuevo perfil generado se le asigna la identificación UTN_FICA_EFS_PERFIL.

Figura: 134 Creación perfil de certificado para entidad final superadministrador.

3.1.2 A continuación, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

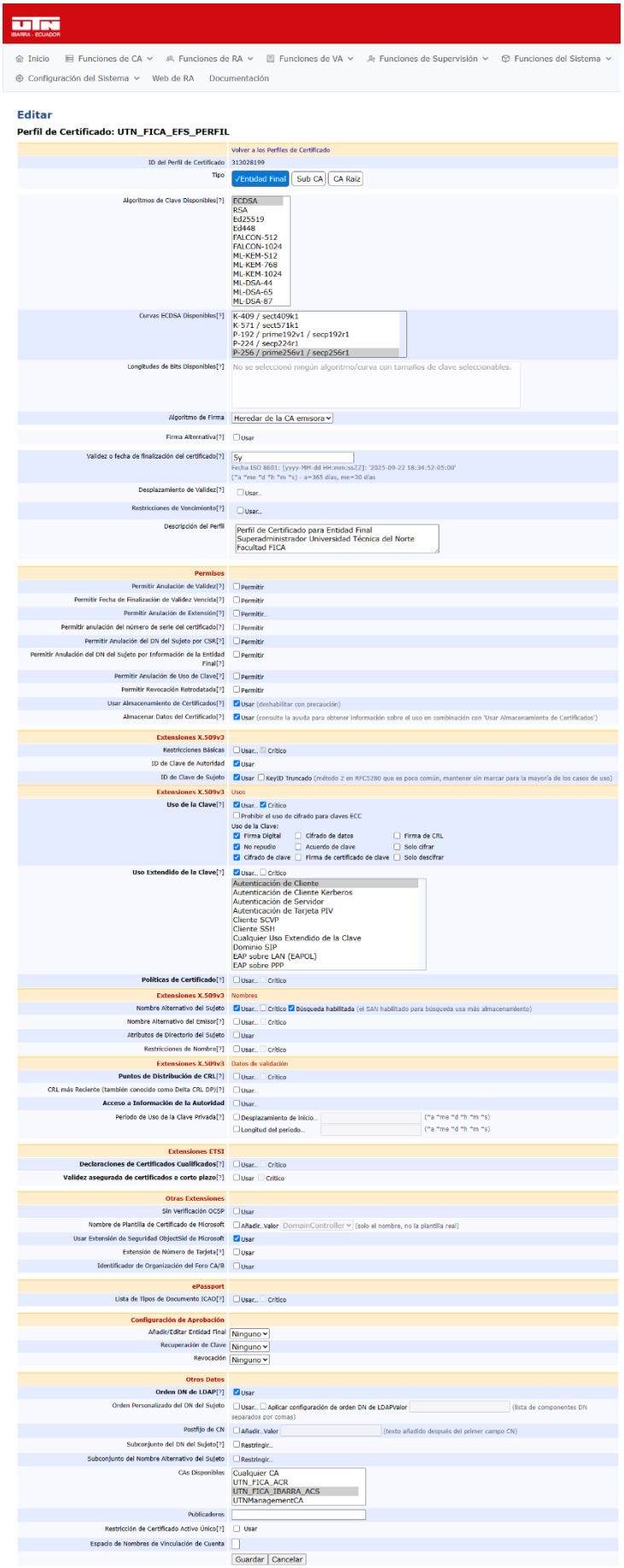

Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar
Perfil de Certificado: UTN_FICA_EFS_PERFIL
Volver a los Perfiles de Certificado
ID del Perfil de Certificado
313028199
Tipo
✓Entidad Final
Sub CA
CA Raíz
Algoritmos de Clave Disponibles[?]
ECDSA
RSA
Ed25519
Ed448
FALCON-512
FALCON-1024
ML-KEM-512
ML-KEM-768
ML-KEM-1024
ML-DSA-44
ML-DSA-65
ML-DSA-87
Curvas ECDSA Disponibles[?]
K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1
Longitudes de Bits Disponibles[?]
No se seleccionó ningún algoritmo/curva con tamaños de clave seleccionables.
Algoritmo de Firma
Heredar de la CA emisora
Firma Alternativa[?]
Usar
Validez o fecha de finalización del certificado[?]
5y
Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 18:34:52-05:00'
("a "me "d "h "m "s) - a=365 días, me=30 días
Desplazamiento de Validez[?]
Usar..
Restricciones de Vencimiento[?]
Usar..
Descripción del Perfil
Perfil de Certificado para Entidad Final
Superadministrador Universidad Técnica del Norte
Facultad FICA
Permisos
Permitir Anulación de Validez[?]
Permitir
Permitir Fecha de Finalización de Validez Vencida[?]
Permitir
Permitir Anulación de Extensión[?]
Permitir..
Permitir anulación del número de serie del certificado[?]
Permitir
Permitir Anulación del DN del Sujeto por CSR[?]
Permitir
Permitir Anulación del DN del Sujeto por Información de la Entidad Final[?]
Permitir
Permitir Anulación de Uso de Clave[?]
Permitir
Permitir Revocación Retrodatada[?]
Permitir
Usar Almacenamiento de Certificados[?]
Usar (deshabilitar con precaución)
Almacenar Datos del Certificado[?]
Usar (consulte la ayuda para obtener información sobre el uso en combinación con 'Usar Almacenamiento de Certificados')
Extensiones X.509v3
Restricciones Básicas
Usar.. Crítico
ID de Clave de Autoridad
Usar
ID de Clave de Sujeto
Usar KeyID Truncado (método 2 en RFC5280 que es poco común, mantener sin marcar para la mayoría de los casos de uso)
Extensiones X.509v3
Usos
Uso de la Clave[?]
Usar.. Crítico
Prohibir el uso de cifrado para claves ECC
Uso de la Clave:
Firma Digital
Cifrado de datos
Firma de CRL
No repudio
Acuerdo de clave
Solo cifrar
Cifrado de clave
Firma de certificado de clave
Solo descifrar
Uso Extendido de la Clave[?]
Usar.. Crítico
Autenticación de Cliente
Autenticación de Cliente Kerberos
Autenticación de Servidor
Autenticación de Tarjeta PIV
Cliente SCVP
Cliente SSH
Cualquier Uso Extendido de la Clave
Dominio SIP
EAP sobre LAN (EAPOL)
EAP sobre PPP
Políticas de Certificado[?]
Usar.. Crítico
Extensiones X.509v3
Nombres
Nombre Alternativo del Sujeto
Usar.. Crítico Búsqueda habilitada (el SAN habilitado para búsqueda usa más almacenamiento)
Nombre Alternativo del Emisor[?]
Usar.. Crítico
Atributos de Directorio del Sujeto
Usar
Restricciones de Nombre[?]
Usar.. Crítico
Extensiones X.509v3
Datos de validación
Puntos de Distribución de CRL[?]
Usar.. Crítico
CRL más Reciente (también conocido como Delta CRL DP)[?]
Usar..
Acceso a Información de la Autoridad
Usar..
Período de Uso de la Clave Privada[?]
Desplazamiento de Inicio..
("a "me "d "h "m "s)
Longitud del período..
("a "me "d "h "m "s)
Extensiones ETSI
Declaraciones de Certificados Cualificados[?]
Usar.. Crítico
Validez asegurada de certificados a corto plazo[?]
Usar Crítico
Otras Extensiones
Sin Verificación OCSP
Usar
Nombre de Plantilla de Certificado de Microsoft
Añadir..Valor
DomainController
(solo el nombre, no la plantilla real)
Usar Extensión de Seguridad ObjectSid de Microsoft
Usar
Extensión de Número de Tarjeta[?]
Usar
Identificador de Organización del Foro CA/B
Usar
ePassport
Lista de Tipos de Documento ICAO[?]
Usar.. Crítico
Configuración de Aprobación
Añadir/Editar Entidad Final
Ninguno
Recuperación de Clave
Ninguno
Revocación
Ninguno
Otros Datos
Orden DN de LDAP[?]
Usar
Orden Personalizado del DN del Sujeto
Usar.. Aplicar configuración de orden DN de LDAPValor
(lista de componentes DN separados por comas)
Postfijo de CN
Añadir..Valor
(texto añadido después del primer campo CN)
Subconjunto del DN del Sujeto[?]
Restringir..
Subconjunto del Nombre Alternativo del Sujeto
Restringir..
CAs Disponibles
Cualquier CA
UTN_FICA_ACR
UTN_FICA_IBARRA_ACS
UTNManagementCA
Publicadores
Restricción de Certificado Activo Único[?]
Usar
Espacio de Nombres de Vinculación de Cuenta
Guardar
Cancelar

Figura: 135 Configuración perfil de certificado para entidad final superadministrador.

3.2 Creación del perfil de entidad final superadministrador

3.2.1 Desde las funciones de la autoridad registro (RA), se accede a la opción perfiles de entidad final, donde se crea un nuevo perfil con la denominación UTN_FICA_EFS.

Figura: 136 Creación entidad final superadministrador.

3.2.2 A continuación, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

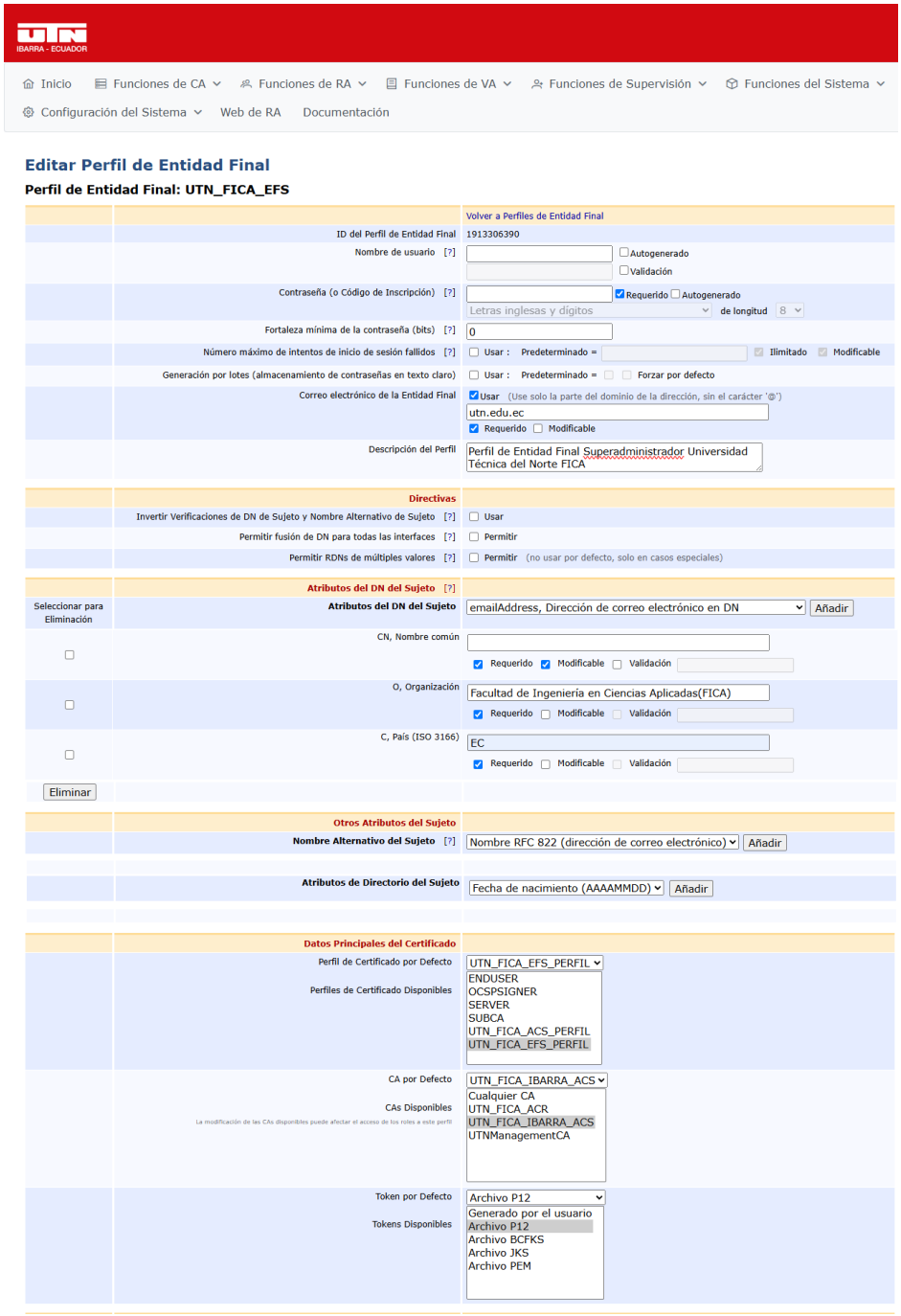


Figura: 137 Configuración entidad final superadministrador.

4. Creación de entidad final autoridad de registro

4.1 Creación del perfil de certificado

4.1.1 Desde las funciones de la autoridad certificadora (CA), se accede a la opción perfiles de certificados, donde se clona el perfil preexistente denominado ENDUSER. Al nuevo perfil generado se le asigna la identificación de UTN_FICA_EFAR_PERFIL.

Figura: 138 Creación perfil de certificado para entidad final autoridad registro.

4.1.2 A continuación, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

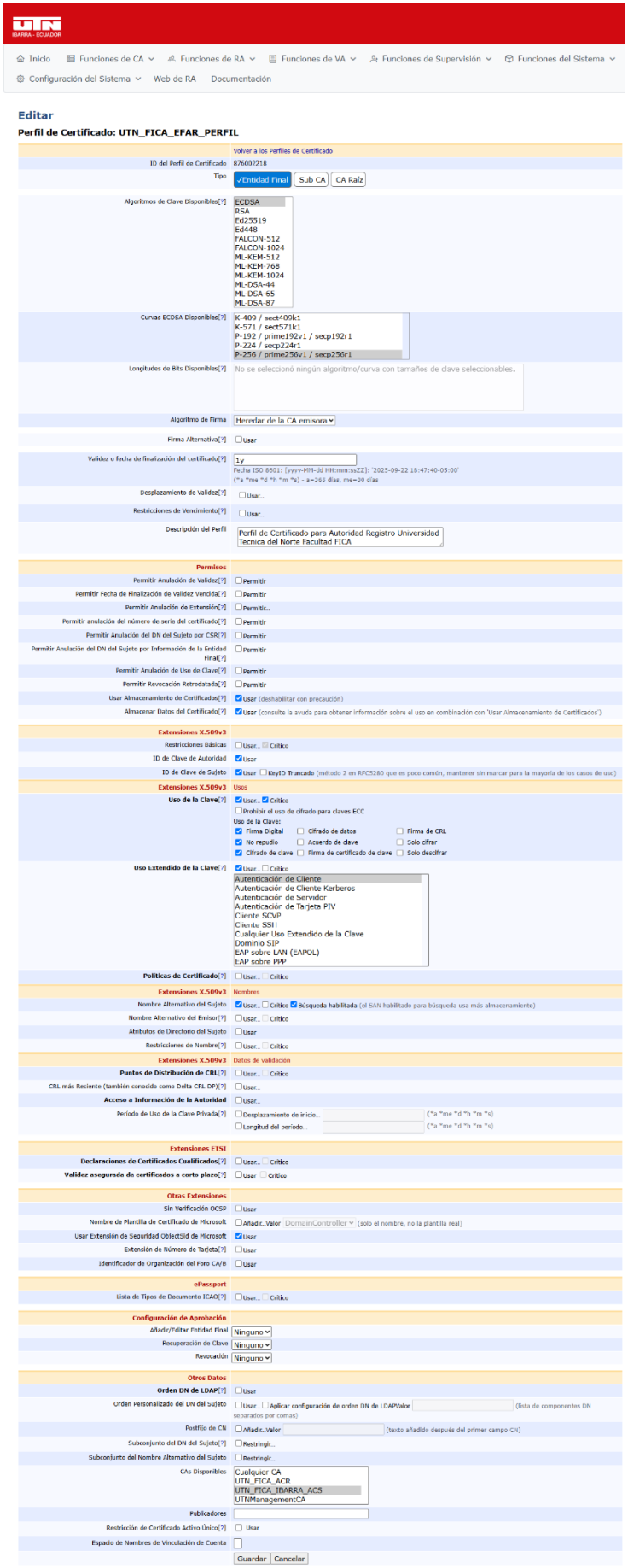

UTN
IBARRA - ECUADOR
Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar
Perfil de Certificado: UTN_FICA_EFAR_PERFIL
Volver a los Perfiles de Certificado
ID del Perfil de Certificado
87602218
Tipo
✓Entidad Final
Sub CA
CA Raíz
Algoritmos de Clave Disponibles[?]
ECDSA
RSA
Ed25519
Ed448
FALCON-512
FALCON-1024
ML-KEM-512
ML-KEM-768
ML-KEM-1024
ML-DSA-44
ML-DSA-65
ML-DSA-87
Curvas ECDSA Disponibles[?]
K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1
Longitudes de Bits Disponibles[?]
No se seleccionó ningún algoritmo/curva con tamaños de clave seleccionables.
Algoritmo de Firma
Heredar de la CA emisora
Firma Alternativa[?]
Usar
Validez o fecha de finalización del certificado[?]
1y
Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 18:47:40-05:00'
("a "me "d "h "m "s) - a=365 días, me=30 días
Desplazamiento de Validez[?]
Usar..
Restricciones de Vencimiento[?]
Usar..
Descripción del Perfil
Perfil de Certificado para Autoridad Registro Universidad Tecnica del Norte Facultad FICA
Permisos
Permitir Anulación de Validez[?]
Permitir
Permitir Fecha de Finalización de Validez Vencida[?]
Permitir
Permitir Anulación de Extensión[?]
Permitir..
Permitir anulación del número de serie del certificado[?]
Permitir
Permitir Anulación del DN del Sujeto por CSR[?]
Permitir
Permitir Anulación del DN del Sujeto por Información de la Entidad Final[?]
Permitir
Permitir Anulación de Uso de Clave[?]
Permitir
Permitir Revocación Retrodatada[?]
Permitir
Usar Almacenamiento de Certificados[?]
Usar (deshabilitar con precaución)
Almacenar Datos del Certificado[?]
Usar (consulte la ayuda para obtener información sobre el uso en combinación con 'Usar Almacenamiento de Certificados')
Extensiones X.509v3
Restricciones Básicas
Usar.. Crítico
ID de Clave de Autoridad
Usar
ID de Clave de Sujeto
Usar KeyID Truncado (método 2 en RFC5280 que es poco común, mantener sin marcar para la mayoría de los casos de uso)
Extensiones X.509v3
Usos
Uso de la Clave[?]
Usar.. Crítico
Prohibir el uso de cifrado para claves ECC
Uso de la Clave:
Firma Digital
Cifrado de datos
Firma de CRL
No repudio
Acuerdo de clave
Solo cifrar
Cifrado de clave
Firma de certificado de clave
Solo descifrar
Uso Extendido de la Clave[?]
Usar.. Crítico
Autenticación de Cliente
Autenticación de Cliente Kerberos
Autenticación de Servidor
Autenticación de Tarjeta PIV
Cliente SCVP
Cliente SSH
Cualquier Uso Extendido de la Clave
Dominio SIP
EAP sobre LAN (EAPOL)
EAP sobre PPP
Políticas de Certificado[?]
Usar.. Crítico
Extensiones X.509v3
Nombres
Nombre Alternativo del Sujeto
Usar.. Crítico Búsqueda habilitada (el SAN habilitado para búsqueda usa más almacenamiento)
Nombre Alternativo del Emisor[?]
Usar.. Crítico
Atributos de Directorio del Sujeto
Usar
Restricciones de Nombre[?]
Usar.. Crítico
Extensiones X.509v3
Datos de validación
Puntos de Distribución de CRL[?]
Usar.. Crítico
CRL más Reciente (también conocido como Delta CRL DP)[?]
Usar..
Acceso a Información de la Autoridad
Usar..
Período de Uso de la Clave Privada[?]
Desplazamiento de inicio..
("a "me "d "h "m "s)
Longitud del período..
("a "me "d "h "m "s)
Extensiones ETSI
Declaraciones de Certificados Cualificados[?]
Usar.. Crítico
Validez asegurada de certificados a corto plazo[?]
Usar Crítico
Otras Extensiones
Sin Verificación OCSP
Usar
Nombre de Plantilla de Certificado de Microsoft
Añadir..Valor DomainController (solo el nombre, no la plantilla real)
Usar Extensión de Seguridad ObjectSid de Microsoft
Usar
Extensión de Número de Tarjeta[?]
Usar
Identificador de Organización del Foro CA/B
Usar
ePassport
Lista de Tipos de Documento ICAO[?]
Usar.. Crítico
Configuración de Aprobación
Añadir/Editar Entidad Final
Ninguno
Recuperación de Clave
Ninguno
Revocación
Ninguno
Otros Datos
Orden DN de LDAP[?]
Usar
Orden Personalizado del DN del Sujeto
Usar.. Aplicar configuración de orden DN de LDAP/Valor
(lista de componentes DN separados por comas)
Postfijo de CN
Añadir..Valor
(texto añadido después del primer campo CN)
Subconjunto del DN del Sujeto[?]
Restringir..
Subconjunto del Nombre Alternativo del Sujeto
Restringir..
CAs Disponibles
Cualquier CA
UTN_FICA_ACR
UTN_FICA_IBARRA_ACS
UTNManagementCA
Publicadores
Restricción de Certificado Activo Único[?]
Usar
Espacio de Nombres de Vinculación de Cuenta
Guardar
Cancelar

Figura: 139 Configuración perfil de certificado para entidad final autoridad registro.

4.2 Creación de perfil de entidad final

4.2.1 Desde las funciones de la autoridad registro (RA), se accede a la opción perfiles de entidad final, donde se crea un nuevo perfil con la denominación UTN_FICA_EFAR.

Figura: 140 Creación entidad final autoridad registro.

