ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Implantación y Certificación del Servicio de Firma Electrónica en la Universidad de las Fuerzas Armadas “ESPE” – Sede Latacunga, utilizando ITIL V4

Jaramillo Araujo, Brandon Steven

Contenido

01

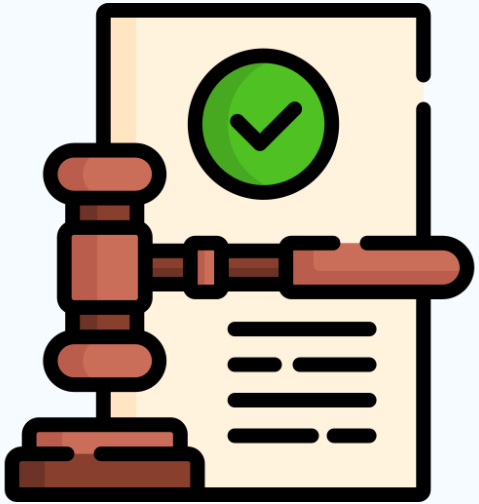
Introducción

Problema

La firma manuscrita en la ESPE, es el medio usado por los estudiantes para legalizar un documento.

- Uso excesivo e innecesario de papel
- Falta de espacio físico
- Dificultad para verificar las firmas
- Falsificación de firmas
- Riesgo de perdida o alteración de documentos
- Dificulta la eficiencia y agilidad en la gestión documental

Problema



La ausencia de una certificación por parte de la ARCOTEL, deja sin respaldo legal a las firmas electrónicas.

- Desconfianza
- Sin validez jurídica
- Limita el uso de la firma electrónica.

Justificación

Adoptar un Servicio de Firma Electrónica permitirá que la gestión documental en procesos administrativos, se pueda realizar de manera digital.

- Ahorro de papel y espacio físico
- Facilidad para verificar las firmas
- Documentos inalterables y fuera de objeto de fraude
- Mejora la eficiencia y agilidad en la gestión documental

Justificación

La certificación por parte de la ARCOTEL, otorga un respaldo legal y validez jurídica a la firma electrónica.

- Permite el uso de la firma electrónica dentro y fuera de la Universidad.

Objetivos

General

Implantar el Servicio de Firma Electrónica para la Universidad de las Fuerzas Armadas ESPE, sede Latacunga, en la comunidad conformada por docentes, estudiantes y personal administrativo de la Sede, realizar los procesos necesarios para obtener la certificación por parte del organismo de control para estar en capacidad de ampliar el servicio a las diferentes sedes de la Universidad.

Objetivos

Específicos

- Establecer el estado del Arte
- Implantar el Servicio de firma electrónica en la Sede Latacunga de la ESPE, utilizando ITIL V4.
- Determinar los requisitos técnico-legales para la certificación del Servicio de firma digital con las características diseñadas e implantado en el ESPE-CERT para la comunidad de la ESPE sede Latacunga.

Objetivos

Específicos

- Evaluación técnico informática de pre certificación del servicio de firma digital para la ESPE sede Latacunga.
- Mejora del Servicio y resolución de las no conformidades.

02

Fundamentación teórica

Infraestructura de Clave Pública (PKI)

Conceptos clave

Criptografía asimétrica

Método criptográfico para encriptar y desencriptar mensajes de datos, usando una llave privada y una llave pública.

Hashing

Método criptográfico que transforma un mensaje de datos en valores hash compactos y fijos.

Certificado digital

Archivo digital que contiene información personal, sobre la identidad de un usuario o entidad final y un par de llaves criptográficas (pública y privada).

