DIRECCIÓN DE GESTIÓN POR RESULTADOS

DIGER
DIRECCIÓN DE GESTIÓN POR RESULTADOS

DOCUMENTO DE INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

CÓDIGO	**MAN-PKI-IT-001-2025**
VERSIÓN	**1.0**
FECHA DE APROBACIÓN	**AGOSTO 2025**
APROBADO POR:	**MINISTRO ING. MARCIO SIERRA**

CÓDIGO: MAN-PKI-IT-001-2025			
	DOCUMENTO DE INFRAESTRUCTURA DE CLAVE PÚBLICA		
	Elaborado por: Ing. César Maldonado /Ing. Dennis Vásquez	**Revisado por:** Ing. Henry Ortez / MBA Omar Palacios	**Autorizado por:** Ing. Marcio Sierra Discua
	Fecha de Elaboración 25/06/2025	**Fecha de Revisión** 15/8/2025	**Fecha de Aprobación** 27/8/2025

ACTIVIDAD	NOMBRE	FIRMA
Elaborado por:	César Maldonado Especialista en Infraestructura	
Responsable de Revisión Técnica	Henry Ortez Desarrollador de Sistemas	
	Raúl Aguilar Especialista en Ciberseguridad	
	Dennis Vásquez Jefe de Área de Infraestructura	
Revisión	Omar Palacios Coordinador de AGEHRED	
	Ángel Orlando Paz Coordinador de Sistemas de Gobierno Digital	

VERSIÓN	FECHA	TIPO DE CAMBIO	MODIFICADO POR:	DESCRIPCIÓN DEL CAMBIO
1.0.	27/8/2025	☒NUEVA ☐REVISIÓN ☐MODIFICACIÓN		

TABLA DE CONTENIDO

1. DEFINICIONES

- Documento: Infraestructura de Clave Pública DIGER (PKI)
- **ACS:** (Administrator Card Set / Conjunto de Tarjetas de Administrador. Conjunto de tarjetas inteligentes utilizadas para la administración del Security World en los HSM. Requeridas para operaciones de inicialización, respaldo y restauración del entorno criptográfico.
- **API:** (Application Programming Interface / Interfaz de Programación de Aplicaciones) Conjunto de definiciones y protocolos que permiten la interacción entre aplicaciones y sistemas.
- **Arquitectura Lógica:** Modelo que describe las relaciones funcionales entre los distintos componentes de la PKI.
- **Arquitectura Física:** Modelo que describe la disposición física de los componentes de la infraestructura PKI.
- **Backend:** Zona lógica de la red donde residen los sistemas principales, servidores, NAS y bases de datos.
- Protegido mediante firewall y segmentación de red.
- **CA:** (Certification Authority / Autoridad de Certificación). Entidad responsable de emitir, gestionar y revocar certificados digitales. Puede ser:
- CA Raíz (Root CA): emite certificados para CAs subordinadas.
- CA Subordinada (Sub-CA): emite certificados a usuarios finales.
- **CPD:** (Centro de Procesamiento de Datos). Ubicación física que alberga la infraestructura tecnológica de La DIGER.
- **DPC:** (Declaración de Prácticas de Certificación). Documento que describe las políticas y procedimientos operativos de una CA.
- **DMZ:** (Demilitarized Zone / Zona Desmilitarizada). Segmento de red que separa los sistemas accesibles desde el exterior del resto de la red interna.
- **Data Blob:** Bloque cifrado de datos críticos protegido por el HSM.
- **ECC:** (Elliptic Curve Cryptography / Criptografía de Curvas Elípticas). Criptografía de clave pública basada en curvas elípticas.
- **Entorno Core PKI:** Segmento de la infraestructura que aloja bases de datos, NAS y componentes críticos de la PKI.