4.2.2 A continuación, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

Editar Perfil de Entidad Final

Perfil de Entidad Final: UTN_FICA_EFAR

		Volver a Perfiles de Entidad Final
	ID del Perfil de Entidad Final	2050351845
	Nombre de usuario [?]	☐ Autogenerado ☐ Validación
	Contraseña (o Código de Inscripción) [?]	☑ Requerido ☐ Autogenerado; Letras inglesas y dígitos; de longitud 8
	Fortaleza mínima de la contraseña (bits) [?]	0
	Número máximo de intentos de inicio de sesión fallidos [?]	☐ Usar : Predeterminado = ☑ Ilimitado ☑ Modificable
	Generación por lotes (almacenamiento de contraseñas en texto claro)	☐ Usar : Predeterminado = ☐ Forzar por defecto
	Correo electrónico de la Entidad Final	☑ Usar (Use solo la parte del dominio de la dirección, sin el carácter '@') utn.edu.ec ☑ Requerido ☐ Modificable
	Descripción del Perfil	Perfil de Entidad Final Autoridad Registro Universidad Técnica del Norte Facultad FICA
	Directivas	
	Invertir Verificaciones de DN de Sujeto y Nombre Alternativo de Sujeto [?]	☐ Usar
	Permitir fusión de DN para todas las interfaces [?]	☐ Permitir
	Permitir RDNs de múltiples valores [?]	☐ Permitir (no usar por defecto, solo en casos especiales)
	Atributos del DN del Sujeto [?]	
Seleccionar para Eliminación	**Atributos del DN del Sujeto**	emailAddress, Dirección de correo electrónico en DN — Añadir
☐	CN, Nombre común	☑ Requerido ☑ Modificable ☐ Validación
☐	O, Organización	Facultad de Ingeniería en Ciencias Aplicadas(FICA) ☑ Requerido ☐ Modificable ☐ Validación
☐	C, País (ISO 3166)	EC ☑ Requerido ☐ Modificable ☐ Validación
Eliminar		
	Otros Atributos del Sujeto	
	Nombre Alternativo del Sujeto [?]	Nombre RFC 822 (dirección de correo electrónico) — Añadir
	Atributos de Directorio del Sujeto	Fecha de nacimiento (AAAAMMDD) — Añadir
	Datos Principales del Certificado	
	Perfil de Certificado por Defecto	UTN_FICA_EFAR_PERFIL
	Perfiles de Certificado Disponibles	ENDUSER, OCSPSIGNER, SERVER, SUBCA, UTN_FICA_ACS_PERFIL, UTN_FICA_EFAR_PERFIL, UTN_FICA_EFS_PERFIL
	CA por Defecto	UTN_FICA_IBARRA_ACS
	CAs Disponibles (La modificación de las CAs disponibles puede afectar el acceso de los roles a este perfil)	Cualquier CA, UTN_FICA_ACR, UTN_FICA_IBARRA_ACS, UTNManagementCA
	Token por Defecto	Archivo P12
	Tokens Disponibles	Generado por el usuario, Archivo P12, Archivo BCFKS, Archivo JKS, Archivo PEM
	Otros Datos del Certificado	
	Número de serie del certificado personalizado [?]	☐ Usar
	Hora de inicio de la validez del certificado [?]	☐ Usar : Valor ☑ Modificable (Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 18:56:07-05:00' o días:horas:minutos)
	Hora de finalización de la validez del certificado [?]	☐ Usar : Valor ☑ Modificable (Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 18:56:07-05:00' o días:horas:minutos)
	Número de tarjeta [?]	☐ Usar ☐ Requerido
	Restricciones de Nombre, Permitidas [?]	☐ Usar ☐ Requerido
	Restricciones de Nombre, Excluidas [?]	☐ Usar ☐ Requerido
	Datos de extensión de certificado personalizados [?]	☐ Usar
	Declaración QC ETSI PSD2 [?]	☐ Usar
	Identificador de Organización del Foro CA/B [?]	☐ Usar : Valor ☐ Requerido ☑ Modificable
	Otros Datos	
	Número de solicitudes permitidas [?]	☐ Usar : Predeterminado = 1
	Permitir renovación antes de la expiración [?]	☐ Usar : Días antes del vencimiento: -1
	Motivo de revocación a establecer después de la emisión del certificado [?]	☐ Usar : Valor = Activo ☑ Modificable
	Ocultar Nombre del Sujeto de los registros [?]	☐ Permitir Solo se ocultarán SubjectDN y SubjectAltName de los registros de auditoría y del servidor
	Enviar Notificación [?]	☐ Usar : Predeterminado = ☐ Forzar por defecto Añadir
		Guardar Cancelar

Figura: 141 Configuración de entidad final autoridad registro.

5. Creación de entidad final estudiante

5.1 Creación del perfil de certificado

5.1.1 Desde las funciones de la autoridad certificadora (CA), se accede a la opción perfiles de certificados, donde se clona el perfil preexistente denominado ENDUSER. Al nuevo perfil generado se le asigna la identificación de UTN_FICA_EFE_PERFIL.

Figura: 142 Creación perfil de certificado para entidad final estudiante.

5.1.2 A continuación, los parámetros restantes se ajustan conforme a lo detallado en la figura siguiente.

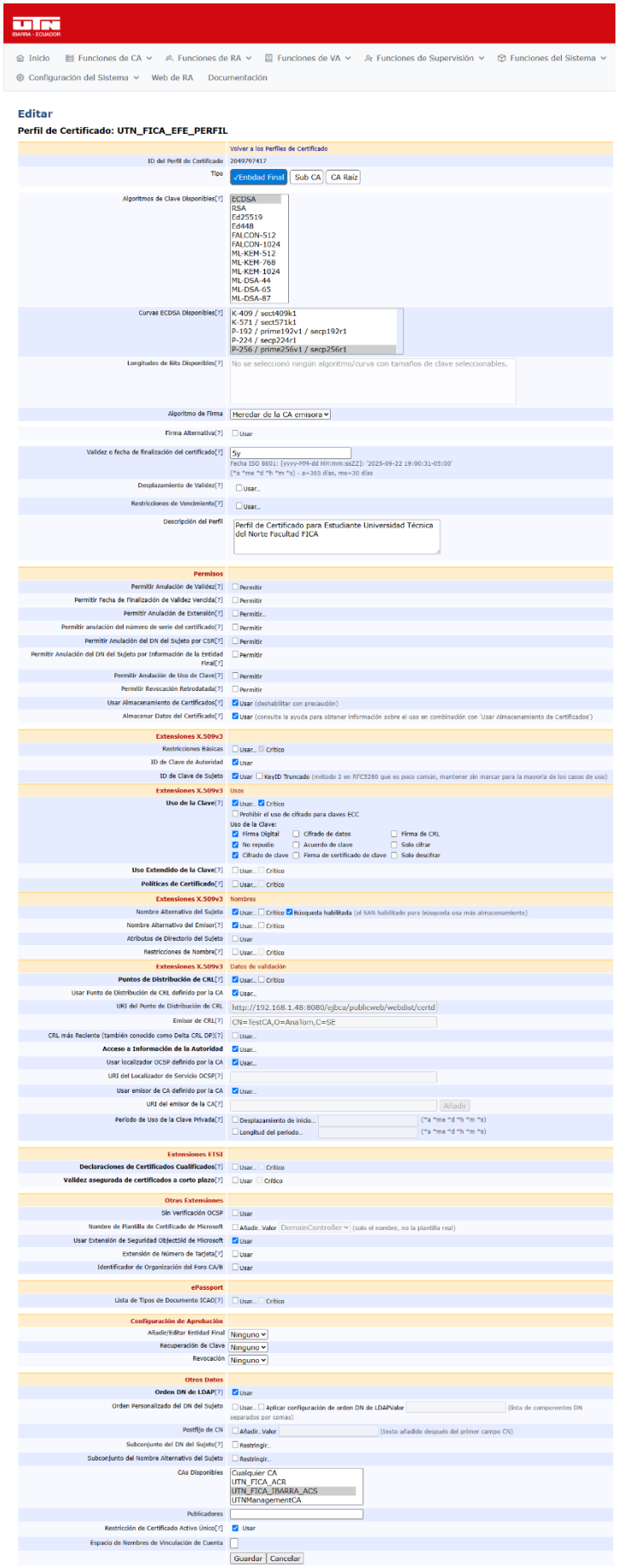

Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar
Perfil de Certificado: UTN_FICA_EFE_PERFIL
Volver a los Perfiles de Certificado
ID del Perfil de Certificado
2049707417
Tipo
√Entidad Final
Sub CA
CA Raíz
Algoritmos de Clave Disponibles[?]
ECDSA
RSA
Ed25519
Ed448
FALCON-512
FALCON-1024
ML-KEM-512
ML-KEM-768
ML-KEM-1024
ML-DSA-44
ML-DSA-65
ML-DSA-87
Curvas ECDSA Disponibles[?]
K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1
Longitudes de Bits Disponibles[?]
No se seleccionó ningún algoritmo/curva con tamaños de clave seleccionables.
Algoritmo de Firma
Heredar de la CA emisora
Firma Alternativa[?]
Usar
Validez o fecha de finalización del certificado[?]
5y
Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 19:00:31-05:00'
("a "me "d "h "m "s) - a=365 días, me=30 días
Desplazamiento de Validez[?]
Usar..
Restricciones de Vencimiento[?]
Usar..
Descripción del Perfil
Perfil de Certificado para Estudiante Universidad Técnica del Norte Facultad FICA
Permisos
Permitir Anulación de Validez[?]
Permitir
Permitir Fecha de Finalización de Validez Vencida[?]
Permitir
Permitir Anulación de Extensión[?]
Permitir..
Permitir anulación del número de serie del certificado[?]
Permitir
Permitir Anulación del DN del Sujeto por CSR[?]
Permitir
Permitir Anulación del DN del Sujeto por Información de la Entidad Final[?]
Permitir
Permitir Anulación de Uso de Clave[?]
Permitir
Permitir Revocación Retrodatada[?]
Permitir
Usar Almacenamiento de Certificados[?]
Usar (deshabilitar con precaución)
Almacenar Datos del Certificado[?]
Usar (consulte la ayuda para obtener información sobre el uso en combinación con 'Usar Almacenamiento de Certificados')
Extensiones X.509v3
Restricciones Básicas
Usar.. Crítico
ID de Clave de Autoridad
Usar
ID de Clave de Sujeto
Usar KeyID Truncado (método 2 en RFC5280 que es poco común, mantener sin marcar para la mayoría de los casos de uso)
Extensiones X.509v3
Usos
Uso de la Clave[?]
Usar.. Crítico
Prohibir el uso de cifrado para claves ECC
Uso de la Clave:
Firma Digital
Cifrado de datos
Firma de CRL
No repudio
Acuerdo de clave
Solo cifrar
Cifrado de clave
Firma de certificado de clave
Solo descifrar
Uso Extendido de la Clave[?]
Usar.. Crítico
Políticas de Certificado[?]
Usar.. Crítico
Extensiones X.509v3
Nombres
Nombre Alternativo del Sujeto
Usar.. Crítico Búsqueda habilitada (el SAN habilitado para búsqueda usa más almacenamiento)
Nombre Alternativo del Emisor[?]
Usar.. Crítico
Atributos de Directorio del Sujeto
Usar
Restricciones de Nombre[?]
Usar.. Crítico
Extensiones X.509v3
Datos de validación
Puntos de Distribución de CRL[?]
Usar.. Crítico
Usar Punto de Distribución de CRL definido por la CA
Usar..
URI del Punto de Distribución de CRL
http://192.168.1.48:8080/ejbca/publicweb/webdist/certd
Emisor de CRL[?]
CN=TestCA,O=AnaTom,C=SE
CRL más Reciente (también conocido como Delta CRL DP)[?]
Usar..
Acceso a Información de la Autoridad
Usar..
Usar localizador OCSP definido por la CA
Usar..
URI del Localizador de Servicio OCSP[?]
Usar emisor de CA definido por la CA
Usar..
URI del emisor de la CA[?]
Añadir
Período de Uso de la Clave Privada[?]
Desplazamiento de inicio..
("a "me "d "h "m "s)
Longitud del periodo..
("a "me "d "h "m "s)
Extensiones ETSI
Declaraciones de Certificados Cualificados[?]
Usar.. Crítico
Validez asegurada de certificados a corto plazo[?]
Usar Crítico
Otras Extensiones
Sin Verificación OCSP
Usar
Nombre de Plantilla de Certificado de Microsoft
Añadir..Valor
DomainController
(solo el nombre, no la plantilla real)
Usar Extensión de Seguridad ObjectSid de Microsoft
Usar
Extensión de Número de Tarjeta[?]
Usar
Identificador de Organización del Foro CA/B
Usar
ePassport
Lista de Tipos de Documento ICAO[?]
Usar.. Crítico
Configuración de Aprobación
Añadir/Editar Entidad Final
Ninguno
Recuperación de Clave
Ninguno
Revocación
Ninguno
Otros Datos
Orden DN de LDAP[?]
Usar
Orden Personalizado del DN del Sujeto
Usar.. Aplicar configuración de orden DN de LDAPValor
(lista de componentes DN separados por comas)
Postfijo de CN
Añadir..Valor
(texto añadido después del primer campo CN)
Subconjunto del DN del Sujeto[?]
Restringir..
Subconjunto del Nombre Alternativo del Sujeto
Restringir..
CAs Disponibles
Cualquier CA
UTN_FICA_ACR
UTN_FICA_IBARRA_ACS
UTNManagementCA
Publicadores
Restricción de Certificado Activo Único[?]
Usar
Espacio de Nombres de Vinculación de Cuenta
Guardar
Cancelar

Figura: 143 Configuración perfil de certificado para entidad final estudiante.

5.2 Creación del perfil de entidad final.

5.2.1 Desde las funciones de la autoridad registro (RA), se accede a la opción perfiles de entidad final, donde se crea un nuevo perfil con la denominación UTN_FICA_EFE.

Figura: 144 Creación entidad final estudiante.

5.2.2 Este perfil presenta una configuración particular respecto a los demás, ya que será utilizado para la emisión de certificados digitales destinados a los estudiantes. En este caso, se establecen los datos que el estudiante debe proporcionar al momento de realizar su solicitud, tales como el nombre de usuario, correo institucional, identificación institucional y nombres completos. Adicionalmente, se configura los eventos de notificación mediante correo electrónico, de manera que el estudiante sea informado cuando su certificado haya sido generado o, en su defecto, revocado. El detalle de esta configuración se muestra en la figura siguiente.

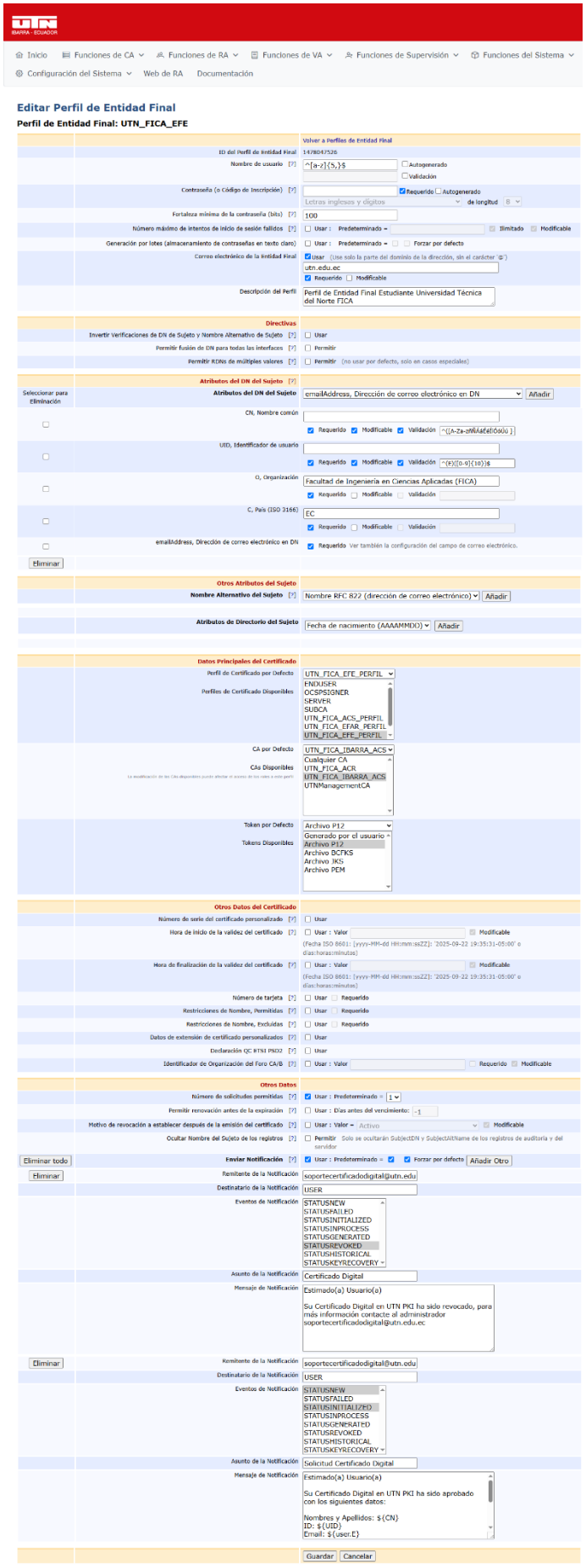

Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar Perfil de Entidad Final
Perfil de Entidad Final: UTN_FICA_EFE
Volver a Perfiles de Entidad Final
ID del Perfil de Entidad Final
1478047526
Nombre de usuario
^[a-z]{5,}$
Autogenerado
Validación
Contraseña (o código de Inscripción)
Requerido
Autogenerado
Letras inglesas y dígitos
de longitud
8
Fortaleza mínima de la contraseña (bits)
100
Número máximo de intentos de inicio de sesión fallidos
Usar :
Predeterminado =
Ilimitado
Modificable
Generación por lotes (almacenamiento de contraseñas en texto claro)
Usar :
Predeterminado =
Forzar por defecto
Correo electrónico de la Entidad Final
Usar
(Use solo la parte del dominio de la dirección, sin el carácter '@')
utn.edu.ec
Requerido
Modificable
Descripción del Perfil
Perfil de Entidad Final Estudiante Universidad Técnica del Norte FICA
Directivas
Invertir Verificaciones de DN de Sujeto y Nombre Alternativo de Sujeto
Usar
Permitir fusión de DN para todas las interfaces
Permitir
Permitir RDNs de múltiples valores
Permitir
(no usar por defecto, solo en casos especiales)
Atributos del DN del Sujeto
Seleccionar para Eliminación
Atributos del DN del Sujeto
emailAddress, Dirección de correo electrónico en DN
Añadir
CN, Nombre común
Requerido
Modificable
Validación
^([A-Za-zñÑáÁéÉíÍóÓúÚ]
UID, Identificador de usuario
Requerido
Modificable
Validación
^([0-9]{10})$
O, Organización
Facultad de Ingeniería en Ciencias Aplicadas (FICA)
Requerido
Modificable
Validación
C, País (ISO 3166)
EC
Requerido
Modificable
Validación
emailAddress, Dirección de correo electrónico en DN
Requerido
Ver también la configuración del campo de correo electrónico.
Eliminar
Otros Atributos del Sujeto
Nombre Alternativo del Sujeto
Nombre RFC 822 (dirección de correo electrónico)
Añadir
Atributos de Directorio del Sujeto
Fecha de nacimiento (AAAAMMDD)
Añadir
Datos Principales del Certificado
Perfil de Certificado por Defecto
UTN_FICA_EFE_PERFIL
Perfiles de Certificado Disponibles
ENDUSER
OCSPSIGNER
SERVER
SUBCA
UTN_FICA_ACS_PERFIL
UTN_FICA_EFAR_PERFIL
UTN_FICA_EFE_PERFIL
CA por Defecto
UTN_FICA_IBARRA_ACS
CAs Disponibles
Cualquier CA
UTN_FICA_ACR
UTN_FICA_IBARRA_ACS
UTNManagementCA
Token por Defecto
Archivo P12
Tokens Disponibles
Generado por el usuario
Archivo P12
Archivo DCFKS
Archivo JKS
Archivo PEM
Otros Datos del Certificado
Número de serie del certificado personalizado
Usar
Hora de inicio de la validez del certificado
Usar : Valor
Modificable
(Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 19:35:31-05:00' o días:horas:minutos)
Hora de finalización de la validez del certificado
Usar : Valor
Modificable
(Fecha ISO 8601: [yyyy-MM-dd HH:mm:ssZZ]: '2025-09-22 19:35:31-05:00' o días:horas:minutos)
Número de tarjeta
Usar
Requerido
Restricciones de Nombre, Permitidas
Usar
Requerido
Restricciones de Nombre, Excluidas
Usar
Requerido
Datos de extensión de certificado personalizados
Usar
Declaración QC RTSI PSD2
Usar
Identificador de Organización del Foro CA/B
Usar : Valor
Requerido
Modificable
Otros Datos
Número de solicitudes permitidas
Usar : Predeterminado =
1
Permitir renovación antes de la expiración
Usar : Días antes del vencimiento:
-1
Motivo de revocación a establecer después de la emisión del certificado
Usar : Valor =
Activo
Modificable
Ocultar Nombre del Sujeto de los registros
Permitir
Solo se ocultarán SubjectDN y SubjectAltName de los registros de auditoría y del servidor
Eliminar todo
Enviar Notificación
Usar : Predeterminado =
Forzar por defecto
Añadir Otro
Eliminar
Remitente de la Notificación
soportecertificadodigital@utn.edu
Destinatario de la Notificación
USER
Eventos de Notificación
STATUSNEW
STATUSFAILED
STATUSINITIALIZED
STATUSINPROCESS
STATUSGENERATED
STATUSREVOKED
STATUSHISTORICAL
STATUSKEYRECOVERY
Asunto de la Notificación
Certificado Digital
Mensaje de Notificación
Estimado(a) Usuario(a)
Su Certificado Digital en UTN PKI ha sido revocado, para más información contacte al administrador
soportecertificadodigital@utn.edu.ec
Eliminar
Remitente de la Notificación
soportecertificadodigital@utn.edu
Destinatario de la Notificación
USER
Eventos de Notificación
STATUSNEW
STATUSFAILED
STATUSINITIALIZED
STATUSINPROCESS
STATUSGENERATED
STATUSREVOKED
STATUSHISTORICAL
STATUSKEYRECOVERY
Asunto de la Notificación
Solicitud Certificado Digital
Mensaje de Notificación
Estimado(a) Usuario(a)
Su Certificado Digital en UTN PKI ha sido aprobado con los siguientes datos:
Nombres y Apellidos: ${CN}
ID: ${UID}
Email: ${user.E}
Guardar
Cancelar

Figura: 145 Configuración entidad final estudiante.

Configuración de la arquitectura del servicio de firma electrónica.