Firma electrónica

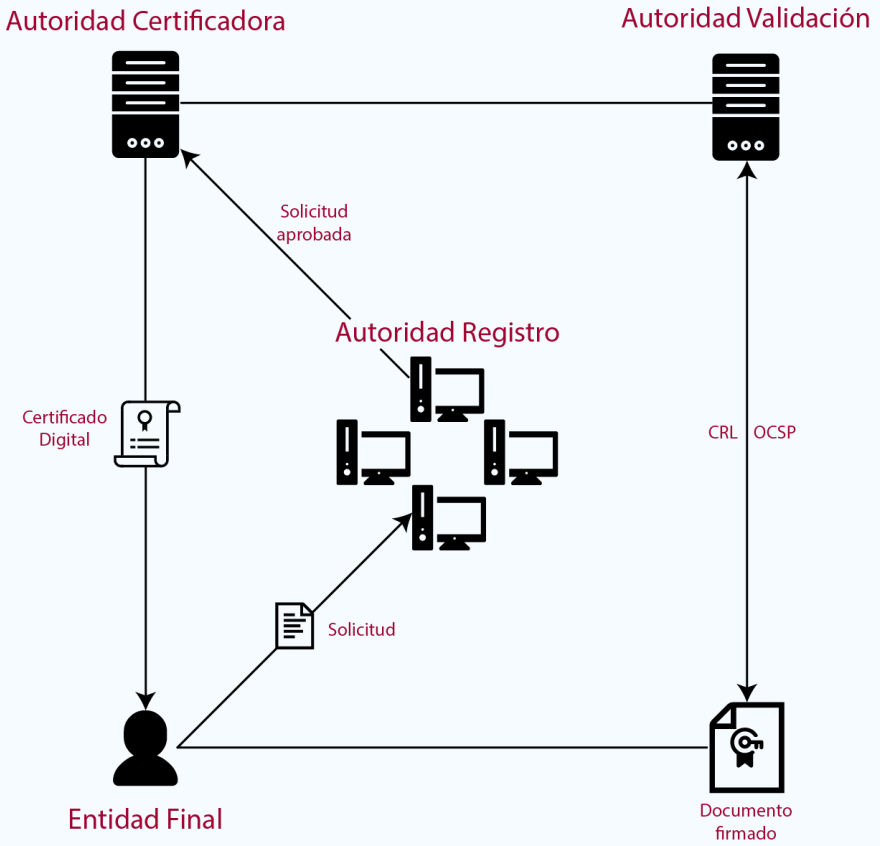
Método tecnológico que reemplaza la firma manuscrita, para firmar documentos a través de medios electrónicos, haciendo uso de un certificado digital.

Infraestructura de Clave Pública (PKI)

Conjunto de tecnologías y estándares que se utilizan para administrar y facilitar el uso de certificados digitales y llaves criptográficas.

Componentes

- Autoridad Certificadora (CA)
- Autoridad Registro (RA)
- Autoridad Validación (VA)
- Entidad Final (EE)
- Certificado digital



Firma electrónica

El funcionamiento de la firma electrónica se basa en el uso de la criptografía.

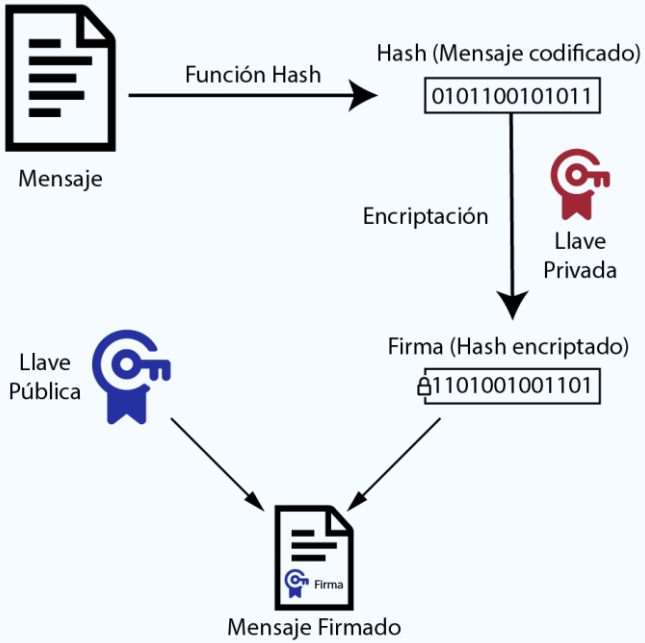
La implementación de la firma electrónica se realiza a través de lo que se conoce como certificado electrónico o certificado digital.

Con la firma electrónica, se crea un método tecnológico que permite garantizar la **autenticidad**, **integridad** y **no repudio** de documentos a través de los medios digitales.