- **Entorno DMZ:** Zona expuesta para servicios accesibles desde Internet, como TSA, RA, VA.
- **Firewall:** Dispositivo de red que controla el tráfico entre diferentes zonas de red según reglas predefinidas.
- **Frontend:** Segmento de la infraestructura que expone servicios hacia usuarios o redes externas.
- **HSM:** (Hardware Security Module / Módulo de Seguridad de Hardware). Dispositivo dedicado a la protección y gestión de claves criptográficas.
- **ICMP:** (Internet Control Message Protocol / Protocolo de Mensajes de Control de Internet)
  Protocolo para el intercambio de mensajes de control en la red.
- **MSTP:** (Multiple Spanning Tree Protocol / Protocolo de Árbol de Expansión Múltiple) Protocolo que permite optimizar la redundancia y evitar bucles en redes con múltiples VLANs.
- **NAS:** (Network Attached Storage / Almacenamiento Conectado en Red). Dispositivo de almacenamiento conectado en red.
- **OCS:** (Operator Card Set / Conjunto de Tarjetas de Operador). Conjunto de tarjetas inteligentes utilizadas para la operación normal de los HSM y el acceso a claves protegidas.
- **OCSP:** (Online Certificate Status Protocol / Protocolo de Estado de Certificado en Línea) Protocolo para validar en tiempo real el estado de revocación de un certificado digital.
- **OID:** (Object Identifier / Identificador de Objeto) Identificador único para atributos, políticas o extensiones en certificados digitales.
- **PCIe:** (Peripheral Component Interconnect Express / Interconexión Periférica Express) Interfaz de alta velocidad para la conexión de hardware en servidores.
- **PKCS#11:** (Public-Key Cryptography Standards #11 / Estándar de Criptografía de Clave Pública #11). Estándar de API para la gestión de claves criptográficas en dispositivos HSM.
- **PKI:** (Public Key Infrastructure / Infraestructura de Clave Pública) Conjunto de tecnologías, políticas y procedimientos para emitir, gestionar y revocar certificados digitales.
- **QSCD:** (Qualified Signature Creation Device / Dispositivo de Creación de Firma Cualificada). Dispositivo de creación de firmas cualificadas conforme al reglamento eIDAS.

- **Quórum (ACS y OCS):** Número mínimo de tarjetas ACS u OCS requerido para autorizar determinadas operaciones en los HSM.
- **RA:** (Registration Authority / Autoridad de Registro). Entidad encargada de verificar la identidad de los solicitantes de certificados y gestionar su ciclo de vida.
- **SD-WAN:** (Software-Defined Wide Area Network / Red de Área Amplia Definida por Software). Tecnología para optimizar la gestión de tráfico en redes de área amplia.
- **Security World:** Modelo de gestión unificada de claves en HSM Entrust nShield.
- **Segmentación Física:** Separación física de componentes en distintas redes o segmentos.
- **Segmentación Lógica:** Separación virtual de componentes mediante VLANs, reglas de firewall o contenedores.
- **Servidor de Firma Centralizada:** Servidor equipado con HSM que permite realizar firmas electrónicas avanzadas y longevas.
- **Spanning Tree Protocol:** Protocolo que evita bucles de red en configuraciones redundantes.
- **Srv PROD:** Servidor de Producción.
- **Srv TEST:** Servidor de Pruebas.
- **Subred de Producción:** Segmento de red que conecta los componentes en producción.
- **Subred de Servicios:** Red dedicada a servicios críticos y esenciales de la PKI.
- **Switch:** Dispositivo que conecta múltiples equipos en una red local.
- **TSA:** (Time-Stamping Authority / Autoridad de Sellado de Tiempo). Entidad que emite sellos electrónicos de tiempo con valor legal.
- **TLS v1.3:** (Transport Layer Security Version 1.3 / Seguridad de la Capa de Transporte Versión 1.3). Protocolo de cifrado para comunicaciones seguras.
- **VA:** (Validation Authority / Autoridad de Validación) Sistema que ofrece servicios de validación de certificados digitales.
- **VDOM:** (Virtual Domain / Dominio Virtual). Instancia virtual dentro de un firewall Fortinet que permite dividir su configuración y tráfico en zonas separadas.
- **VLAN:** (Virtual Local Area Network / Red de Área Local Virtual). Segmento lógico de red definido por configuración, independiente de la topología física.
- **VPN:** (Virtual Private Network / Red Privada Virtual). Tecnología para crear conexiones cifradas sobre redes públicas.