Una vez concluida la configuración de la jerarquía PKI, se procede a ajustar el sistema para que opere conforme a la arquitectura definida. En esta etapa es necesario establecer los roles de usuario, las reglas de acceso, los perfiles de aprobación y, además, emitir los certificados digitales de administración correspondientes para las autoridades de registro y el superadministrador.

1. Configuración del rol de superadministrador

1.1 Emisión del certificado digital de superadministrador

Este certificado constituye el mecanismo de autenticación que permitirá el acceso completo a todas las funciones del sistema.

1.1.1 Desde la consola de administración del RA, se accede a la opción nueva solicitud, a fin de iniciar el proceso de generación del certificado.

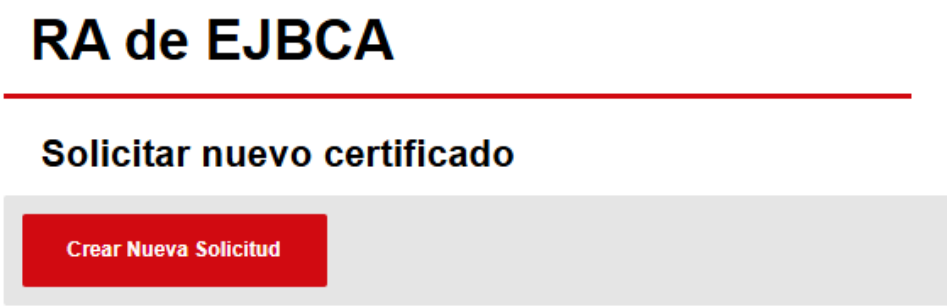


Figura: 146 Creación certificado digital superadministrador.

1.1.2 Se selecciona el perfil de certificado de superadministrador denominado UTN_FICA_EFS

1.1.3 Se indica que el par de claves criptográficas sea generado directamente por la autoridad certificadora UTN (CA).

1.1.4 A continuación, se completa el formulario de solicitud con la información requerida, incluyendo la definición de un usuario y una contraseña asociados al perfil.

1.1.5 Finalmente, se procede con la descarga del certificado digital correspondiente.

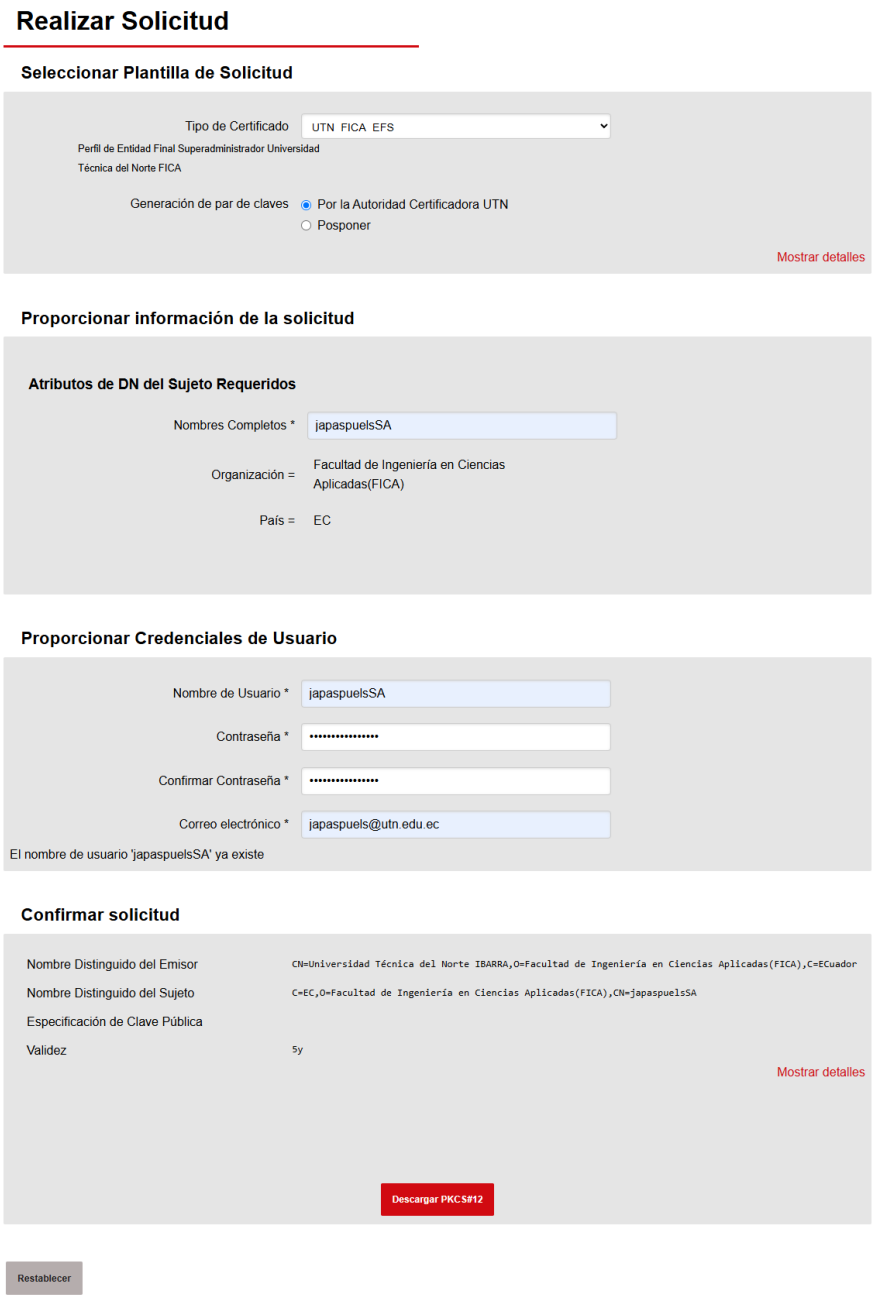


Figura: 147 Solicitud certificado digital superadministrador.

1.2 Configuración del rol superadministrador

1.2.1 Se instala el certificado digital de superadministrador previamente descargado, iniciando el asistente de importación de certificados del sistema operativo.

1.2.2 Durante el proceso de importación, se selecciona el certificado a instalar.

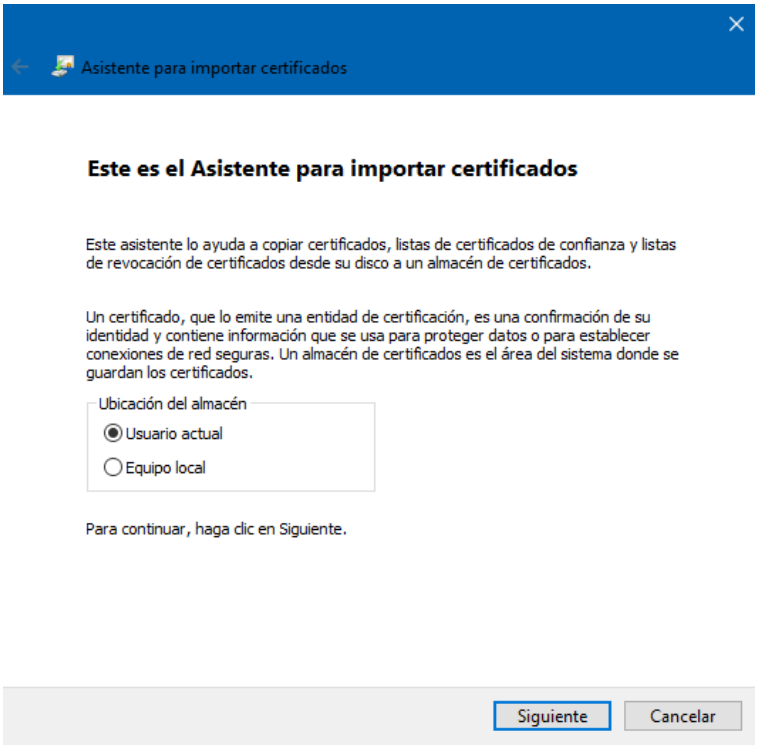


Figura: 148 Selección de ubicación del almacén a instalar el certificado.

1.2.3 Se selecciona el certificado digital a importar.

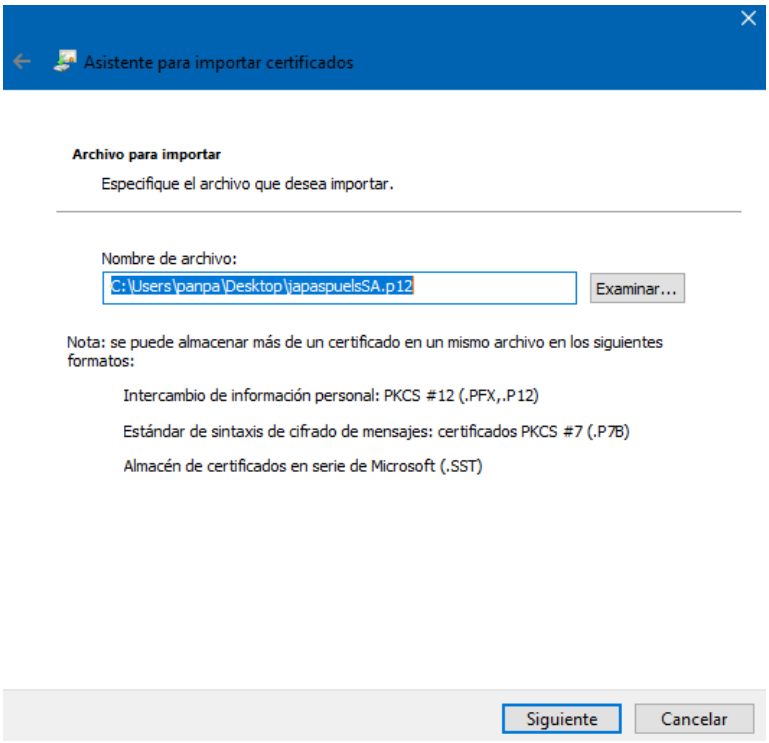


Figura: 149 Selección del certificado a instalar.

1.2.4 Ingresamos la contraseña del certificado.

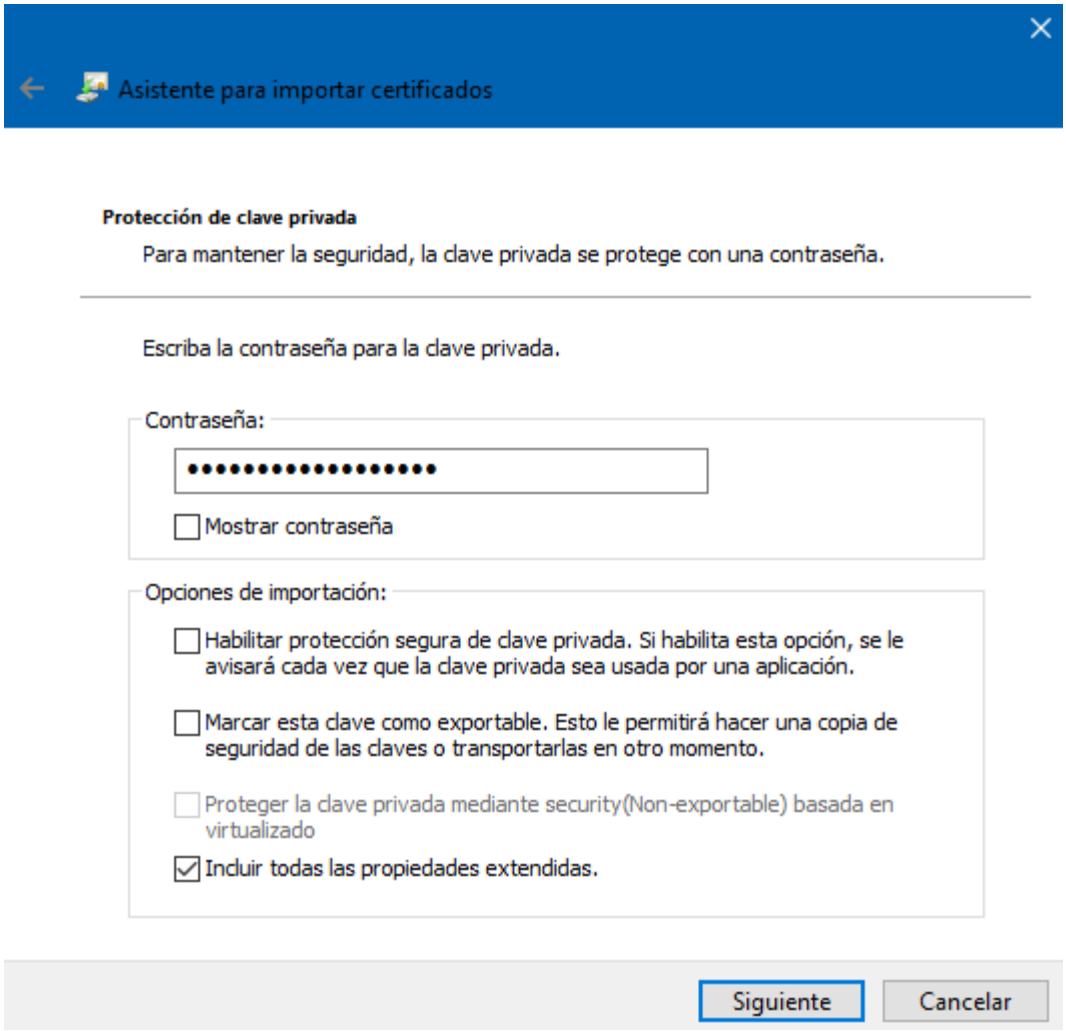


Figura: 150 Verificación de contraseña del servidor.

1.2.5 Se mantiene habilitada la opción que permite al sistema ubicar automáticamente el certificado en el almacén correspondiente, de acuerdo con su tipo.

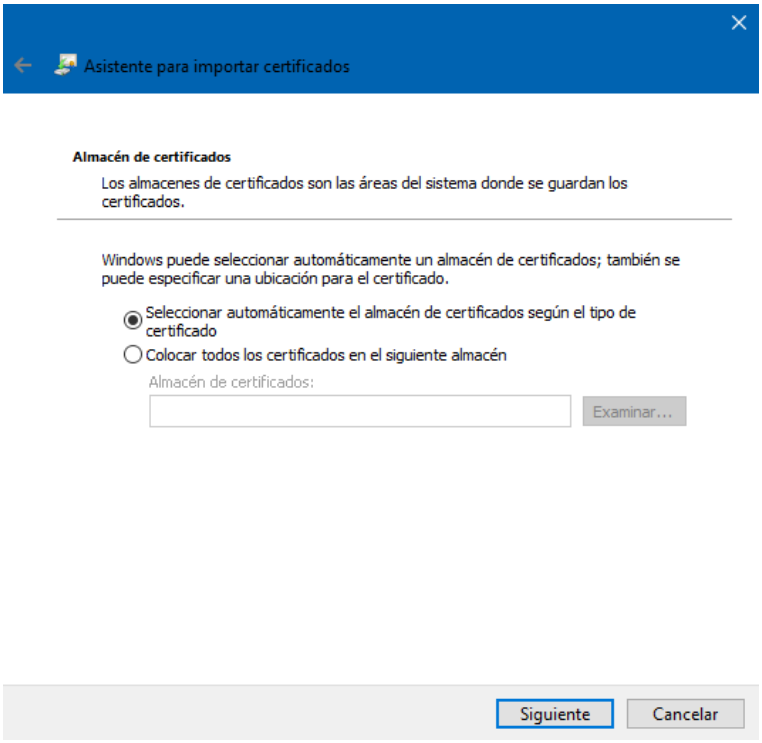


Figura: 151 Selección automática del almacén donde se instalará el certificado.

1.2.6 Una vez instalado el certificado, se accede a la consola de administración de EJBCA y dentro del apartado funciones del sistema se ingresa en la opción roles y reglas de acceso.

Figura: 152 Sección roles y reglas de acceso.

1.2.7 Desde allí, se selecciona el rol de superadministrador y se procede a agregar el usuario previamente creado como miembro del rol. La configuración se define para que la autenticación se realice mediante la coincidencia de los nombres completos contenidos en el certificado con los datos registrados en el sistema. Finalmente, se guardan los cambios.

Figura: 153 Agregando el usuario al grupo de miembros de usuarios Superadministradores.

2. Integración de la nueva autoridad certificadora (CA)

2.1 Incorporación de la CA al truststore de confianza de Wildfly

2.1.1 Desde la terminal del servidor donde se encuentra implementado el sistema de firma electrónica, se navega hasta la carpeta correspondiente a EJBCA.

```
root@192:/home/ejbca# cd /opt/ejbca_ce_9_1_1/
```

Figura: 154 Ubicación de EJBCA.

2.1.2 A continuación, se ejecuta el siguiente comando, que incorpora la nueva CA al archivo truststore.

```
root@192:/opt/ejbca_ce_9_1_1# ant -Dca.name="UTN_FICA_IBARRA_ACS" javatruststore
```

```
ejbca:javatruststore:
    [input] skipping input as property ca.name has already been set.
     [echo] Getting root certificate in DER format...
     [echo] ca getcacert "UTN_FICA_IBARRA_ACS" /tmp/rootca.der -der
     [echo] Adding to or creating keystore: /opt/ejbca_ce_9_1_1/p12/truststore.p12

ejbca:javatruststore-removeold:
     [exec] [Almacenando /opt/ejbca_ce_9_1_1/p12/truststore.p12]
     [exec] Se ha agregado el certificado al almacén de claves
     [exec] [Almacenando /opt/ejbca_ce_9_1_1/p12/truststore.p12]
   [delete] Deleting: /tmp/rootca.der

customejbca.message:
  [taskdef] Could not load definitions from resource org/jacoco/ant/antlib.xml. It could not be found.

set-paths-jboss7:

set-paths:

jee:deploytruststore:
     [copy] Copying 1 file to /opt/wildfly/standalone/configuration/keystore

BUILD SUCCESSFUL
Total time: 4 seconds
```

Figura: 155 Comando para incorporar la nueva CA.

2.1.3 Una vez incorporada la nueva autoridad certificadora en el truststore, se asignan nuevamente los permisos de ejecución al usuario wildfly mediante los comandos correspondientes.

```
root@192:/opt/ejbca_ce_9_1_1# chown -R wildfly:wildfly /opt/wildfly/standalone/configuration/keystore/
root@192:/opt/ejbca_ce_9_1_1# chmod 600 /opt/wildfly/standalone/configuration/keystore/*.p12
```

Figura: 156 Comando para asignar permisos al usuario wildlfy.

2.1.4 Posteriormente, se procede a reiniciar el servidor de aplicaciones Wildfly, de manera que los cambios aplicados en la configuración del truststore entren en vigor.

```
ejbca@192:/opt/ejbca_ce_9_1_1$ sudo systemctl restart wildfly
```

Figura: 157 Comando para reiniciar el servidor de aplicaciones Wildfly.

2.1.5 Finalmente, se ejecuta el siguiente comando para mostrar los certificados de confianza de truststore. En la salida obtenida, se revisa el apartado denominado “Acceptable client certificate CA names”, donde debe constar la nueva Autoridad Certificadora previamente integrada, confirmando así su correcta incorporación al entorno de confianza del sistema.

```
ejbca@192:/opt/ejbca_ce_9_1_1$ openssl s_client -connect 192.168.1.48:8443 -showcerts
```

```
Acceptable client certificate CA names
CN=UTNManagementCA, O=UTN, C=EC
C=ECuador, O=Facultad de Ingeniería en Ciencias Aplicadas(FICA), CN=Universidad Técnica del Norte IBARRA
```

Figura: 158 Comando para revisar contenido del archivo truststore.

3. Configuración de rol autoridad de registro

3.1 Emisión del certificado digital de la autoridad de registro

Con el fin de habilitar la autenticación y posterior asignación de privilegios de gestión a la autoridad de registro (RA), se procede a la emisión de su certificado digital siguiendo los pasos que se detallan a continuación:

3.1.1 Cerramos y volvemos a acceder a la consola de administración, cuando el navegador nos pregunte que certificado usar, seleccionamos el recién instalado.

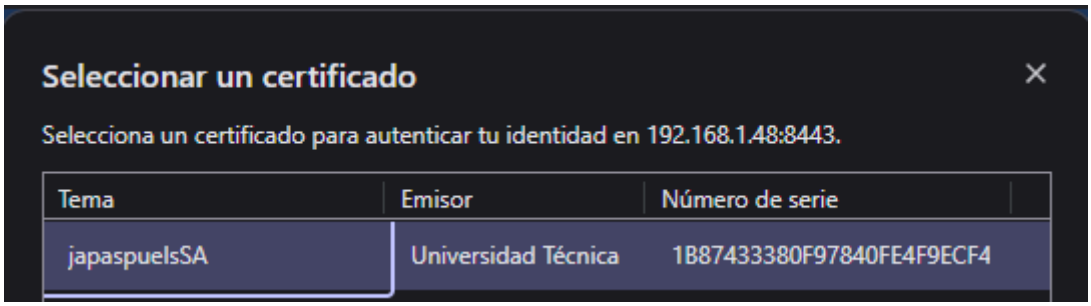


Figura: 159 Autenticación superadministrador.

Figura: 160 Verificación de autenticación.

3.1.2 Nos dirigimos a la opción de roles y reglas de acceso, y eliminamos el rol de acceso público.

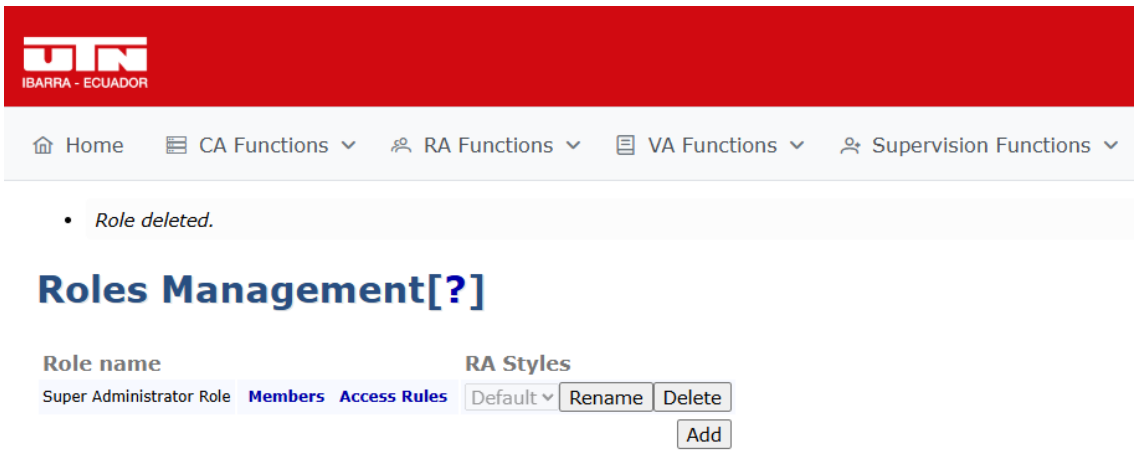


Figura: 161 Eliminación rol de acceso público.