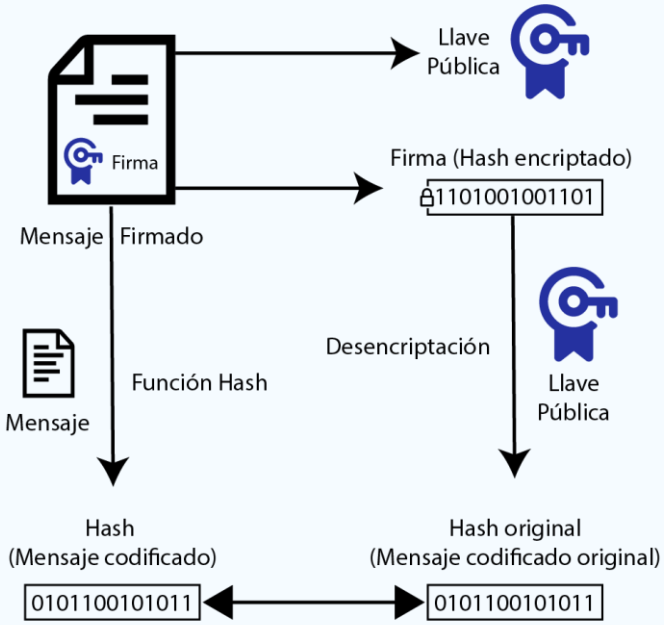
Firma electrónica

Funcionamiento

Firma

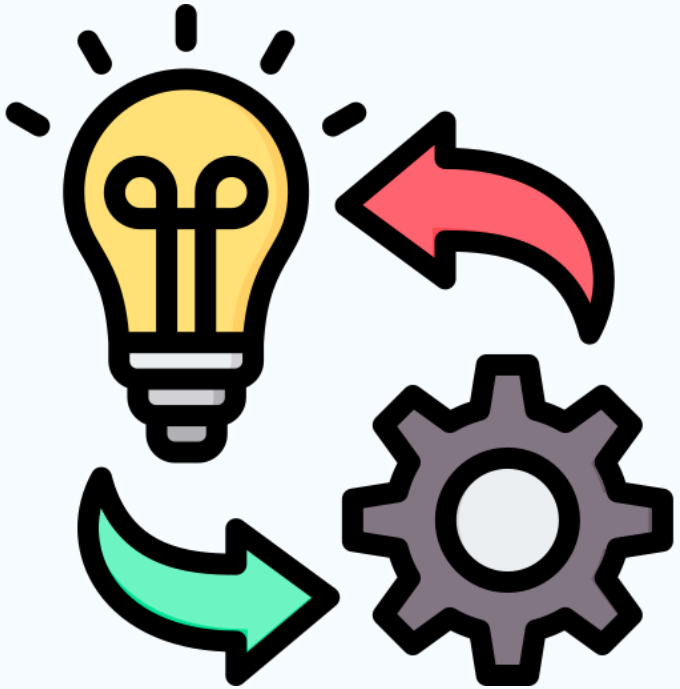


Verificación



03

Implementación



Software

EJBCA

(Enterprise Java Beans Certificate Authority)

- KeyFactor
- Más usado
- Enterprise y **Open Source**
- Multiplataforma (Java)
- Incluye todos los componentes para una PKI

MariaDB

- MySQL
- Versión mejorada de MySQL
- Open Source
- Recomendado por EJBCA

Docker

Instalación-Configuración

MariaDB

```
sudo apt install mariadb-server
sudo systemctl start mariadb.service
sudo systemctl enable mariadb.service

sudo mysql_secure_installation

CREATE USER ejbca IDENTIFIED BY “**********”;
CREATE DATABASE ejbca CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
GRANT ALL PRIVILEGES ON ejbca.* TO ejbca;
FLUSH PRIVILEGES;
```