3.1.3 Desde la consola de administración de la RA, se accede a la opción "Realizar nueva solicitud"

3.1.4 Se selecciona el perfil de certificado correspondiente a la autoridad de registro, previamente configurado bajo la denominación UTN_FICA_EFAR.

3.1.5 Se indica que el par de claves requerido será generado directamente por la autoridad certificadora UTN (CA).

3.1.6 Se completa el formulario de la solicitud, proporcionando los datos requeridos, incluyendo un usuario y contraseña de acceso asociados al certificado.

3.1.7 Finalmente, se procede a descargar el certificado digital emitido, el cual servirá como credencial para la autenticación de la Autoridad de Registro dentro del sistema de firma electrónica.

3.2 Configuración del rol de autoridad de registro y reglas de acceso.

3.2.1 Se procede a instalar el certificado digital de la autoridad de registro siguiendo el mismo procedimiento aplicado previamente para el certificado de superadministrador.

3.2.2 En la sección funciones del sistema, se accede a la opción roles y reglas de acceso, donde se crea un nuevo rol bajo la denominación autoridad registro rol.

Figura: 162 Creación autoridad registro role.

3.2.3 A continuación, en la opción miembros del rol se incorpora al usuario generado anteriormente como integrante de este nuevo rol.

Figura: 163 Incorporación de usuario al grupo de miembros del rol autoridad registro.

3.2.4 Posteriormente, en la administración de roles, se configura las reglas de acceso del rol autoridad registro, seleccionando como base la plantilla administradores RA, lo que le otorga las capacidades administrativas correspondientes. Además, se establece explícitamente que perfiles de entidades finales pueden ser gestionados por este rol.

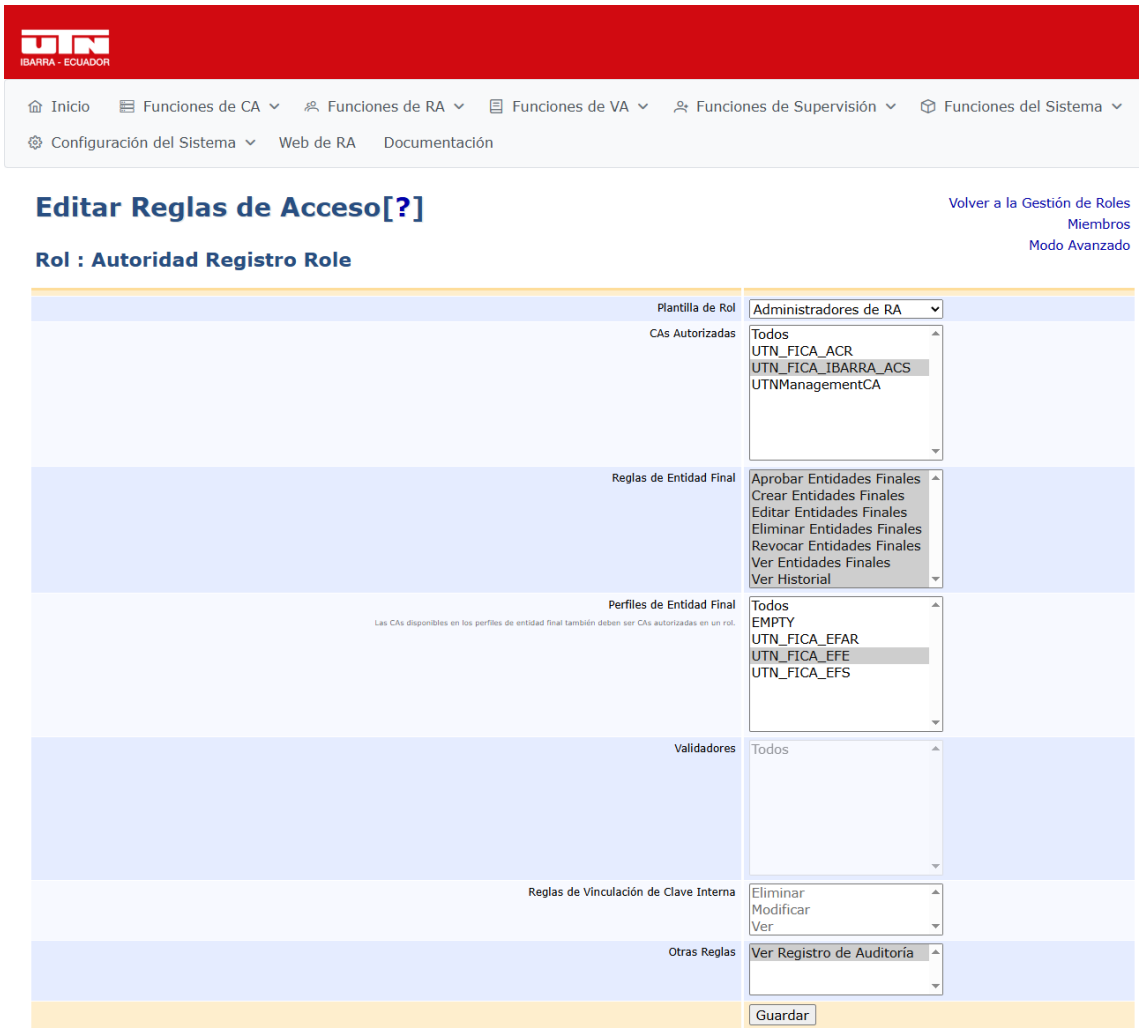


Figura: 164 Configuración de reglas de acceso para el rol autoridad registro.

4. Configuración del rol estudiante

4.1 Creación del rol y definición de reglas de acceso

4.1.1 Desde la sección funciones del sistema, en la opción roles y reglas de acceso, se crea un nuevo rol denominado estudiante rol.

Figura: 165 Creación estudiante role.

4.1.2 Se definen los miembros de este rol de forma que el acceso pueda realizarse de manera abierta mediante el protocolo HTTPS, permitiendo la autenticación de cualquier estudiante con credenciales válidas.

Figura: 166 Configuración de miembros para el rol estudiante.

4.1.3 A nivel de reglas de acceso, se limita el alcance de este rol únicamente a las funciones de solicitar un nuevo certificado y descargarlo. Para ello, se accede al modo avanzado de edición de reglas, a fin de aplicar estas restricciones de forma precisa.


Inicio
Funciones de CA
Funciones de RA
Funciones de VA
Funciones de Supervisión
Funciones del Sistema
Configuración del Sistema
Web de RA
Documentación
Editar Reglas de Acceso[?]
Volver a la Gestión de Roles
Miembros
Modo Básico
Resumen
Rol : Estudiante Role
Reglas de Acceso Basadas en Roles
Reglas de Acceso Regulares
Reglas de Acceso de CA
Reglas de Acceso del Validador
Reglas de Acceso al Perfil de Entidad Final
Reglas de Acceso a Crypto Token
Reglas de Acceso a la Fuente de Datos del Usuario
Reglas de Vinculación de Clave Interna
Reglas del Registro de Auditoría

Figura: 167 Configuración reglas de acceso del rol estudiante.

5. Creación del perfil de aprobación para estudiantes.

Con el fin de garantizar un control riguroso en la emisión de certificados digitales a los estudiantes, se establece un proceso de aprobación intermedio. De esta manera, cada solicitud generada debe ser válida por una autoridad de registro antes de su emisión definitiva.

5.1 Desde la sección funciones de supervisión, se accede a la opción perfiles de aprobación y se crea un nuevo perfil denominado UTN_FICA_PAE.

Figura: 168 Creación perfil aprobación estudiante.

5.2 En la configuración del perfil, se establece como tipo de perfil aprobación particionada, lo que permite dividir el proceso de validación en pasos claramente definidos.

5.3 Se configura el tiempo de expiración de la solicitud en 7 días, garantizando que las solicitudes inactivas no permanezcan indefinidamente en el sistema.

5.4 En los pasos de aprobación, se completan los parámetros necesarios y se asigna la revisión al rol autoridad registro, con el objetivo de que únicamente esta instancia valide y apruebe las solicitudes de los estudiantes.

5.5 Se agrega un sistema de notificación por correo electrónico para informar al estudiante sobre el estado de su solicitud cada vez que se produzca un cambio, ya sea por aprobación, rechazo o expiración.

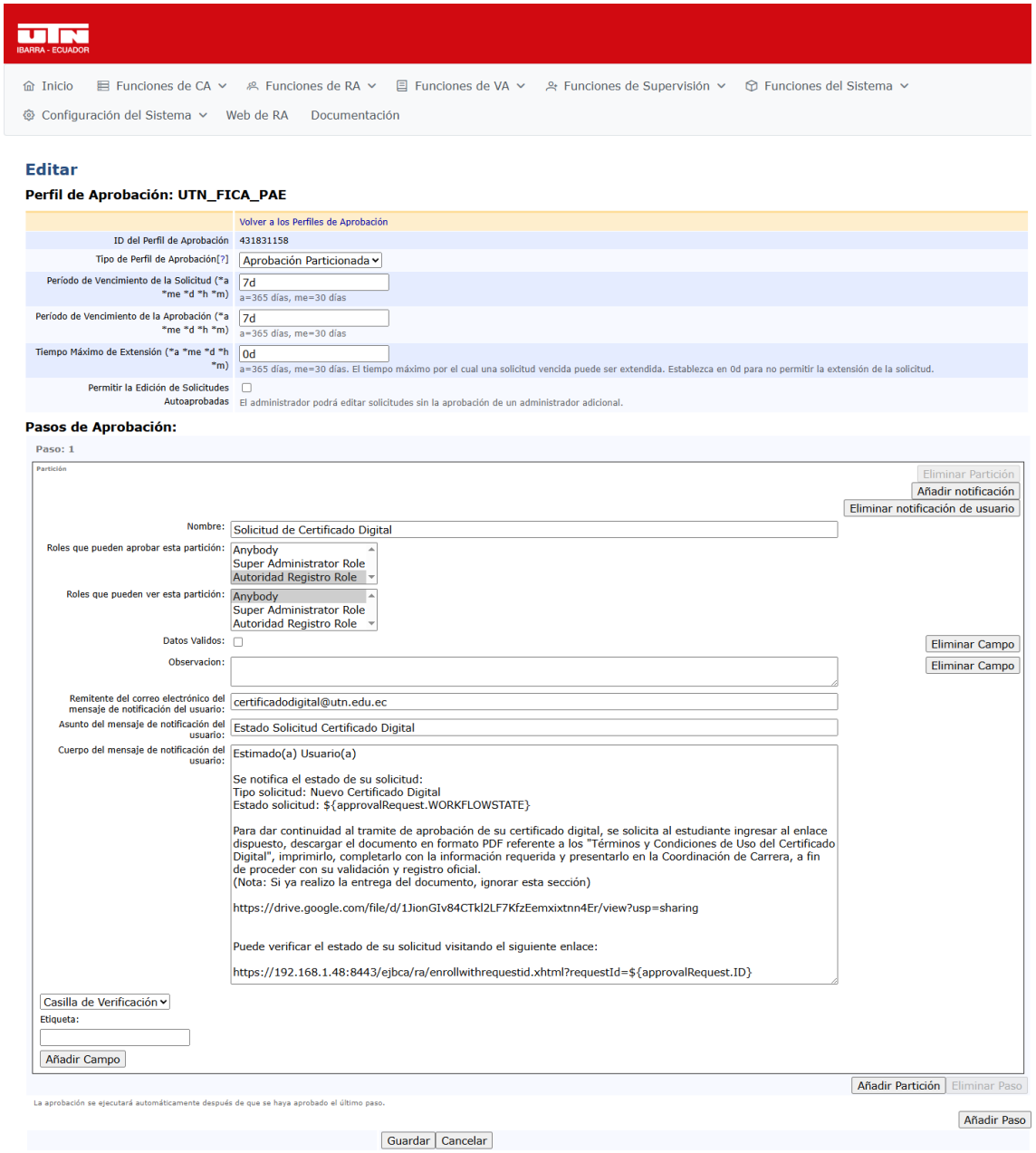


Figura: 169 Configuración perfil aprobación estudiante.

5.6 Finalmente, se vincula este perfil de aprobación con el perfil de certificado de estudiante UTN_FICA_EFE_PERFIL.

5.6.1 Para ello, desde las funciones de CA, se edita el perfil de certificado UTN_FICA_EFE_PERFIL.

5.6.2 En la sección configuración de aprobación, dentro del campo agregar/editar entidad final, se selecciona el perfil de aprobación UTN_FICA_PAE, quedando así integrado en el flujo de emisión de certificados estudiantiles.

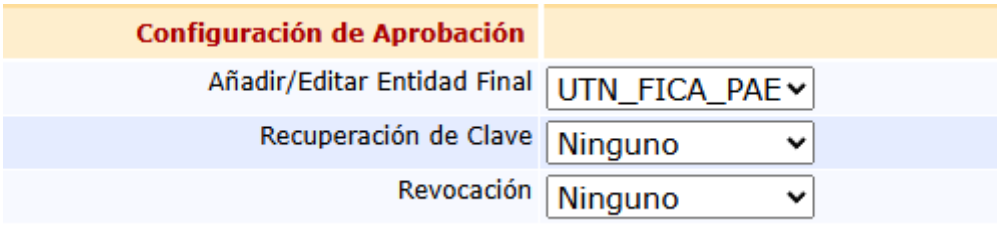


Figura: 170 Asignación del perfil aprobación estudiante al perfil de certificado estudiante.

3.1.6.7 Capacitación de usuarios

Con el propósito de facilitar la capacitación de los estudiantes en el uso del sistema de firma electrónica, se han dispuesto recursos de apoyo que permiten la correcta obtención de un certificado digital sin requerir experiencia previa en el uso de la plataforma. Para ello, se elaboró un video tutorial y un manual de usuario en formato PDF, desarrollados conforme a los procedimientos definidos en el presente proyecto.

El manual describe de manera detallada las actividades que el estudiante debe realizar para solicitar y obtener un certificado digital (**Anexo E**). Adicionalmente, se explica el procedimiento para la aplicación de la firma electrónica sobre documentos digitales mediante el uso del certificado emitido. El video correspondiente al manual de usuario se encuentra disponible en el siguiente enlace:

https://www.youtube.com/watch?v=cuXpfrZ7b0o

3.1.6.8 Operación y pruebas del servicio

El servicio de firma electrónica se encuentra actualmente operativo en el laboratorio de administración de la Facultad de Ingeniería en Ciencias Aplicadas (FICA), bajo la responsabilidad de la Ing. Ludmila Starodub, jefa de Laboratorio de Sistemas FICA. Dicho servicio se ha desplegado sobre la infraestructura tecnológica de la Facultad y se encuentra disponible para su utilización por parte de la comunidad universitaria a través de la red interna institucional (eduroam) de la Universidad Técnica del Norte (UTN), garantizando un entorno controlado para la ejecución de pruebas iniciales.

En una primera fase de validación del sistema, el servicio fue sometido a pruebas con estudiantes de nuevo ingreso pertenecientes a la facultad FICA de la UTN, considerando una muestra total de 237 estudiantes. Durante esta etapa, los usuarios

realizaron únicamente el proceso de solicitud de certificados digitales, que incluyó el acceso al sistema y el registro de la información requerida para la emisión del certificado. Esta fase tuvo como objetivo evaluar el comportamiento del sistema ante múltiples solicitudes concurrentes, evidenciando un funcionamiento estable, sin presentarse problemas de saturación, errores en el registro de solicitudes ni inconvenientes relacionados con el rendimiento de la plataforma.

3.2 Análisis y clasificación de amenazas en el servicio implementado

En esta sección se identifica y analizan las amenazas más relevantes en la implementación realizada del servicio de firma electrónica basado en infraestructura de clave pública (PKI) en la FICA-UTN, tomando como referencia la Tabla 1. Se identifican principalmente en aquellas que afectan directamente la autenticidad del firmante, la protección de las claves privadas y la validez de los certificados digitales. Si bien la seguridad de la Autoridad Certificadora y la solidez de los algoritmos criptográficos constituyen elementos fundamentales dentro del modelo PKI, el análisis contextualizado al entorno académico evidencia que riesgos como el robo de claves privadas, la ingeniería social, la pérdida o compromiso de dispositivos de firma y las deficiencias en los mecanismos de revocación de certificados presentan un mayor nivel de criticidad para la operación institucional. Estas amenazas pueden derivar en suplantación de identidad, emisión de firmas fraudulentas y pérdida de validez jurídica de los documentos electrónicos. Por consiguiente, la implementación realizada prioriza controles técnicos adecuados, mecanismos de gestión segura de credenciales y estrategias de concienciación dirigidas a los usuarios, con el propósito de fortalecer la confianza, integridad y sostenibilidad del servicio.

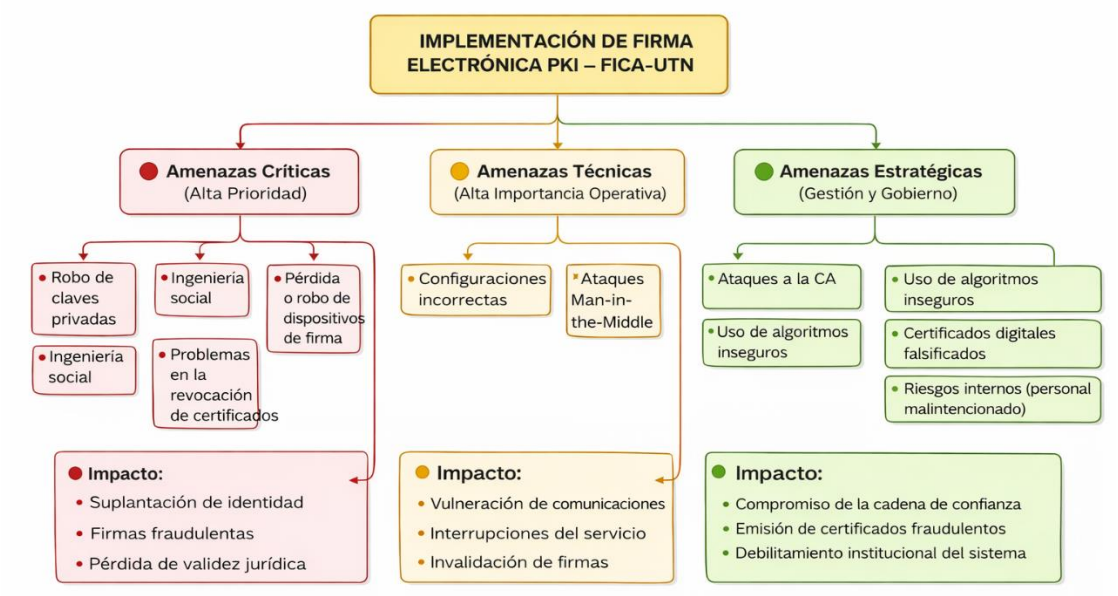


Figura: 171 Mapa conceptual de clasificación de amenazas en la implementación de PKI.

3.3 Investigación de certificación

3.3.1 Investigación de los requisitos técnicos y legales de certificación.

En esta sección se llevó a cabo un análisis de los requisitos técnicos y legales establecidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), a través de la información disponible en su portal web institucional, accesible mediante el enlace https://www.arcotel.gob.ec/.

Dentro de dicho portal se identificó la sección denominada “Requisitos: Entidades de Certificación”, en la cual se detallan los lineamientos necesarios para obtener la certificación correspondiente, conformados por un total de doce literales que contemplan tanto aspectos técnicos (**Anexo B**) como legales (**Anexo C**).

Adicionalmente, se efectuó una investigación complementaria sobre procesos de certificación similares, identificándose en el repositorio institucional de la Universidad de las Fuerzas Armadas ESPE, un proyecto de titulación que documenta una reunión, con personal administrativo de la ARCOTEL.

Como resultado de este acercamiento, se obtuvo una explicación más precisa y detallada de cada uno de los requisitos técnicos exigidos para el proceso de certificación [22] (**Anexo B**).

3.4 Análisis de certificación

Una vez concluida la investigación relacionada con los requisitos de certificación, se presenta a continuación un análisis que sintetiza los principales aspectos identificados, así como las conclusiones generales derivadas de la revisión de los requisitos legales y técnicos.

3.4.1 Análisis de los requisitos legales

En relación con la documentación de carácter legal que debe ser presentada, se determinó que su elaboración no representa un nivel significativo de complejidad. No obstante, varios de los requisitos establecidos excluyen explícitamente a las instituciones públicas, condición que aplica para la Universidad Técnica del Norte. Entre los requisitos que no aplican a este tipo de institución se encuentran los siguientes:

- **Copia certificada e inscrita en el Registro Mercantil del nombramiento del representante legal**: Este requisito no es aplicable a la UTN, al tratarse de una institución pública.
- **Copia certificada e inscrita en el Registro Mercantil de la escritura de constitución de la empresa o compañía y sus respectivas reformas**: No aplica en el caso de la UTN; sin embargo, debe presentarse un decreto oficial de creación u otro documento emitido por el Estado ecuatoriano que respalde su constitución como universidad pública.
- **Certificado de cumplimiento de obligaciones emitido por la Superintendencia de Compañías o de Bancos y Seguros**: Este requisito no aplica para las instituciones del Estado.
- **Documentación que demuestre la capacidad económica y financiera para la prestación del servicio de certificación**: En este caso, al depender de recursos públicos, la UTN debe acreditar su solvencia financiera mediante certificados emitidos por el Ministerio de Finanzas, en los cuales se evidencie la asignación presupuestaria correspondiente. Dichos recursos deben cubrir los costos asociados al proceso de acreditación, tales como el valor de la certificación, la garantía de acreditación, el recurso humano y la adquisición de la infraestructura tecnológica necesaria para la implementación del servicio de firma electrónica.

3.4.2 Análisis de los requisitos técnicos

Tal como se indica en la descripción de los requisitos técnicos, la documentación solicitada constituye el conjunto mínimo exigido para iniciar el proceso de acreditación. A partir de este análisis, se infiere que el servicio de firma electrónica actualmente implantado, como se ilustra en la **Figura 2**, requiere una arquitectura más robusta, acompañada de procedimientos de seguridad más estrictos y mecanismos que garanticen una alta disponibilidad del servicio.

Para asegurar la continuidad operativa y la disponibilidad del sistema, es necesario que ciertos componentes internos de la infraestructura PKI, como la Autoridad de Registro (RA) y la Autoridad de Validación (VA), se encuentren distribuidos en múltiples servidores. Este tipo de arquitectura, con capacidades avanzadas de escalabilidad y tolerancia a fallos, se encuentra disponible en la versión empresarial del software EJBCA. En contraste, la implementación actual, mostrada en la **Figura 2**, permite desplegar estos servicios en un único servidor, lo cual podría generar limitaciones operativas al extender el servicio a toda la comunidad universitaria. En virtud de lo expuesto, se plantea como una alternativa viable la adquisición de la versión empresarial del software utilizado para el servicio de firma electrónica.

3.4.3 Diferenciación entre robustez técnica y acreditación legal del servicio de firma electrónica

Tomando como base el análisis previo de los requisitos legales y técnicos, resulta necesario establecer una diferenciación conceptual entre un servicio de firma electrónica técnicamente robusto y un servicio legalmente acreditado como entidad certificadora. Si bien la infraestructura actual basada en EJBCA permite la emisión y validación de certificados digitales dentro del entorno institucional de la Universidad Técnica del Norte, su implementación responde principalmente a criterios de funcionalidad tecnológica y operación interna. En contraste, un escenario de acreditación formal implica no solo el fortalecimiento de la arquitectura tecnológica mediante mecanismos de alta disponibilidad, segregación de roles y controles de seguridad avanzados, sino también el cumplimiento estricto de obligaciones regulatorias, auditorías periódicas, responsabilidades legales y garantías financieras exigidas por el marco normativo nacional. Por tanto, la robustez técnica constituye una condición necesaria, pero no suficiente, para alcanzar el reconocimiento jurídico formal del servicio de certificación digital.

A continuación, se presenta una tabla que detalla las principales diferencias entre el estado actual del servicio y el escenario proyectado bajo un esquema de acreditación formal.

Aspecto	Estado actual – servicio técnicamente robusto	Escenario acreditado – servicio legalmente reconocido
Alcance del servicio	Servicio institucional interno orientado a la comunidad universitaria (estudiantes).	Servicio formal de certificación reconocido por el organismo regulador nacional, con validez jurídica plena ante terceros.
Validez legal	Validez funcional dentro del entorno institucional.	Validez jurídica nacional conforme a la normativa ecuatoriana de firma electrónica y certificación digital.
Reconocimiento externo	No reconocido por entidades externas al ámbito universitario.	Reconocido oficialmente por organismos públicos y privados a nivel nacional.
Obligaciones regulatorias	No está sujeto a auditorías externas obligatorias de acreditación como entidad certificadora.	Debe cumplir auditorías periódicas, controles regulatorios, políticas de certificación formalizadas y estándares técnicos exigidos por el ente de control.
Arquitectura tecnológica	Puede operar en un único servidor (Figura 10), con escalabilidad limitada.	Requiere arquitectura distribuida, alta disponibilidad, redundancia, segregación de roles (CA, RA, VA), y mayores controles de seguridad.
Nivel de seguridad exigido	Seguridad adecuada para entorno interno; depende de buenas prácticas institucionales.	Seguridad certificada, controles estrictos, posible uso de HSM, cumplimiento de estándares formales.

Costos de implementación	Costos moderados: infraestructura básica, recursos humanos institucionales y software libre.	Costos elevados: tasas de acreditación, garantía económica, auditorías, infraestructura redundante, versión empresarial del software.
Costos de mantenimiento	Mantenimiento técnico interno gestionado por administración de laboratorios FICA.	Mantenimiento técnico, cumplimiento normativo continuo, auditorías periódicas, renovación de acreditación.
Responsabilidad legal	Responsabilidad limitada al ámbito institucional.	Alta responsabilidad legal frente al Estado y terceros por la emisión de certificados digitales.
Tipo de usuario impactado	Principalmente comunidad universitaria interna.	Comunidad universitaria, potencialmente terceros externos que confíen en la entidad certificadora acreditada.
Nivel de riesgo institucional	Riesgo técnico: caídas del sistema, limitaciones operativas.	Riesgo técnico, riesgo legal y reputacional ante incumplimiento normativo.
Continuidad del servicio	Dependiente de infraestructura actual.	Debe garantizar alta disponibilidad y continuidad operativa formalmente documentada.

Tabla 5 Comparación entre el servicio de firma electrónica técnicamente robusto y el escenario de acreditación legal.

3.4.4 Análisis de presupuesto para la certificación legal del servicio

Como resultado de la investigación realizada sobre los requisitos y el proceso de certificación, se presenta el siguiente análisis presupuestario, cuyo objetivo es estimar la inversión total necesaria para que el servicio de firma electrónica pueda operar de manera legal, formalmente constituida y debidamente acreditada.

En primer término, se considera el costo correspondiente al proceso de acreditación, el cual permite obtener la calificación como Entidad de Certificación de la Información. Este valor asciende a USD 22.000. Adicionalmente, es obligatorio disponer

de un monto destinado a la garantía de acreditación, cuyo propósito es cubrir eventuales daños o perjuicios que pudieran generarse a los usuarios del servicio de firma electrónica; dicho valor se establece en USD 400.000.

Por otra parte, dado que se plantea la alternativa de implementar la versión empresarial del software PKI, se identifican dos costos asociados a esta solución. El primero corresponde al paquete completo del software EJBCA Enterprise, cuyo valor estimado es de USD 20.000, el cual incluye, además, un módulo de seguridad de hardware (HSM). El segundo corresponde a la licencia o soporte empresarial, con un costo de USD 24.000, cuya vigencia es anual. En consecuencia, esta licencia debe renovarse cada año, manteniendo el mismo valor de adquisición, es decir, USD 24.000 por período de renovación.

Especificación	**Valor**	**Renovación**
Acreditación	$ 22,000	No
Garantía de acreditación	$ 400,000	No
Paquete software completo	$ 20,000	No
EJBCA y HSM (opcional)	$ 20,000	No
Licencia EJBCA (opcional)	$ 24.000	Si
Total	$ 466,000	

Tabla 6 Presupuesto de certificación.

El monto total estimado de inversión correspondiente al primer año de operación del servicio asciende a USD 466.000, tal como se especifica en la **Tabla 5**. Cabe señalar que este valor constituye una estimación, ya que no contempla posibles costos adicionales asociados a la adquisición de infraestructura tecnológica ni a la contratación de recursos humanos especializados.

CAPÍTULO IV

RESULTADOS Y ANÁLISIS

En el presente capítulo se tabulan y discuten los resultados obtenidos tras la aplicación de la metodología de evaluación definida, basada en los principios del Cuestionario de Usabilidad de Sistemas Informáticos (CSUQ). Los datos recopilados a través de la encuesta de satisfacción han sido procesados y analizados estadísticamente para determinar la viabilidad, usabilidad y aceptación del servicio de firma electrónica implementado en la FICA-UTN. El análisis se centra en contrastar los resultados cuantitativos con los objetivos planteados, permitiendo emitir juicios de valor y triangular la información.

4.1 Metodología de evaluación

Para validar el funcionamiento y la aceptación del servicio de firma electrónica basado en PKI, se aplicó una técnica de investigación cuantitativa mediante una encuesta estructurada.

- **Fundamentación metodológica:** La estructura de la encuesta, que utiliza la escala de Likert y mide dimensiones clave como la calidad de la interfaz, la calidad de la información y la satisfacción general, se alinea con los principios establecidos por la metodología de evaluación CSUQ. Si bien el instrumento no es el CSUQ estándar, está diseñado para evaluar la Usabilidad Percibida y la Satisfacción del Usuario (SUS), métricas fundamentales en la evaluación de sistemas.
- **Población y muestra:** La población estuvo conformada por todos los estudiantes matriculados en primer semestre de la Facultad de Ingeniería en Ciencias Aplicadas (FICA-UTN) durante el período académico analizado, con un total de N = 237. La evaluación se desarrolló mediante un censo por curso, aplicando el sistema de firma electrónica y la encuesta de manera presencial, paralelo por paralelo, a los estudiantes asistentes en cada jornada académica. Como resultado, se obtuvo una muestra efectiva de 200 estudiantes. Este procedimiento no correspondió a un muestreo voluntario ni probabilístico, sino a una aplicación estructurada en el entorno académico formal, lo que garantiza una adecuada representatividad del grupo evaluado.

- **Instrumento:** El cuestionario consta de 15 ítems que miden la experiencia de usuario (UX) en las etapas críticas del servicio. Se utilizó una escala de Likert de 5 puntos para la medición de variables, lo que facilitó la cuantificación de percepciones cualitativas.

4.2 Resultados y discusión

A continuación, se presenta el análisis de los datos agrupados por dimensiones de calidad, enfocándose en la interpretación crítica y la triangulación de la información para dar respuesta a los objetivos específicos.

4.2.1 Dimensión de calidad: Usabilidad y diseño de interfaz (Quality of Interface)

Esta dimensión evalúa la barrera de entrada al sistema, la claridad de su interfaz gráfica y la facilidad para interactuar con sus elementos (Preguntas 1, 2 y 13).

Indicador (Escala Likert)	**Frecuencia (Acceso, P1)**	**Porcentaje (Acceso)**	**Frecuencia (Interfaz, P2)**	**Porcentaje (Interfaz)**
Muy fácil / Muy clara	58	29.0%	45	22.5%
Fácil / Clara	77	38.5%	89	44.5%
Regular	57	28.5%	52	26.0%
Difícil / Poco clara	7	3.5%	7	3.5%
Muy difícil / Confusa	1	0.5%	7	3.5%
Total	200	100%	200	100%

Tabla 7 Percepción de la facilidad de acceso y claridad de la interfaz

Los resultados de la **Tabla 6** son consistentes con una alta usabilidad percibida. El 67.5% de los estudiantes percibe el acceso como "Fácil" o "Muy fácil" y el 67% percibe la interfaz como "Clara" o "Muy clara". Este alto grado de usabilidad valida el diseño frontend y la baja curva de aprendizaje del sistema, un factor clave en la adopción de nuevas tecnologías según la metodología CSUQ.

Sin embargo, el 28.5% de los usuarios que calificaron la experiencia como "Regular" señala un área de mejora específica. Al triangular esta calificación con los datos

de la Pregunta 13 (Mejoras Visuales), los estudiantes mencionaron la "Distribución de los elementos en pantalla" y la "Claridad y tamaño de los botones" como aspectos a optimizar. Esto sugiere que, mientras la funcionalidad es intuitiva, la experiencia estética y ergonómica debe refinarse, especialmente para garantizar la accesibilidad a diversos dispositivos, como lo exige la normativa vigente en gestión de servicios de TI (ITIL v4).

4.2.2 Dimensión de calidad: eficiencia y fiabilidad (System Efficiency)

Esta dimensión evalúa el rendimiento técnico del sistema, incluyendo la velocidad de carga (P3), la respuesta a la solicitud (P6), la recepción de notificaciones (P12) y el éxito en la descarga del certificado (P10).

Indicador	Siempre rápido / Sin problemas	Generalmente rápido / Pequeños problemas	Regular / Errores o lento
Velocidad de carga (P3)	32.5%	56.0%	11.5%
Éxito en la descarga (P10)	58.0%	22.5%	6.0%
Notificaciones (P12)	62.5%	22.0%	15.5%

Tabla 8 Desempeño técnico, notificaciones y descarga exitosa.

La fiabilidad del sistema es alta. El 88.5% de los usuarios calificó la velocidad de carga como "Siempre" o "Generalmente rápido" (P3), lo que confirma que la infraestructura de backend (servidor Wildfly) está configurada adecuadamente para el volumen de usuarios.

En cuanto a la funcionalidad crítica, el 80.5% de los estudiantes reportó éxito en la descarga del certificado (.p12) (P10). El 6% de fallos en la descarga, aunque minoritario, es un indicador de que existen bugs específicos. Estos errores, triangulados con los comentarios, sugieren problemas de encoding o manejo de caracteres especiales en la capa de autenticación y generación de claves. La resolución de este 6% es vital para lograr la máxima fiabilidad del sistema, que es un requisito de seguridad crítica en una PKI.

Además, el 84.5% de recepción oportuna de notificaciones (P12) demuestra la transparencia del proceso, lo cual mejora la experiencia del usuario al reducir la ansiedad por el estado del trámite.

4.2.3 Dimensión: satisfacción global y adopción (Overall Satisfaction - CSUQ)

Esta dimensión integra la satisfacción con el proceso completo y mide la intención de recomendación, un indicador similar al Net Promoter Score (NPS), fundamental en la métrica CSUQ.

Indicador	Definitivamente sí / Muy satisfecho	Probablemente sí / Satisfecho	No estoy seguro / Neutral	Probablemente no / Insatisfecho
Recomendación (P15)	45.0%	42.0%	11.0%	2.0%
Satisfacción (P7, Solicitud)	40.0%	42.0%	16.0%	2.0%
Satisfacción (P11, Descarga)	36.5%	39.5%	19.5%	4.5%

Tabla 9 Satisfacción global del proceso y probabilidad de recomendación

La satisfacción global es sumamente alta, con un 82% de usuarios "Satisfechos" o "Muy Satisfechos" con la solicitud (P7) y un 76% con la descarga (P11). El indicador clave de adopción, la recomendación (P15), alcanza un impresionante 87% ("Definitivamente sí" y "Probablemente sí").

Este resultado aprueba la hipótesis central de la investigación: la implementación del servicio de firma electrónica no solo cumple con los requisitos técnicos de seguridad (PKI), sino que mejora la experiencia del usuario en la gestión documental estudiantil en comparación con la metodología manual previa.

El hecho de que el sistema se considere ampliamente recomendable lo posiciona como una solución sostenible y escalable dentro de la estrategia de transformación digital de la FICA-UTN, cumpliendo con las expectativas de valor definidas en el contexto de ITIL v4.

4.3 Análisis descriptivo por ítem

En esta sección se presenta el desglose pormenorizado de los resultados obtenidos para cada una de las interrogantes planteadas en el instrumento de evaluación. Se incluye la representación gráfica de las frecuencias y su respectiva interpretación estadística y cualitativa.

4.3.1 Facilidad de acceso al sistema (Pregunta 1)

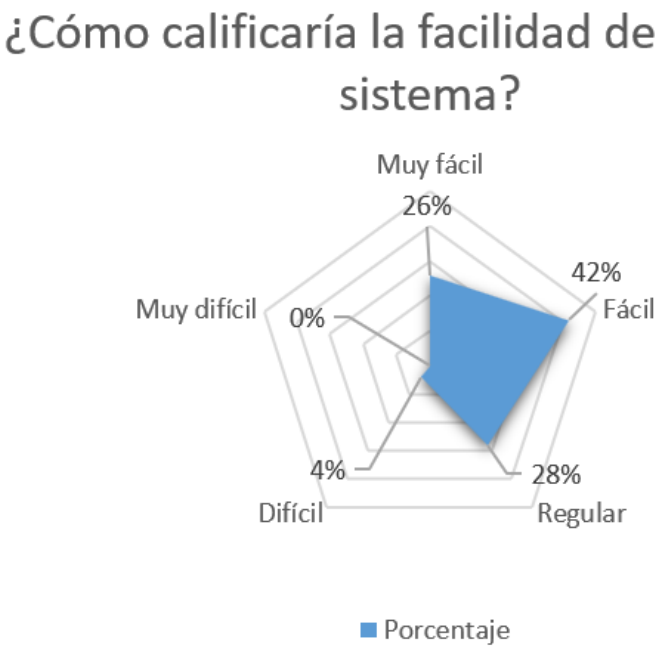


Figura: 172 Pregunta 1. ¿Cómo calificaría la facilidad de acceso al sistema?

Los resultados evidencian una recepción mayoritariamente positiva respecto al ingreso a la plataforma. El 68% de los encuestados calificó el acceso como "Fácil" (42%) o "Muy fácil" (26%), lo que indica que las barreras de entrada iniciales son mínimas. Sin embargo, un segmento representativo del 28% lo valoró como "Regular". Este grupo, sumado al 4% que experimentó dificultades, sugiere que factores externos como la conectividad o la falta de familiaridad con el entorno web institucional pudieron influir en la primera impresión del usuario.

4.3.2 Claridad de la interfaz gráfica (Pregunta 2)

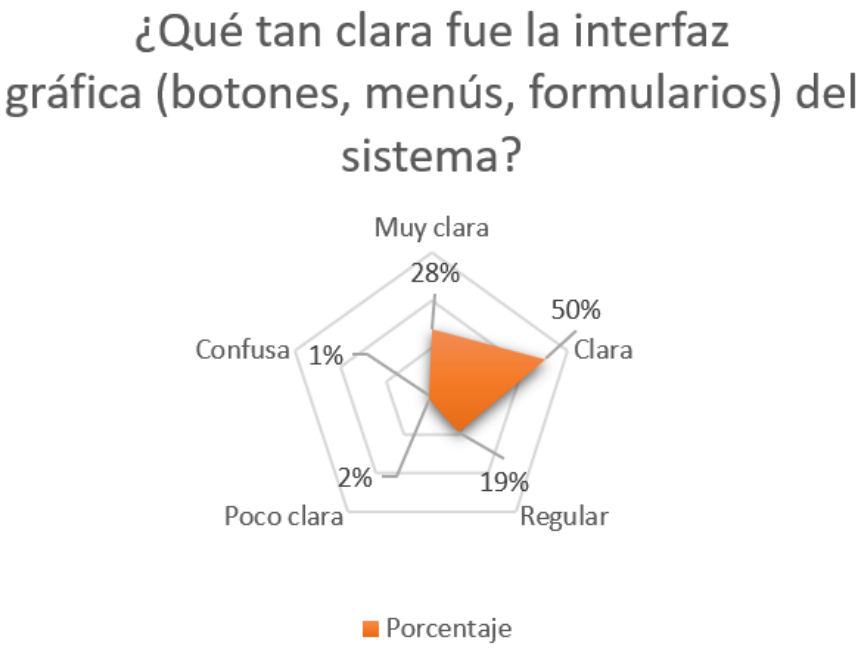


Figura: 173 Pregunta 2. ¿Qué tan clara fue la interfaz gráfica (botones, menús, formularios) del sistema?

La usabilidad visual del sistema obtuvo una valoración favorable. El 78% de la muestra considera que la disposición de elementos es "Clara" (50%) o "Muy clara" (28%), validando el diseño frontend orientado a la intuición del usuario. Solo un 3% percibió la interfaz como "poco clara" o "confusa", mientras que el 19% mantuvo una postura neutral ("regular"), lo que confirma que el diseño es funcional para la gran mayoría de la población estudiantil.

4.3.3 Velocidad de carga y rendimiento (Pregunta 3)

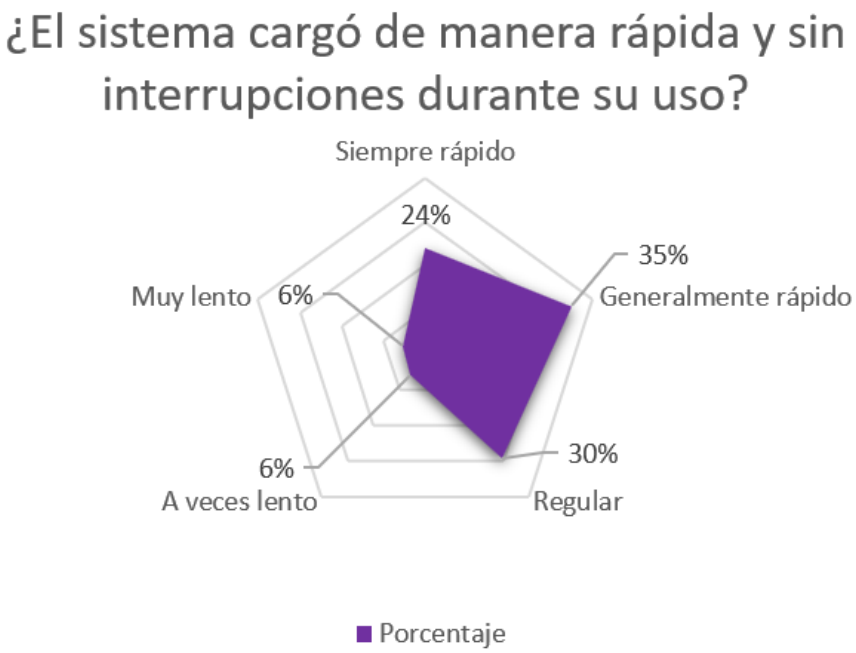


Figura: 174 Pregunta 3. ¿El sistema cargó de manera rápida y sin interrupciones durante su uso?

En términos de rendimiento, el 59% de los usuarios reportó que el sistema funcionó de manera "Siempre rápida" o "Generalmente rápida". Un grupo considerable del 29.5% calificó la velocidad como "Regular", y un 11.5% experimentó lentitud. Estos datos reflejan que, si bien el servidor Wildfly respondió adecuadamente para la mayoría, existen picos de latencia que se relacionan directamente con la conectividad lenta de la red eduroam institucional, que afectaron a cerca de un tercio de la muestra, identificándose como un punto clave para futuras optimizaciones de infraestructura.