Instalación-Configuración

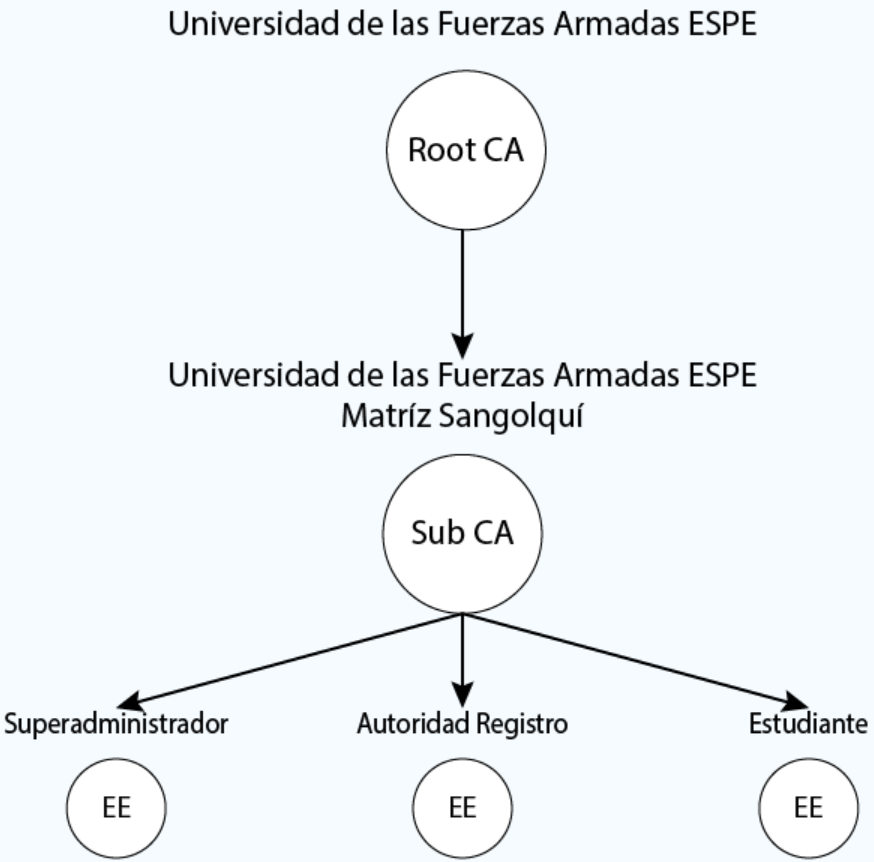
EJBCA

```
sudo docker run -it -d --name espepki -p 80:8080 -p 444:8443 -h 10.9.9.242
-e "DATABASE_JDBC_URL=jdbc:mariadb://10.9.9.243:3306/ejbca"
-e "DATABASE_USER=ejbca"
-e "DATABASE_PASSWORD=***************"
-e "SMTP_DESTINATION=smtp.gmail.com"
-e "SMTP_DESTINATION_PORT=587"
-e "SMTP_FROM=firmadigital@espe.edu.ec"
-e "SMTP_USERNAME=firmadigital@espe.edu.ec"
-e "SMTP_PASSWORD=************"
-e "SMTP_TLS_ENABLED=true"
-e "SMTP_SSL_ENABLED=false"
keyfactor/ejbca-ce
```

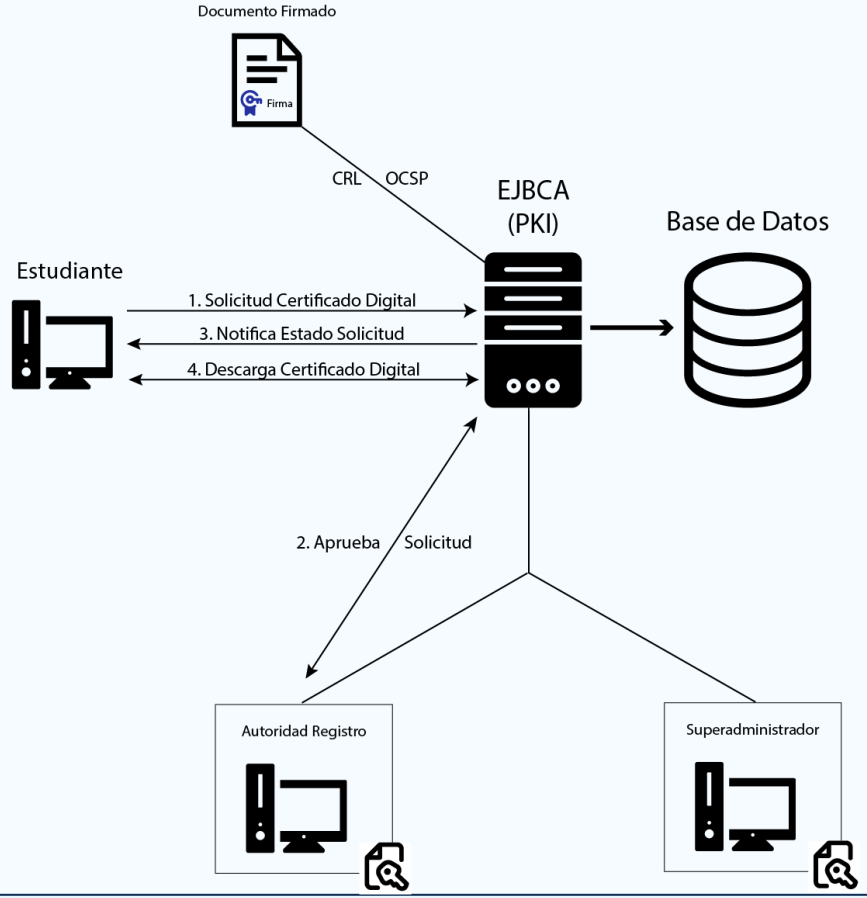
Jerarquía PKI

- Estructura jerárquica que permite mejorar la confianza y organización en la forma en como una PKI emite sus certificados digitales.

- Los niveles superiores, autorizan o certifican a los niveles inferiores, respectivamente.



Arquitectura

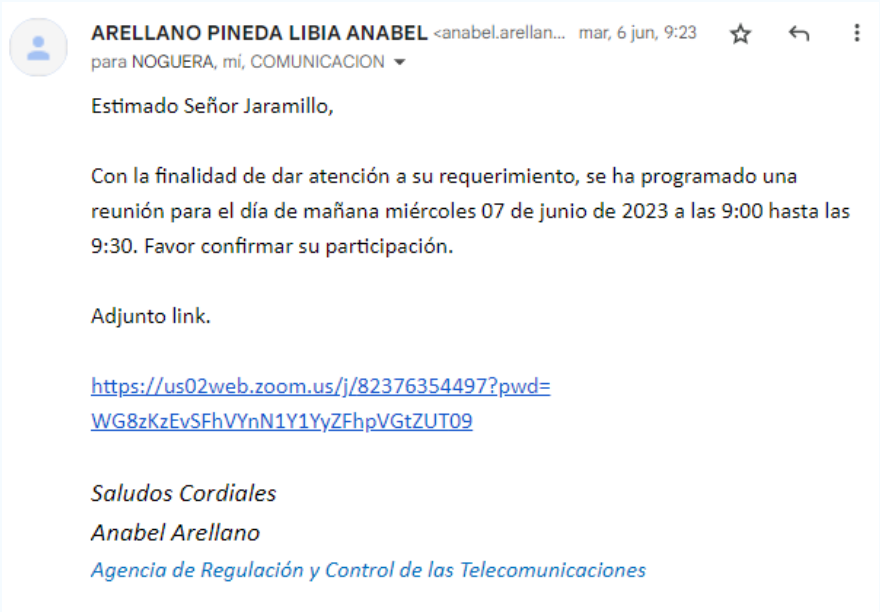


04

Análisis de certificación

Reunión con ARCOTEL

- Visita a ARCOTEL
- Reunión por Zoom



ARELLANO PINEDA LIBIA ANABEL <anabel.arellan... mar, 6 jun, 9:23

para NOGUERA, mí, COMUNICACION

Estimado Señor Jaramillo,

Con la finalidad de dar atención a su requerimiento, se ha programado una reunión para el día de mañana miércoles 07 de junio de 2023 a las 9:00 hasta las 9:30. Favor confirmar su participación.

Adjunto link.

https://us02web.zoom.us/j/82376354497?pwd=WG8zKzEvSFhVYnN1Y1YyZFhpVGtZUT09

Saludos Cordiales

Anabel Arellano

Agencia de Regulación y Control de las Telecomunicaciones

Requerimientos legales

- Solicitud dirigida al Director Ejecutivo de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, detallando nombres y apellidos completos del representante legal, dirección domiciliaria de la empresa unipersonal o compañía.
- Copia de la cédula de ciudadanía del representante legal o pasaporte según corresponda.
- Copia del certificado de votación del último proceso eleccionario (correspondiente al representante legal, excepto cuando se trate de ciudadanos extranjeros)
- 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).
- Información que demuestre la capacidad económica y financiera para la prestación de servicios de certificación de información y servicios relacionados.