4.3.4 Sencillez del llenado de solicitud (Pregunta 4)

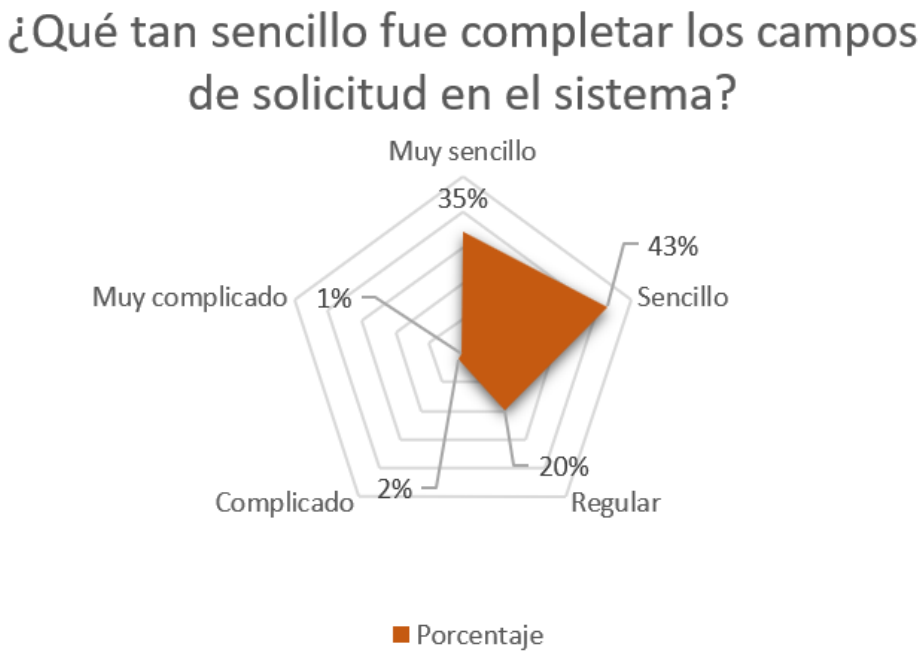


Figura: 175 Pregunta 4. ¿Qué tan sencillo fue completar los campos de solicitud en el sistema?

El proceso de ingreso de datos demostró ser altamente eficiente. Un contundente 77.5% lo describió como "Sencillo" o "Muy sencillo". La validación de campos y la estructura del formulario evitaron confusiones, dejando solo a un 2.5% con percepción de complicación. El 20% restante lo calificó como "Regular", lo que sugiere que el formulario cumple su función sin generar fricción significativa en el trámite.

4.3.5 Comprensión de reglas de contraseña (Pregunta 5)

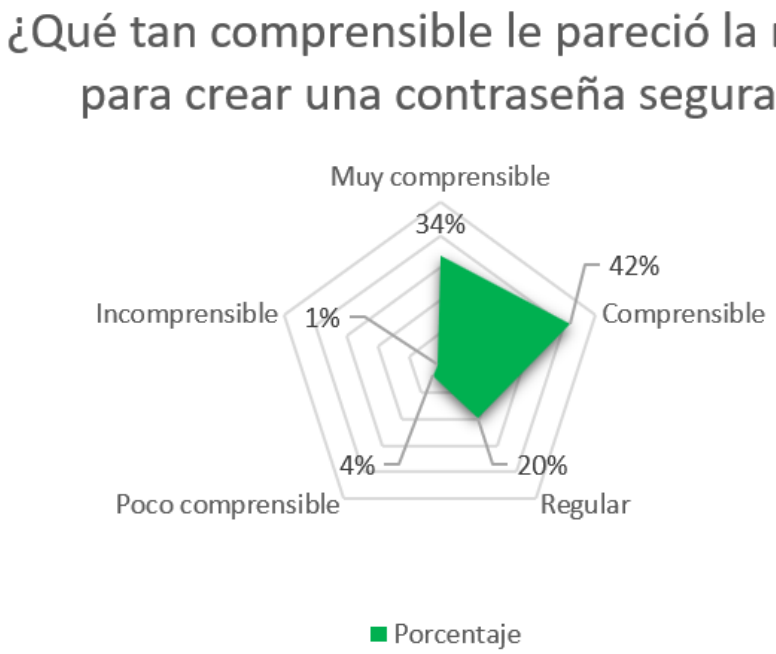


Figura: 176 Pregunta 5. ¿Qué tan comprensible le pareció la regla para crear una contraseña segura?

La comunicación de las políticas de seguridad (longitud, caracteres especiales) fue efectiva para el 76% de los participantes, quienes entendieron las reglas como "Comprensibles" o "Muy comprensibles". Dado que la seguridad es un pilar de la infraestructura PKI, este alto porcentaje es crucial. El 19.5% que lo consideró "Regular" podría beneficiarse de ayudas visuales en tiempo real (tooltips) más explícitas durante la creación de credenciales.

4.3.6 Respuesta del sistema a la confirmación (Pregunta 6)

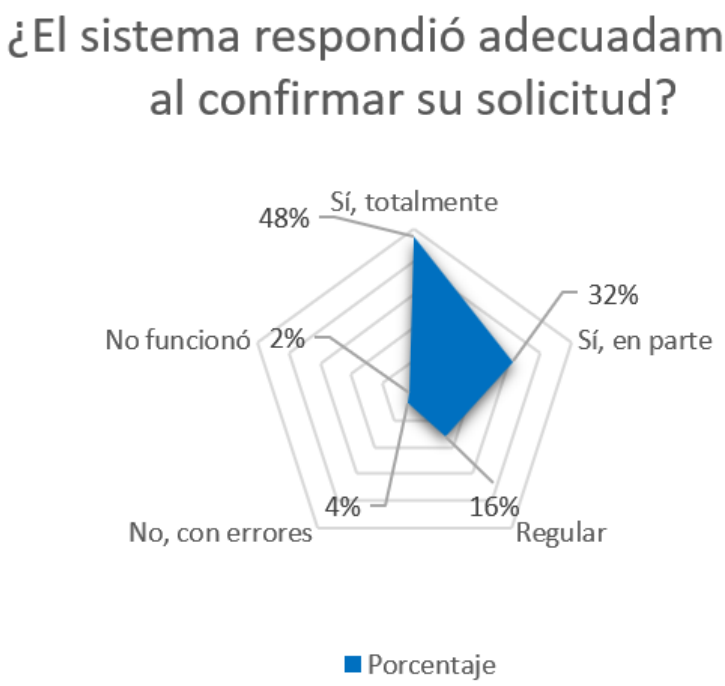


Figura: 177 Pregunta 6. ¿El sistema respondió adecuadamente al confirmar su solicitud?

La retroalimentación del sistema tras enviar el formulario fue exitosa para el 79% de los encuestados, sumando las respuestas "Sí, totalmente" y "Sí, en parte". Solo un 5% reportó errores o fallos funcionales ("No, con errores" o "No funcionó"). Al realizar un análisis sobre la problemática que presentaban los estudiantes inconformes con la confirmación de solicitud, se detectó que la problemática no era relacionada con el sistema implementado, sino por la lenta conectividad de la red Eduroam de la institución.

4.3.7 Satisfacción con el proceso de solicitud (Pregunta 7)

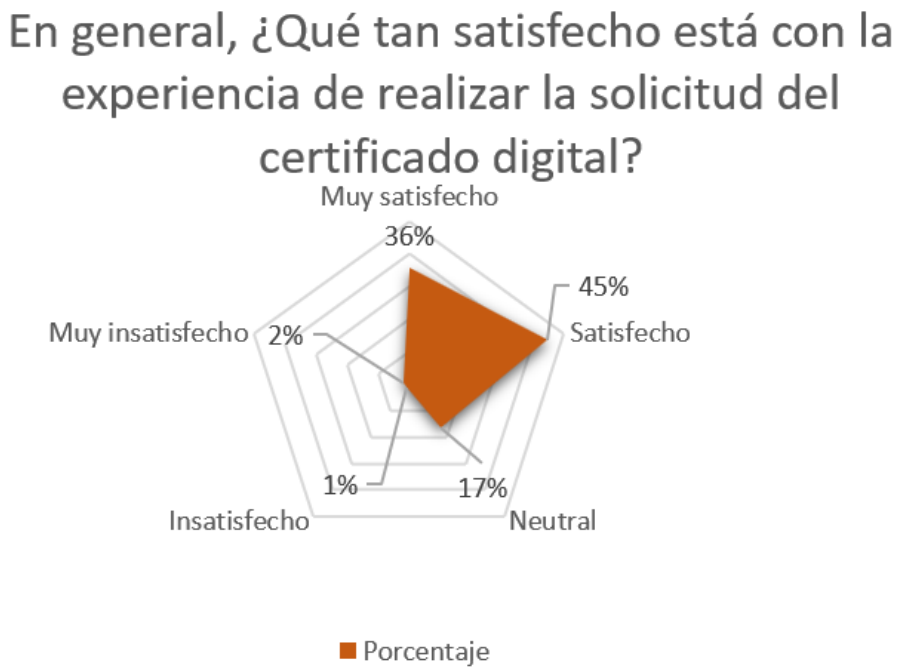


Figura: 178 Pregunta 7. ¿Qué tan satisfecho está con la experiencia de realizar la solicitud del certificado digital?

La satisfacción global con la primera fase del proceso es alta: el 80.5% de los estudiantes se declaró "satisfecho" o "muy satisfecho". Solo un 3% expresó insatisfacción. Este indicador valida que la digitalización del trámite ha sido percibida como una mejora sustancial frente a los métodos anteriores, cumpliendo con las expectativas de agilidad y modernización.

4.3.8 Inicio de sesión (Pregunta 8)

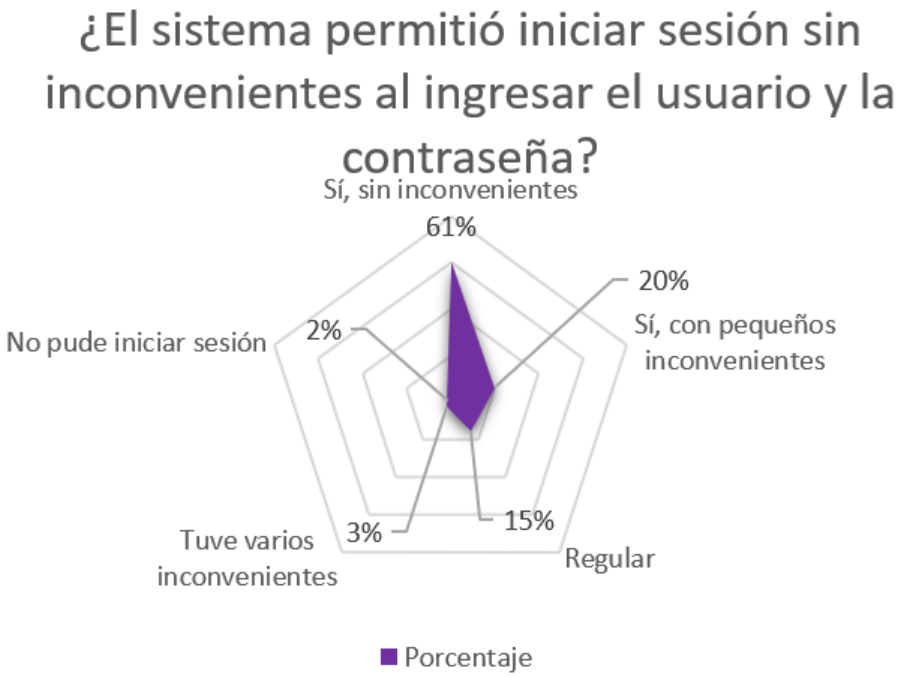


Figura: 179 Pregunta 8. ¿El sistema permitió iniciar sesión sin inconvenientes al ingresar el usuario y la contraseña?

El módulo de autenticación operó correctamente para el 80.5% de la muestra, quienes ingresaron "Sin inconvenientes" o con "Pequeños inconvenientes". Sin embargo, el análisis cualitativo de los comentarios de quienes reportaron problemas revela incidencias específicas con caracteres especiales (como la letra 'ñ') en las credenciales, un hallazgo técnico valioso para el mantenimiento correctivo del software.

4.3.9 Ubicación de la opción de descarga (Pregunta 9)

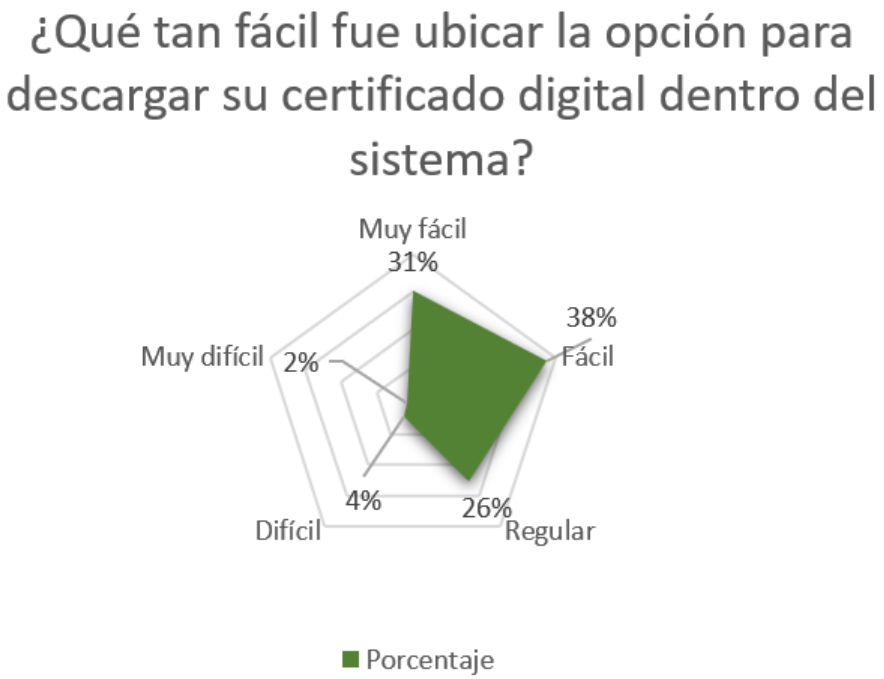


Figura: 180 Pregunta 9. ¿Qué tan fácil fue ubicar la opción para descargar su certificado digital dentro del sistema?

La navegabilidad hacia el producto final (el certificado) fue intuitiva para el 68% de los usuarios. Un 25.5% la calificó como "Regular", lo que sugiere que el botón o enlace de descarga podría destacarse visualmente de mejor manera. A pesar de ello, la tasa de dificultad declarada fue baja (5.5%), indicando que la gran mayoría logró completar el flujo de trabajo.

4.3.10 Ejecución de la descarga (Pregunta 10)

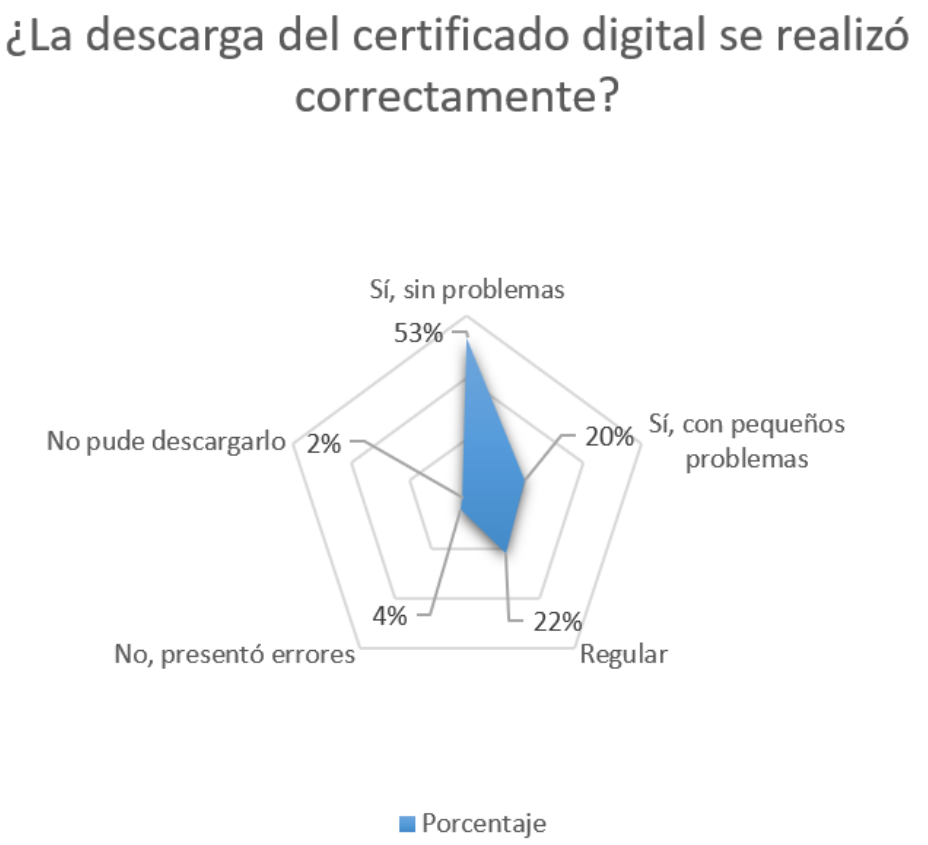


Figura: 181 Pregunta 10. ¿La descarga del certificado digital se realizó correctamente?

Este es uno de los indicadores técnicos más críticos. El 73% descargó el archivo "sin problemas" o con "pequeños problemas". Un 21.5% reportó un funcionamiento "regular" y un 5.5% tuvo errores bloqueantes. Si bien la mayoría obtuvo su certificado, el porcentaje de usuarios con dificultades técnicas en esta etapa final es un área prioritaria de atención para asegurar que la entrega del activo digital sea infalible.

4.3.11 Satisfacción con la descarga (Pregunta 11)

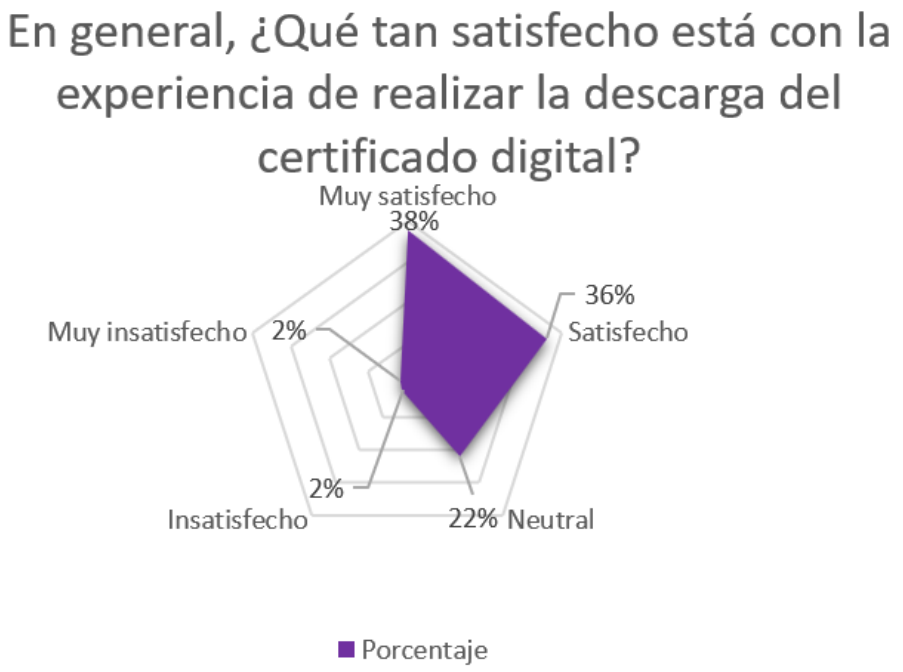


Figura: 182 Pregunta 11. En general, ¿qué tan satisfecho está con la experiencia de realizar la descarga del certificado digital?

A pesar de los retos técnicos mencionados anteriormente, la percepción de valor se mantiene alta. El 74% se mostró "satisfecho" o "muy satisfecho" con la descarga. El 22% de usuarios neutrales refleja la tolerancia debido a que no poseían un computador para culminar con el objetivo final (obtener el certificado).

4.3.12 Recepción de notificaciones (Pregunta 12)

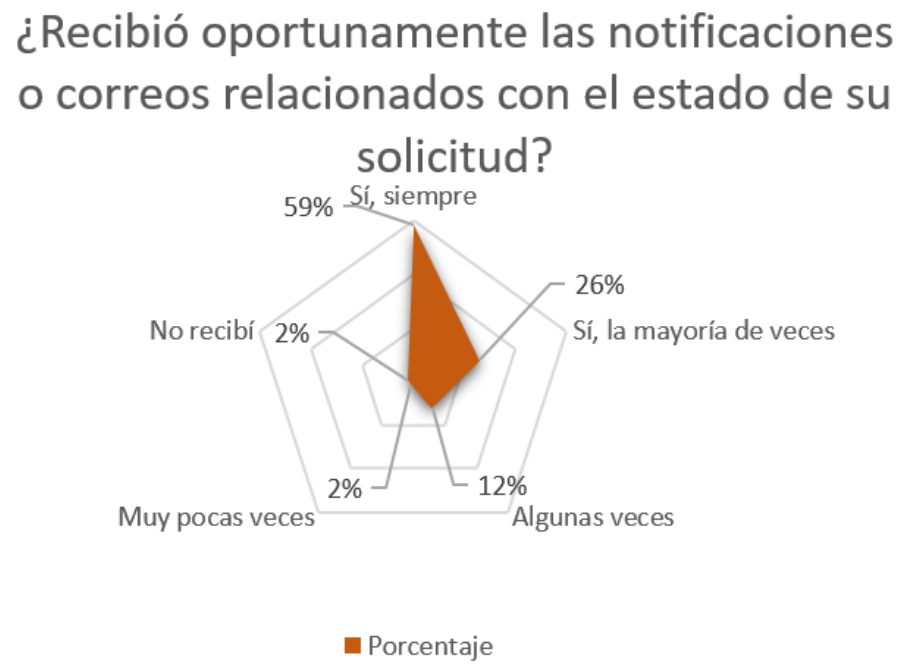


Figura: 183 Pregunta 12. ¿Recibió oportunamente las notificaciones o correos relacionados con el estado de su solicitud?

La comunicación asíncrona fue uno de los puntos fuertes del sistema. El 84.5% de los encuestados afirmó haber recibido las notificaciones "siempre" o "la mayoría de las veces". Esto demuestra que la integración con el servidor de correo institucional (SMTP) es robusta y cumple eficazmente con la función de mantener informado al usuario, un componente esencial de la transparencia administrativa.