Requerimientos técnicos

- Diagrama esquemático y descripción técnica detallada de la infraestructura a ser utilizada, indicando las características técnicas de la misma.

- 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.

- Diagrama técnico detallado de cada "Nodo" o "Sitio Seguro" detallando especificaciones técnicas de los equipos.

- 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**.

Especificación requerimientos técnicos

- Mecanismos de validación: CRL, OCSP
- SSL
- Servicios de emisión, renovación y revocación de certificados digitales
- Roles de administración
- Acceso a servicios desde internet
- Data center
- HSM
- Servidores de respaldo
- IPS
- Firewall
- Balanceadores de carga
- Sistema de control y registro de acceso al centro de computo
- Jerarquía entidad de certificación de información
- Plan de contingencia
- Auditoría de seguridad

Requerimientos económicos

Certificación

$ 22’000.00

Garantía

$ 400’000.00

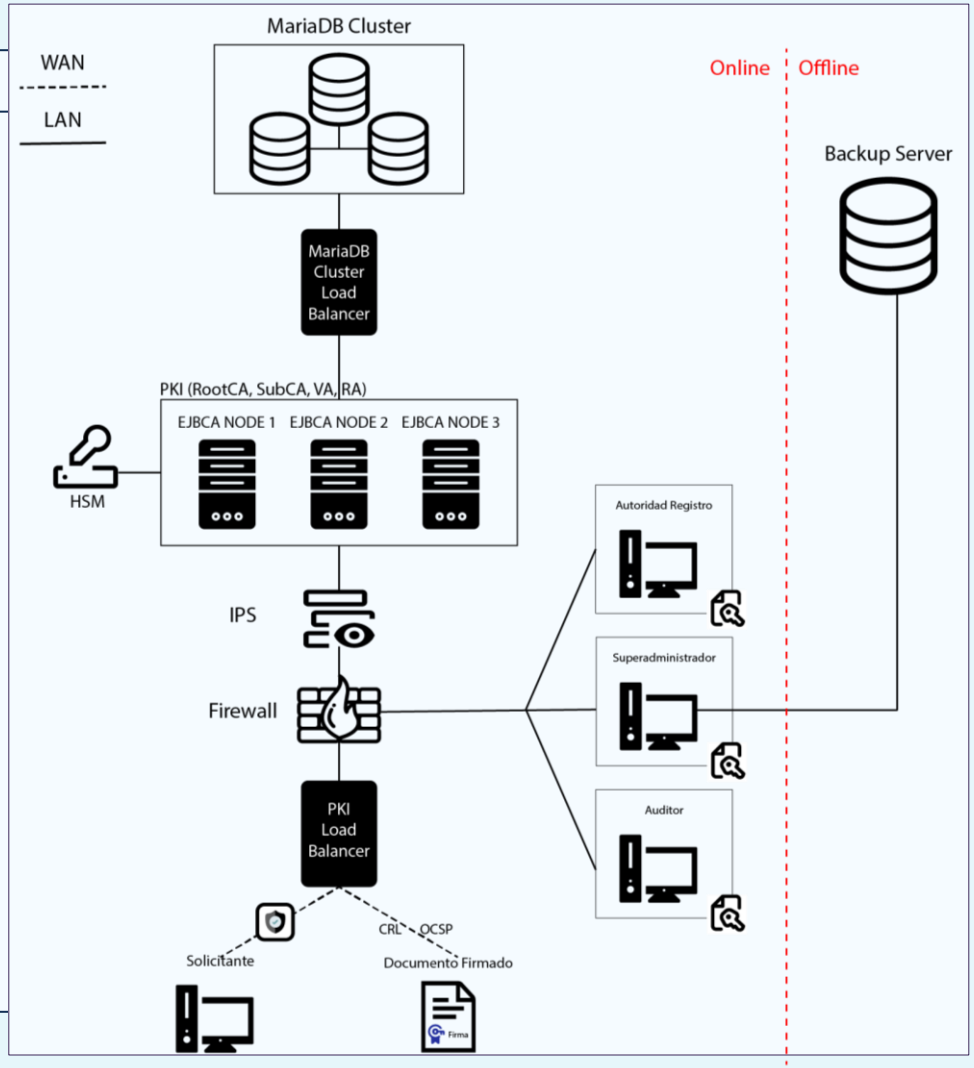
05

Evaluación y mejora

Evaluación de los requerimientos técnicos

- **Mecanismos de validación: CRL, OCSP**
- **SSL**
- **Servicios de emisión, renovación y revocación de certificados digitales**
- **Roles de administración**
- Acceso a servicios desde internet
- Data center
- HSM
- Servidores de respaldo
- IPS
- Firewall
- Balanceadores de carga
- **Centro de cómputo**
- **Sistema de control y registro de acceso al centro de computo**
- **Jerarquía entidad de certificación de información**
- Plan de contingencia
- Auditoría de seguridad

Plan de mejora



06

Conclusiones y recomendaciones

Conclusiones

- Se realizó una nueva implementación mejorada del servicio de firma electrónica en el ESPE CERT del DCCO de la matriz Sangolquí, contemplando una arquitectura y jerarquía de PKI similar a como funcionaría una Entidad de Certificación, con la disponibilidad para prestar el servicio a la comunidad universitaria de esta misma sede y la sede Latacunga. Esta implementación se realizó utilizando únicamente software libre, por lo que adquirir la versión empresarial del software usado, sería opcional en el caso de que se quisiese implementar un servicio mucho más robusto.

- Se realizó un análisis de certificación en el que se determinó los requisitos económicos, legales y técnicos para certificar el servicio de firma electrónica, obteniendo como resultado una pausa en el proceso de certificación, puesto que se necesita una inversión económica grande y una mayor asignación de recursos e infraestructura de TI.

- Se evaluó el servicio de firma electrónica en relación a los requisitos técnicos de certificación, determinando que este no se encuentra listo para obtener la certificación, ya que se requiere que el servicio cuente con altos niveles de seguridad y una mejor distribución de los servicios, para lo cual se necesita una mayor asignación de recursos e infraestructura de TI.

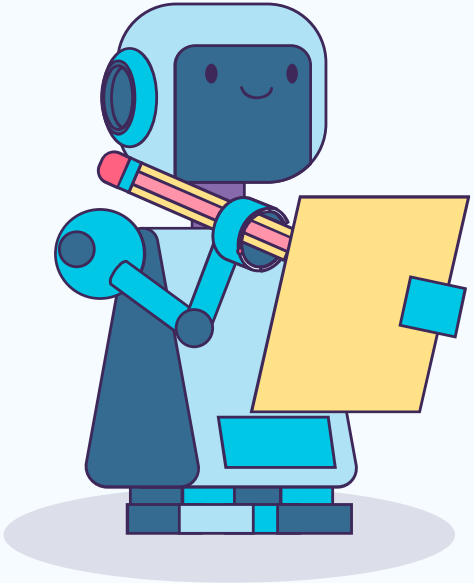
Recomendaciones

- Se pretende extender el servicio de firma electrónica para toda la comunidad universitaria en cada una de las sedes de la ESPE, por lo que se recomienda asignar más recursos e infraestructura de TI para crear un servicio seguro y de alta disponibilidad como se plantea en el plan de mejora.

- En vista de que se debe realizar una inversión económica grande para certificar el servicio de firma electrónica y no se ha podido determinar si se asignarán los recursos económicos en un futuro, se recomienda crear un conjunto de políticas internas y que formen parte del reglamento de la ESPE, en el que se autorice al servicio de firma electrónica implantado en el ESPE CERT, como un medio de legalización y certificación de documentos para tramites dentro de la Universidad.

- El uso de software libre se adapta perfectamente a las necesidades para crear un servicio de firma electrónica para la ESPE, sin embargo, en el caso de requerir características adicionales que se encuentran en la versión empresarial del software, se recomienda realizar un análisis del código fuente del software y determinar si es posible ajustarlo a las necesidades requeridas, puesto que es software libre y se puede modificarlo según se necesite.

Gracias!



Preguntas?

bsjaramillo@espe.edu.ec