4.3.13 Aspectos a mejorar (Preguntas 13 y 14)

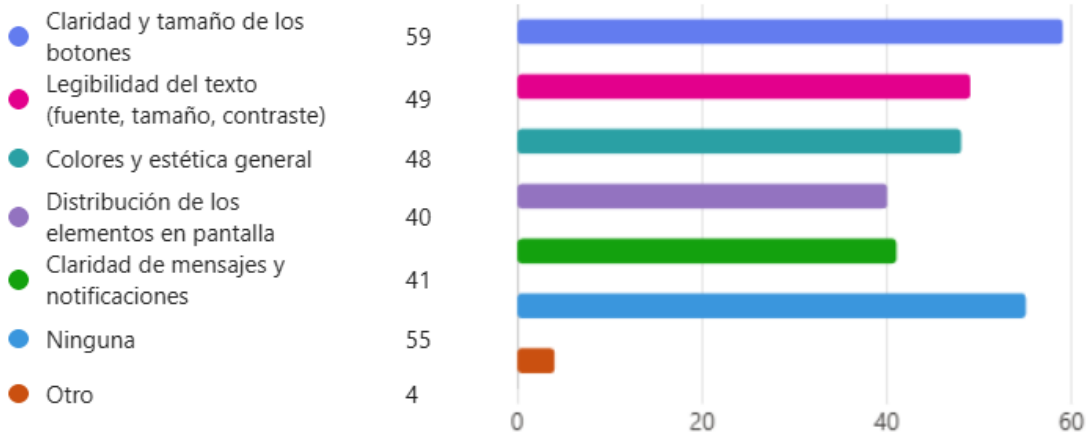


Figura: 184 Pregunta 13 y 14. ¿Qué aspectos visuales o de usabilidad considera que deberían mejorar en el sistema?

Al ser una pregunta de selección múltiple, se identificaron las siguientes prioridades de mejora según la frecuencia de mención:

- Claridad y tamaño de los botones
- Ninguna: Indicador de satisfacción total en este subgrupo.
- Legibilidad del texto
- Colores y estética general
- Claridad de mensajes/notificaciones

Adicionalmente, los comentarios abiertos (Pregunta 14) señalaron aspectos técnicos puntuales como "problemas con caracteres especiales (ñ) en contraseñas", "soporte HTTPS en todos los navegadores" y "bugs al iniciar sesión". Estos hallazgos trazan una hoja de ruta clara para la fase de mantenimiento evolutivo del software.

4.3.14 Recomendación del sistema (Pregunta 15)

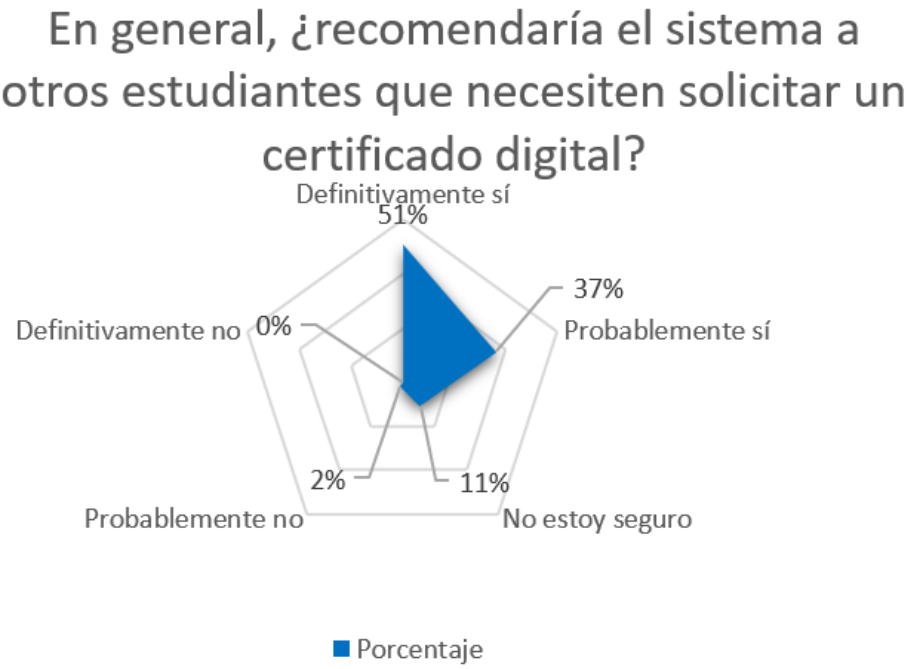


Figura: 185 Pregunta 15. En general, ¿recomendaría el sistema a otros estudiantes que necesiten solicitar un certificado digital?

El índice de adopción proyectada es contundente. El 87% de los estudiantes afirmó que recomendaría el sistema "definitivamente" (50.5%) o "probablemente" (36.5%). Solo un 2% manifestó una postura negativa ("probablemente no"). Este alto nivel de recomendación confirma la aceptación social y funcional de la herramienta dentro de la comunidad universitaria, validando el éxito del proyecto de titulación.

Conclusiones y recomendaciones

Conclusiones

Se llevó a cabo la implementación de un servicio de firma electrónica sustentado en una infraestructura de clave pública (PKI) para la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte, incorporando principios y buenas prácticas alineadas al marco de gestión de servicios ITIL v4. La solución fue desarrollada empleando exclusivamente herramientas de software libre, lo que permitió evidenciar que no es imprescindible la adquisición de licencias comerciales de alto costo para desplegar un sistema seguro, confiable y funcional que responda a las necesidades de gestión documental de la comunidad estudiantil.

Asimismo, se realizó un análisis detallado de los requerimientos técnicos y operativos necesarios para la puesta en producción del servicio, concluyendo que la arquitectura propuesta resulta técnica y económicamente viable para su implementación en la facultad. A diferencia de enfoques tradicionales que demandan una elevada inversión inicial, la solución diseñada aprovecha de manera eficiente la infraestructura tecnológica existente en la universidad, cumpliendo con los estándares de seguridad requeridos para la validación de documentos académicos, sin afectar el presupuesto institucional.

El desempeño del sistema fue evaluado en función de criterios de usabilidad, eficiencia y confiabilidad, determinándose que el servicio se encuentra en condiciones adecuadas para su operación en un entorno productivo dentro de la FICA. Las pruebas realizadas demostraron que la plataforma satisface los requisitos de seguridad, integridad de la información y manejo de concurrencia, asegurando una prestación eficaz del servicio de certificación digital a los estudiantes.

Finalmente, el proceso de validación con los usuarios finales evidenció un alto nivel de aceptación del sistema. De acuerdo con los resultados de la encuesta aplicada a los estudiantes de la FICA, el 87 % de los participantes manifestó su predisposición a recomendar el uso del servicio, resaltando la agilidad y claridad del proceso. Esta valoración positiva confirma que la solución propuesta no solo atiende de manera efectiva la problemática de la gestión documental, sino que también cuenta con el respaldo y aceptación necesarios para su adopción a mayor escala y su sostenibilidad a largo plazo dentro de la facultad.

Recomendaciones

Se recomienda extender de manera progresiva el servicio de firma electrónica, inicialmente implementado para los estudiantes de la Facultad de Ingeniería en Ciencias Aplicadas (FICA), hacia los estudiantes de las demás facultades de la Universidad Técnica del Norte. Esta ampliación deberá contemplar una planificación adecuada de los recursos tecnológicos, con el fin de garantizar la disponibilidad y continuidad del servicio para la comunidad universitaria.

Considerando que el proceso de acreditación como Entidad de Certificación de Información ante los organismos de control nacionales implica altos costos y una elevada complejidad técnica, se sugiere establecer un marco normativo interno que respalde el uso de los certificados digitales emitidos por el sistema para la validación de trámites académicos estudiantiles dentro del ámbito universitario.

Dado que la solución fue implementada utilizando herramientas de software libre, se recomienda fortalecer la capacitación del personal técnico responsable de la administración del sistema, a fin de garantizar su correcta operación, mantenimiento y evolución conforme aumente el número de estudiantes beneficiarios.

Finalmente, en concordancia con el enfoque de mejora continua de ITIL v4 y los hallazgos del análisis de satisfacción de usuario, se recomienda ejecutar un plan de mantenimiento evolutivo centrado en la experiencia de usuario (UX). Es prioritario refinar la interfaz gráfica para mejorar la legibilidad y accesibilidad en diversos dispositivos, asegurando así que la barrera tecnológica sea mínima para los nuevos estudiantes que se incorporen al sistema.

Referencias Bibliográficas

[1] L. Hernandez, A. Pranolo, and A. P. Wibawa, "Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution," *Transactions on Energy Systems and Engineering Applications*, vol. 5, no. 2, pp. 1–20, Nov. 2024, [Online]. Available: https://revistas.utb.edu.co/tesea/article/view/635

[2] B. Gopi and M. Sutharsan, "An Improved Public Key Infrastructure (PKI)-Based Digital Signature Authentication Service for Higher Key Storage System," *BOHR International Journal of Smart Computing and Information Technology*, vol. 2022, no. 1, pp. 51–56, Accessed: Apr. 30, 2025. [Online]. Available: https://www.researchgate.net/publication/367960332_An_Improved_Public_Key_Infrastructure_PKI-Based_Digital_Signature_Authentication_Service_for_Higher_Key_Storage_System

[3] K. Peffers *et al.*, "Design Science Research Process: A Model for Producing and Presenting Information Systems Research," *Cornell University*, Jun. 2020, Accessed: Jun. 21, 2025. [Online]. Available: https://arxiv.org/pdf/2006.02763

[4] M. L. Remache Típan, "Marcos de gestión de tecnologías de información : análisis del marco de gestión ITIL v4.," 2022, Accessed: Jun. 07, 2025. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/22414

[5] Nigel Ivan Jose Montesinos Flores and Jhonatan Rober Tamayo Jaimes, "PROPUESTA DE UNA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE PROYECTOS E INCIDENCIAS CON ENFOQUE ITIL v4.0 PARA MEJORAR LOS SERVICIOS DE TI DEL CENTRO COMERCIAL MEGAPLAZA EN LA CIUDAD DE LIMA ," Universidad Tecnológica del Perú, Lima, 2022. Accessed: Jun. 07, 2025. [Online]. Available: https://repositorio.utp.edu.pe/handle/20.500.12867/6273

[6] Kathleen Richards, "What is Cryptography?," Techtarget Search Segurity. Accessed: Jun. 07, 2025. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/cryptography

[7] P. R. Carrión-Ramírez and R. R. Criollo-Bonilla, "Esquema de certificación digital de documentos electrónicos en la Universidad Católica de Cuenca: Un enfoque basado en principios de seguridad informática," *MQRInvestigar* , vol. 8, no. 3, pp. 1311–1323, Jul. 2024, doi: 10.56048/MQR20225.8.3.2024.1311-1323.

[8] Kely Yohana Rojas Meneses, Leonardo Salamanca Polanco, and José Alejandro Franco Calderon, "FIRMA ELECTRÓNICA EN COLOMBIA: UN ACELERADOR EN LA OPTIMIZACIÓN DE RECURSOS Y PROCESOS," *Revista Ingeniería, Matemáticas y Ciencias de la Información*, pp. 1–22, Jun. 2024, Accessed: Jun. 09, 2025. [Online]. Available: https://ojs.urepublicana.edu.co/index.php/ingenieria/article/view/1095/739

[9] Gina M. Raimondo and Laurie E. Locascio, "Digital Signature Standard (DSS)," *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*, pp. 1–86, Feb. 2023, Accessed: Jun. 09, 2025. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.186-5

[10] S. E. M. Urdaneta, D. M. Vega, and D. F. S. Chacón, "Certificación digital de documentos académicos usando Blockchain Formato IEEE," *Tecnología Investigación y*

Academia, vol. 7, no. 2, pp. 21–27, Jan. 2020, Accessed: Apr. 30, 2025. [Online]. Available: https://revistas.udistrital.edu.co/index.php/tia/article/view/12757

[11] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates Version 2.1.5 ," pp. 1–163, May 2025, Accessed: Jun. 14, 2025. [Online]. Available: https://cabforum.org/working-groups/server/baseline-requirements/documents/CA-Browser-Forum-TLS-BR-2.1.5.pdf

[12] GlobalSign, "What is Code Signing?" Accessed: Jun. 14, 2025. [Online]. Available: https://www.globalsign.com/en/code-signing-certificate/what-is-code-signing

[13] J. Schaad, August Cellars, B. Ramsdell, and Inc. Brute Squad Labs, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification," Apr. 2019. Accessed: Jun. 14, 2025. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc8551.txt.pdf

[14] Adobe Inc., "Manage Digital IDs in Acrobat." Accessed: Jun. 14, 2025. [Online]. Available: https://helpx.adobe.com/acrobat/using/digital-ids.html

[15] Carrera López Alberto Francisco and Celi Jiménez Juan Francisco, "Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente.," Universidad de las Fuerzas Armadas ESPE, Sangolqui, 2022. Accessed: Jun. 13, 2025. [Online]. Available: https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/ddccf8b2-1a8c-4d86-84ea-7df6cba24e40/content

[16] keyfactor, "EJBCA Concepts." Accessed: Jun. 13, 2025. [Online]. Available: https://docs.keyfactor.com/ejbca/latest/ejbca-concepts

[17] F. Marchioni, *WildFly Administration Guide: The ultimate and most up-to-date guide to manage WildFly appication server*, vol. 3. 2020. Accessed: Oct. 04, 2025. [Online]. Available: https://books.google.com/books?hl=es&lr=&id=rufiBAAAQBAJ&oi=fnd&pg=PA1&dq=wildfly+application+server&ots=lbjNPAmcT-&sig=zvecSvYJoZuNWs5my_W8ufMLKss

[18] S. L. Nita and M. I. Mihailescu, "JDK 21: New Features," *Cryptography and Cryptanalysis in Java*, pp. 19–37, 2024, doi: 10.1007/979-8-8688-0441-0_2.

[19] M. De Oliveira Barros, F. De Almeida Farzat, and G. H. Travassos, "Learning from optimization: A case study with Apache Ant," *Inf Softw Technol*, vol. 57, no. 1, pp. 684–704, Jan. 2015, doi: 10.1016/J.INFSOF.2014.07.015.

[20] A. Pilicita Garrido, Y. Borja López, and G. Gutiérrez Constante, "Rendimiento de MariaDB y PostgreSQL," *Revista Científica y Tecnológica UPSE*, vol. 7, pp. 9–16, Jun. 2021, doi: 10.26423/rctu.v7i2.538.

[21] Asamblea Nacional del Ecuador, "LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS," Quito: Registro Oficial, Quito, Aug. 2021. Accessed: Jun. 21, 2025. [Online]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

[22] B. S. Jaramillo Araujo, "Implantación y certificación del servicio de firma electrónica en la Universidad de las Fuerzas Armadas 'ESPE' – Sede Latacunga, utilizando ITIL V4,"

Universidad de las Fuerzas Armadas ESPE, 2023. Accessed: Jul. 14, 2025. [Online]. Available: http://repositorio.espe.edu.ec/handle/21000/37447

[23] E. A. Aranda Vergara, “Valor público de los servicios de certificación digital del estado en la transformación digital 2023,” Universidad San Ignacio de Loyola, Lima, 2023. Accessed: Jul. 14, 2025. [Online]. Available: https://hdl.handle.net/20.500.14005/15585

[24] Ampuero Herrera Renato Mario, “Implementación de la plataforma de firma digital para el proceso de emisión de documentos académicos en la Universidad Nacional de Barranca,” Universidad Cesar Vallejo, LIMA, 2021. Accessed: Jun. 21, 2025. [Online]. Available: https://repositorio.ucv.edu.pe/handle/20.500.12692/60148

[25] A. Vela Gonzales and W. Macedo Rojas, “Desarrollo e implementación de una aplicación web con firma electrónica y certificado digital, para mejorar la gestión de notas de los estudiantes del senati zonal Loreto 2019,” Univesidad Cientifica del Perú, LORETO, 2020. Accessed: Jun. 21, 2025. [Online]. Available: http://hdl.handle.net/20.500.14503/1162

[26] C. R. B. Vermejo Ruiz, “Desarrollo e implementación del Sistema de Firmas Electrónicas y Certificados Digitales del Estado e implantación de la autoridad administrativa competente,” Universidad de Lima, Lima, 2020. Accessed: Jun. 21, 2025. [Online]. Available: https://repositorio.ulima.edu.pe/handle/20.500.12724/12017

[27] J. D. Arcos Poma and R. J. Espín Flores, “Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4,” Universidad de las Fuerzas Armadas ESPE, Quito, 2022. Accessed: Jun. 21, 2025. [Online]. Available: http://repositorio.espe.edu.ec/handle/21000/32744

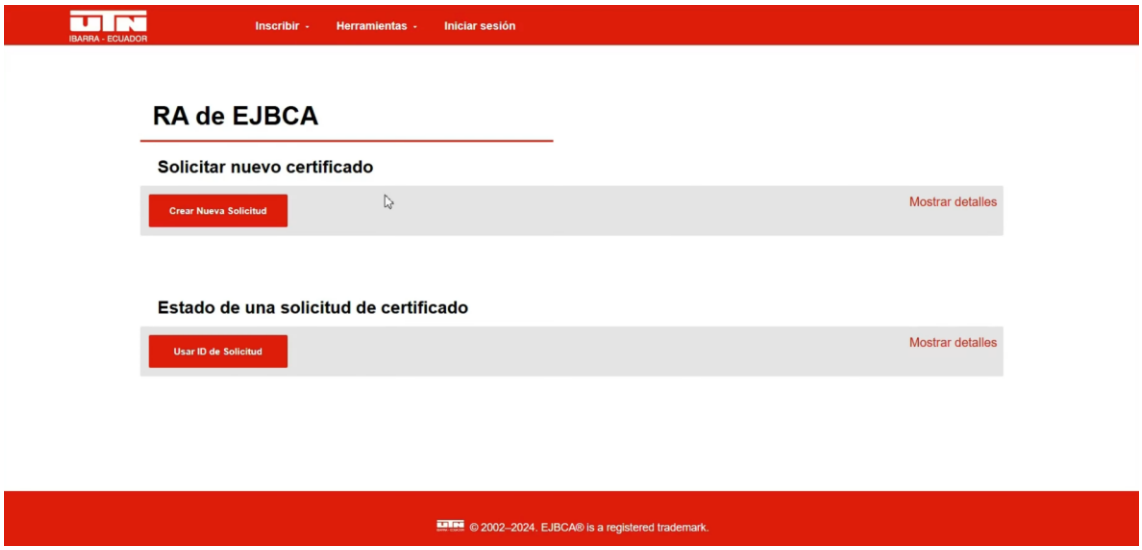
[28] O. Arrayan and L. Marlene, “Implementación del módulo de firmas digitales para el sistema integrado de actividad docente (SIAD) de la carrera de software de la Universidad Técnica del Norte mediante el uso de un token criptográfico aplicando el estándar de infraestructura de clave pública X.509 para automatizar el proceso de entrega de documentos,” Feb. 2020, Accessed: Apr. 30, 2025. [Online]. Available: https://repositorio.utn.edu.ec/handle/123456789/10255

[29] K. F. Galarza-Pauta and R. R. Criollo-Bonilla, “Modelo de vaidación de firmas y certificados digitales embebidos en documentos electrónicos generados por los estudiantes de la Universidad Católica de Cuenca,” *MQRInvestigar*, vol. 8, no. 3, pp. 1371–1387, Jul. 2024, [Online]. Available: https://dspace.ucacue.edu.ec/handle/ucacue/18735

Anexos

Anexo A. Vista general del sistema implementado EJBCA Community.

- Acceso público para la solicitud de certificados digitales del sistema EJBCA.



- Acceso restringido para la administración del servicio de EJBCA

Anexo B. Requisitos técnicos ARCOTEL

Especificación requisitos técnicos.

Se pudo obtener un mejor detalle acerca de la documentación técnica necesaria para la certificación. La información que se presentará a continuación es la documentación mínima que la institución debe presentar para poder obtener la certificación

- Objetivo.
- Introducción
- Diagrama esquemático y descripción técnica detallada de la infraestructura
    - Detalle técnico de la infraestructura de clave pública
    - Jerarquía entidad de certificación de información
    - Administración de la autoridad de certificación
    - Roles y responsabilidades para generación y migración de llaves privadas
    - Procesos de auditoría de seguridad
- Descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles
    - Descripción y alcance detallado de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación
    - Descripción detallada del servicio propuesto como entidad de certificación
    - Mecanismos de validación: CRL, OCSP, LDAP
    - Certificados de servidor seguro (SSL)
    - Servicios de emisión, renovación y revocación de certificados digitales
    - Autoridades de registro (AR)
- Portafolio de servicios/productos de la entidad de certificación de información
- Diagrama técnico detallado de cada "nodo" o "sitio seguro" y especificaciones técnicas de los equipos
    - Sitio seguro principal
        - Descripción del esquema de red
        - Dispositivos de seguridad de borde
        - Acceso a servicios desde internet
        - Conectividad LAN
        - Servidores

        - Almacenamiento
        - Sistema de respaldos
        - Red SAN
        - Data center
        - Seguridad
        - Detalle de hardware y software
        - Ubicación y distribución de equipos
        - Esquema de conectividad
        - Topología de conectividad
        - Esquema de cómputo.
        - Hardware criptográfico HSM
        - Esquema de respaldos.
    - Sitio seguro secundario
        - Descripción del esquema de red
        - Dispositivos de seguridad de borde
        - Almacenamiento
        - Red de comunicaciones
- Ubicación geográfica de cada nodo o sitio seguro
    - Sitio principal
    - Sitio alterno
- Documentos de soporte que confirmen que se dispone de mecanismos de seguridad.
    - Mecanismos de seguridad
        - Seguridad a través de la criptografía
        - Certificado digital
        - Entidad de certificación
        - Algoritmos
    - Contenedores criptográficos

- Especificaciones técnicas de los contenedores
- Estándares y normas internacionales
    - Normas, estándares
    - Infraestructura de clave pública internet.
- Componentes de seguridad perimetral
    - Sistema de prevención de intrusos
    - Firewall
    - Balanceadores
- Esquema de seguridad perimetral
- Esquema de seguridad de la infraestructura de clave pública
- Plan de contingencia
- Sistema de control de acceso al centro de cómputo
- Registro ingreso centro de cómputo
- Dispositivos utilizados para el acceso al centro de cómputo
- Respaldo de información

Anexo C. Requisitos legales ARCOTEL

Requisitos: ENTIDADES DE CERTIFICACIÓN

Personas jurídicas	1. Solicitud dirigida al Director/a Ejecutivo/a de la ARCOTEL, detallando nombres y apellidos completos del representante legal, dirección domiciliaria de la empresa unipersonal o compañía. 2. Copia de pasaporte del Representante Legal en caso de ser extranjero. 3. Copia del certificado de votación del último proceso eleccionario (correspondiente al representante legal, excepto cuando se trate de ciudadanos extranjeros) 4. Copia certificada e inscrita en el Registro Mercantil (excepto las instituciones públicas) del nombramiento del representante legal 5. Copia certificada debidamente registrada en el Registro Mercantil, de la escritura de constitución de la empresa unipersonal o compañía y reformas en caso de haberlas (excepto las instituciones públicas). 6. Original del certificado de cumplimiento de obligaciones emitido por la Superintendencia de Compañías o Bancos y Seguros según corresponda, a excepción de las instituciones del Estado. 7. Diagrama esquemático y descripción técnica detallada de la infraestructura a ser utilizada, indicando las características técnicas de la misma. 8. Descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación. La ARCOTEL podrá ordenar inspecciones o verificaciones a las instalaciones del peticionario cuando lo considere necesario; 9. Documentos de soporte que confirmen que se disponen de mecanismos de seguridad para evitar la falsificación de certificados, precautelar la integridad, resguardo de documentos, protección contra siniestros, control de acceso y confidencialidad durante la generación de claves, descripción de sistemas de seguridad, estándares de seguridad , sistemas de respaldo. 10. Ubicación geográfica inicial, especificando la dirección de cada nodo o sitio seguro. 11. Diagrama técnico detallado de cada «Nodo» o «Sitio Seguro» detallando especificaciones técnicas de los equipos. 12. Información que demuestre la capacidad economica y financiera para la prestación de servicios de certificación de información y servicios relacionados.
Nota	Dentro de las Competencias de la Agencia de Regulación y Control de las Telecomunicaciones está el regular y controlar las actividades relacionadas con el comercio electrónico y firma electrónica, de conformidad con el ordenamiento jurídico vigente.
Nota	Las entidades de certificacion son reguladas por la Ley de Comercio electronico y sus reglamentos vigentes.

Entrate

Anexo D. Manual de instalación del sistema operativo AlmaLinux

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

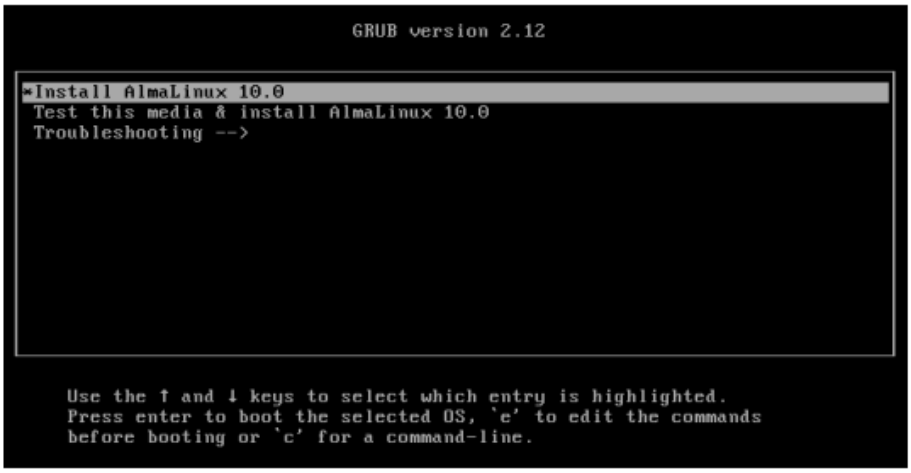
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Manual de Usuario "Instalación de Alma Linux"

1. Menú de Arranque (GRUB)

En la primera pantalla negra del gestor de arranque:

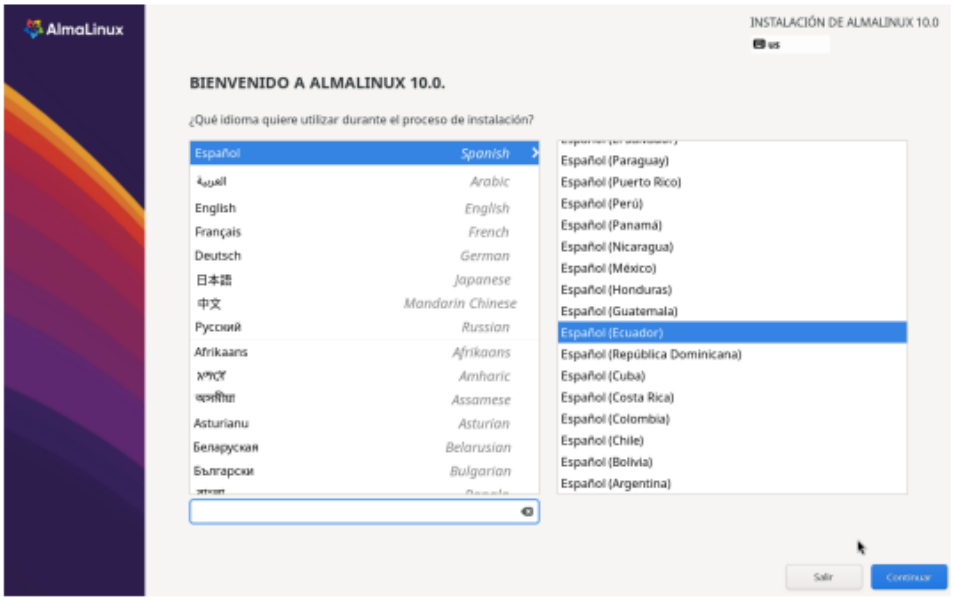
- Usa las flechas del teclado para resaltar la opción **"Install AlmaLinux 10.0"**.



2. Selección de Idioma

Una vez que carga la interfaz gráfica (Anaconda):

- **Acción:** En la columna de la izquierda, selecciona **"Español"**.
- **Acción:** En la columna de la derecha, elige la variante específica **"Español (Ecuador)"**.
- **Botón:** Haz clic en **"Continuar"** en la esquina inferior derecha.



3. Resumen de la Instalación

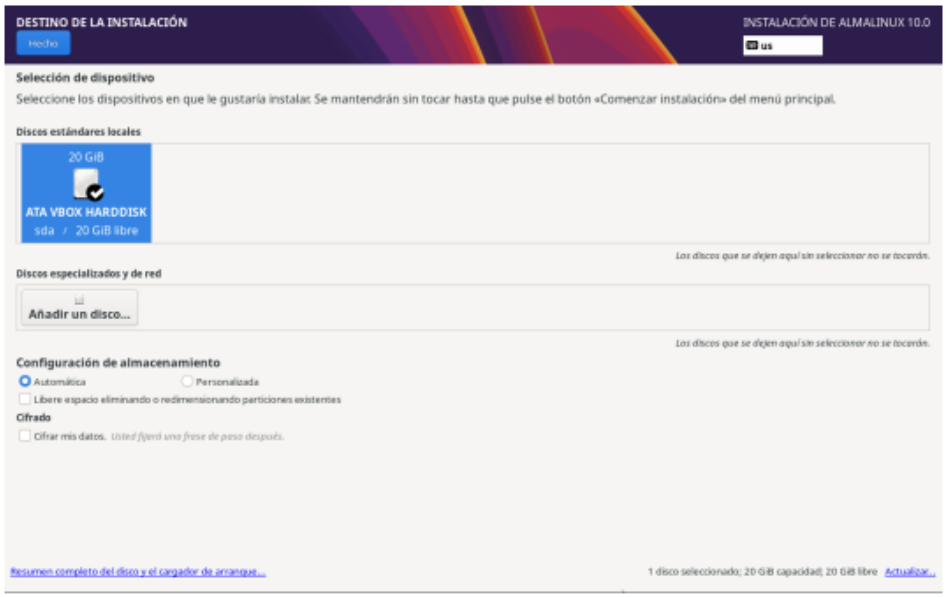
Este es el panel central de configuración. Antes de avanzar, debes revisar los recuadros con iconos de advertencia:

- **Regionalización:** Verifica que el teclado esté en "Inglés (EE. UU.)" (según tu captura) y la zona horaria en "América/Guayaquil".
- **Software:** Se observa que has elegido **"Server with GUI"** (Servidor con interfaz gráfica).
- **Sistema:** Debes entrar en "Destino de la instalación" (donde aparece el aviso).
- **Ajustes de Usuario:** Debes configurar la "Cuenta de root" o la "Creación de usuario" antes de poder empezar.

4. **Destino de la Instalación (Particionado)**

Dentro de este menú:

- **Selección de dispositivo:** Haz clic sobre el disco duro detectado (en tu caso, un **ATA VBOX HARDDISK de 20 GiB**) para que aparezca el icono de la marca de verificación.
- **Configuración de almacenamiento:** Asegúrate de que esté seleccionada la opción **"Automática"**.
- **Botón:** Haz clic en **"Hecho"** en la esquina superior izquierda para regresar al menú principal.

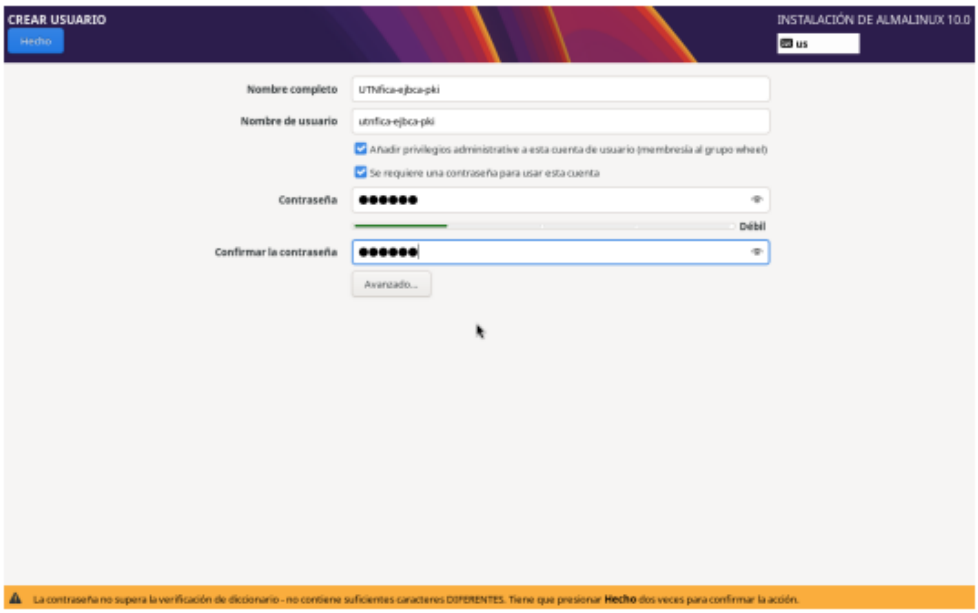


5. Creación de Usuario

Para este paso, has definido las credenciales específicas para tu proyecto:

- **Nombre completo:** Ingresa UTNfica-ejbca-pki.
- **Nombre de usuario:** El sistema sugerirá utnfica-ejbca-pki.
- **Privilegios:** Asegúrate de marcar la casilla **"Añadir privilegios administrativos a esta cuenta..."** (esto añade al usuario al grupo wheel).
- **Contraseña:** Introduce y confirma tu clave.

Nota: Si la contraseña es considerada "Débil" (como muestra la barra roja en tu captura), deberás presionar el botón **"Hecho"** dos veces para confirmar que deseas usarla de todos modos.



6. Progreso de la Instalación

- **Acción:** Una vez configurado el usuario y el disco, haz clic en **"Comenzar la instalación"** en el menú de resumen.
- **Proceso:** Verás una barra de progreso que indica "Instalando el software". Solo queda esperar a que finalice la copia de archivos y la configuración del núcleo.

7. Finalización y Reinicio

Cuando la barra de progreso se complete y aparezca el mensaje "¡Completado!":

- **Acción:** Haz clic en el botón azul **"Reinicio del sistema"** en la esquina inferior derecha.
- **Resultado:** El equipo se reiniciará y podrás iniciar sesión con el usuario utnfica-ejbca-pki que creaste.

Anexo E. Manual de usuario para solicitar y obtener un certificado digital

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Manual de Usuario "Solicitud de Certificado Digital"

1. Primero ingresamos al botón ¨Crear Nueva Solicitud¨

2. Como segundo paso, en la sección de "Seleccionar Plantilla de Solicitud", seleccionamos en generación de par de claves, opción ¨Por la Autoridad Certificadora UTN¨.

3. Como tercer paso, en la sección de "Proporcionar información de la Solicitud", llenamos los campos conforme a las siguientes indicaciones:

Identificador de Usuario: *E1002860460* (la primera letra en mayúsculas "E" y luego el número de cédula).

Nombres Completos: *Juan Jens Pérez Rivaldo* (Poniendo primero los nombres y luego los apellidos, cumplimos con las siguientes reglas:

La primera letra de cada palabra en mayúsculas y el resto del nombre propio en minúsculas).

4. Como cuarto paso, en la sección "Proporcionar Credenciales de Usuario", llenamos lo campos conforme a las siguientes indicaciones:
   Nombre de Usuario: *japaspuels* (El prefijo del correo electrónico personal antes del "@")
   Contraseña: Colocar una contraseña de mínimo 16 dígitos, los cuales incluyen mayúsculas, números y caracteres especiales como por ejemplo el @.
   Confirmar Contraseña: Colocar la misma contraseña que en el campo anterior.
   Correo electrónico: japaspuels@utn.edu.ec colorar nuestro correo personal o institucional, el cual servirá para recibir los estados de la solicitud de firma electrónica y aprobación de la misma.

5. Una vez llenado todos los campos conforme a las indicaciones, hacer clic en "Confirmar Solicitud" y revisar el mensaje de confirmación de "La solicitud fue enviada con éxito y está en espera de aprobación" de color negro.

Anexo E. Notas de la versión 9.1 de EJBCA y certificación.

Contenedor EJBCA y SignServer / Información de lanzamiento / Notas de la versión

Notas de la versión 9.1 de EJBCA

NOVIEMBRE DE 2024

El equipo de EJBCA se complace en anunciar el lanzamiento de EJBCA 9.1.

EJBCA 9.1 incluye soporte para los algoritmos cuánticos seguros aprobados por el NIST ML-DSA y ML-KEM, los primeros estándares completados de Criptografía poscuántica (PQC) del NIST proyecto de estandarización. La versión también amplía la funcionalidad con certificados operativos compatibles con Matter, integración HSM extendida y mejoras en la API REST. Además, la versión aborda un posible problema de cumplimiento y resuelve un posible problema de seguridad.

Estas notas de la versión cubren nuevas características y mejoras implementadas en EJBCA 9.1.0 y EJBCA 9.1.1 (EJBCA 9.1.0 era una versión interna, generalmente no disponible para los clientes).

EJBCA 9 introdujo soporte de validación CAA S/MIME para alinearse con los estándares CA/Browser Forum para la seguridad del correo electrónico. Esta importante versión también introdujo soporte para una pila de tecnología mejorada, que requiere WildFly 32 o JBoss EAP 8 como servidores de aplicaciones y Java 17 como entorno de ejecución. Para obtener más información, consulte el Notas de la versión 9.0 de EJBCA.

Para conocer las opciones de implementación disponibles y las versiones asociadas, consulte Versiones compatibles.

Aspectos destacados

Algoritmos de seguridad cuántica aprobados por el NIST ML-DSA y ML-KEM

EJBCA 9.1 agrega soporte para emitir certificados con algoritmos cuánticos seguros aprobados por el NIST ML-DSA y ML-KEM. Estos algoritmos PQC estandarizados reemplazan los algoritmos candidatos Dilithium y Kyber que eran compatibles con versiones anteriores de EJBCA antes de que se lanzaran los algoritmos aprobados por el NIST.

Para obtener más información, consulte Claves y firmas de criptografía poscuántica.

Certificados Operativos de Materia

matter

Matter es el estándar de la industria para dispositivos domésticos inteligentes interoperables. El soporte para emitir certificados de certificación de dispositivos que cumplan con el estándar Matter se introdujo en EJBCA 8 y EJBCA 9.1 ahora ofrece soporte para emitir certificados operativos que cumplan con el estándar Matter. Para obtener más información, consulte Crear CA para la PKI operativa de Matter.

Compatibilidad con módulos de seguridad de hardware extendidos (HSM)

En EJBCA 9.1, el conjunto de contenedores EJBCA admite el uso de Entrust nShield Connect HSM. Para obtener más información, consulte la documentación del contenedor EJBCA en Integración HSMn. EJBCA 9.1 también introduce soporte para la integración basada en API REST con Securosys HSM mediante la introducción de un nuevo token criptográfico.

Extensiones de API REST

Para las implementaciones configuradas para utilizar certificados híbridos, una extensión de la API REST en EJBCA 9.1 permite a los clientes de la API REST recuperar información sobre algoritmos de clave alternativos disponibles al obtener información sobre perfiles de certificados a través de `/v2/certificate/profile/` endpoint.

Anuncios

Posible problema de cumplimiento de la CAA

Debido a un error lógico en EJBCA al interpretar las respuestas de Autorización de Autoridad de Certificación (CAA), las versiones de EJBCA anteriores a 8.3.3 y 7.1 podrían aprobar incorrectamente la emisión de un certificado comodín relacionado con el nombre de dominio que está prohibido por las entradas de CAA en el DNS. Para obtener más detalles, consulte el artículo del portal de soporte de Keyfactor Posible problema de cumplimiento de la CAA.

Posible problema de seguridad relacionado con la implementación de proxy inverso

Actualizado Seguridad EJBCA La documentación incluye la configuración de proxy inverso recomendada para evitar posibles vulnerabilidades.

Eliminación del soporte de algoritmos GOST y DSTU

Se ha eliminado el soporte para los algoritmos GOST y DSTU. Estos algoritmos quedaron obsoletos en EJBCA 8.3 y ya no están disponibles en esta versión.

Eliminación de la funcionalidad OCSP específica del perfil del certificado

Las siguientes propiedades fueron declaradas obsoletas en EJBCA 8.3:

- ocsp.999.hastaSiguienteActualización
- ocsp.999.revoked.untilNextUpdate
- ocsp.999.maxEdad
- ocsp.999.revoked.maxAge

Estas propiedades permitieron establecer configuraciones específicas basadas en perfiles de certificados individuales. Se han eliminado las propiedades y la funcionalidad asociada.

Eliminación de propiedades no utilizadas de cesecore.properties

Las siguientes propiedades en el *cesecore.propiedades* Los archivos no se utilizan (o no son necesarios) y han sido eliminados.

- *ca.toolateexpiredate*
- *authkeybind.chiphersuite*

- *db.keepinternalcakeystores*
- *ca.keepocspextendedservice*

Mejora del castillo inflable

Bouncy Castle se ha actualizado a la versión 1.79. Para obtener información sobre los últimos lanzamientos de Bouncy Castle, consulte el Notas de lanzamiento de Bouncy Castle.

Actualizar información

Revisa el Notas de actualización de EJBCA para obtener información importante sobre este comunicado. Para obtener instrucciones de actualización e información sobre las rutas de actualización, consulte Actualización de EJBCA.

Registro de cambios: problemas resueltos

Las siguientes listas implementaron características y solucionaron problemas en EJBCA 9.1.0 y EJBCA 9.1.1.

Cuestiones resueltas en 9.1.1

Publicado en noviembre de 2024

Corrección de errores

Regresión ECA-12782: Pocas suites de chips no se movieron después de eliminar las propiedades no utilizadas de cesecore

ECA-12805 La emisión del certificado comodín se permite incorrectamente cuando el registro ";" de emisión de CAA está presente

Problemas resueltos en 9.1.0

Comunicado interno noviembre de 2024

Nuevas características

ECA-12327 Componentes DN específicos de IoT de Add Matter para certificados operativos de nodos

ECA-12371 Implementar la construcción y ejecución de pruebas unitarias

Integración de ECA-12453 nShield Connect con el contenedor EJBCA en Kubernetes

ECA-12576 Representar claves públicas PQC \(alternativa\) para certificados híbridos en la pantalla de certificados de la vista web de RA

ECA-12599 CriptoToken de API REST HSM de Securosys Primus

ECA-12659 Emisión del certificado ML-KEM con CMP v3 mediante prueba de posesión encrCert

ECA-12759 Habilitar el cambio del algoritmo generador de números de serie en el contenedor

Mejoras

ECA-12044 Representar parámetros públicos ML-DSA y ML-KEM en el verificador de certificados web RA

ECA-12084 Eliminar la funcionalidad ocsp específica del perfil de certificado obsoleto

ECA-12270 Política de red para el gráfico de timón EJBCA

ECA-12326 Eliminar soporte para GOST y DSTU

ECA-12423 Permitir OCSP Nonce de hasta 128 bytes según RFC9654

ECA-12578 Actualización a BC 1.79 final

ECA-12645 Se requiere una dirección de correo electrónico en RA Web - Realizar nueva solicitud, pero no está marcada como tal

ECA-12653 Utilice el nombre DNS para el nombre de archivo cuando NO se utiliza DN de asunto

ECA-12666 Devuelve un algoritmo de clave alternativa a través de/v2/certificate/profile/

ECA-12693 Mejorar el registro de ciertos errores EST

ECA-12699 Eliminar propiedades no utilizadas de cesecore.properties

ECA-12704 Documento sobre cómo exportar e importar datos eliminados por database-housekeeping.sql

ECA-12706 Eliminar LegacySoftCryptoToken y clases asociadas

ECA-12712 Eliminar código de muestra del directorio src

ECA-12736 Ignore las entradas sin alias en el par de claves de lista P11NG-CLI, actualice p11ng a 0.25.1

Limpieza ECA-12743: CertTools.genSelfCertForPurpose está obsoleto y las referencias deben eliminarse

ECA-12755 Corrija fallas en las pruebas CMP después de la fusión de encrCert ML-KEM

Corrección de errores

ECA-12394 Manejo adecuado de los miembros del rol de acceso público durante el inicio del contenedor

ECA-12471 El error del token infinito

ECA-12523 RA Web - Certificado de inspección: la clave pública no se presenta correctamente cuando se utiliza el algoritmo PQ

ECA-12529 Los cachés no se actualizan después de que se hayan recargado las configuraciones externas

ECA-12608 Admin Web - Nuevo token criptográfico - NPE al crear un nuevo token pkcs#11NG \(mejora del mensaje de error\)

ECA-12691 Admin Web - Crear CA - CVC disponible, pero deshabilitado \(Inconsistencia de CE\)

ECA-12692 REST y point v1/cas devuelven un emisorDN incorrecto para tres jerarquías de nivel \(o más\)

La respuesta REST del comando ECA-12719 KF no se lee completamente durante las inscripciones en Proxy CA

ECA-12726 EJBCA CE - PKCS#11 no funciona después de actualizar EJBCA a JDK17

Regresión ECA-12729: APPSERVER_USE_MANAGED_ID

ECA-12734 Actualizar la versión BC en jboss-deployment-structure.xml