2. INTRODUCCIÓN

La Dirección de Gestión por Resultados (DIGER), en su calidad de entidad pública responsable de la prestación de servicios electrónicos de confianza en el marco de la Ley Sobre Firmas Electrónicas de la República de Honduras, ha implementado una Infraestructura de Clave Pública (PKI) con el propósito de garantizar la autenticidad, integridad, confidencialidad y no repudio de los datos y documentos electrónicos generados y gestionados por los distintos actores institucionales.

Este documento presenta una descripción detallada de la arquitectura lógica, funcional, física y de seguridad de la Infraestructura de Clave Pública de La DIGER, sustentada en principios de diseño alineados con estándares internacionales, como ISO/IEC 27001, ETSI EN 319 411-1/2, NIST SP 800-57 y el marco eIDAS de la Unión Europea. Asimismo, incorpora lineamientos específicos de la Declaración de Prácticas de Certificación (DPC) de La DIGER y considera requerimientos de seguridad aplicables a sistemas críticos bajo esquemas de Alta Disponibilidad (HA) y entornos segmentados física y lógicamente.

La PKI de La DIGER está diseñada para operar bajo una arquitectura jerárquica de dos niveles, compuesta por una Autoridad de Certificación Raíz (CA Raíz) y una o más Autoridades de Certificación Subordinadas (Sub-CA), complementadas por servicios de Autoridad de Registro (RA), Autoridad de Validación (VA), Autoridad de Sellado de Tiempo (TSA), y un servidor de firma centralizada. Todo ello desplegado en un entorno seguro, segregado y altamente disponible, alojado en el Centro de Procesamiento de Datos institucional, con controles técnicos y operativos auditables.

El presente documento tiene como finalidad servir de insumo técnico para auditorías, procesos de acreditación, revisiones de cumplimiento normativo y validación de controles técnicos, así como para sustentar la trazabilidad y consistencia del diseño de la infraestructura tecnológica que habilita los servicios de certificación digital prestados por La DIGER.

3. REFERENCIAS NORMATIVAS

- Norma ISO/IEC 27001

4. OBJETIVO Y ALCANCE

El presente documento describe en detalle la arquitectura lógica, funcional y física de la Infraestructura de Clave Pública (PKI) de La DIGER, en su calidad de Prestador de Servicios de Certificación, con el fin de documentar y sustentar su diseño, operación segura y cumplimiento con los requisitos normativos vigentes.

La Infraestructura de Clave Pública (PKI) de La DIGER está conformada por los siguientes componentes principales, en concordancia con el modelo de confianza adoptado:

- Hardware Security Module (HSM): Componente dedicado a almacenar y proteger la llave maestra utilizada en la generación y gestión de todos los pares de claves criptográficas del sistema.
- Autoridad de Certificación (CA): Infraestructura jerárquica de dos niveles compuesta por una CA Raíz (offline), encargada de emitir certificados exclusivamente para las CA Subordinadas, y una o varias CA Subordinadas (Sub-CA), responsables de emitir certificados digitales a entidades finales (usuarios, sistemas, servicios, sellado de tiempo, OCSP).
- Autoridad de Registro (RA): Aplicación de front-end que permite a los operadores gestionar el ciclo de vida completo de los certificados emitidos.
- Autoridad de Validación (VA): Servicio que proporciona información en línea sobre el estado de validez de los certificados.
- Autoridad de Sellado de Tiempo (TSA): Servicio que emite sellos electrónicos de tiempo con validez legal.
- Servidor de Firma Centralizada: Plataforma de tipo enterprise con HSM incorporado que almacena de manera segura las claves privadas de los usuarios finales, permitiendo:
    - Firma electrónica en el lado del servidor.
    - Firma electrónica longeva de documentos electrónicos con valor legal.

- Base de Datos (DB): Sistema que almacena de manera estructurada y segura toda la información generada y administrada por la infraestructura PKI.
- Firewall: Sistema de seguridad de red encargado de supervisar y controlar el tráfico de red conforme a políticas y reglas de seguridad predefinidas.
  La arquitectura de la PKI se encuentra segregada en los siguientes entornos:
- Entorno DMZ: Comprende los sistemas de producción y pruebas accesibles desde el exterior mediante canales controlados.
- Entorno Core PKI: Abarca los sistemas de almacenamiento (NAS) y las bases de datos en el núcleo de la infraestructura.

- Este documento desarrolla a continuación la descripción técnica de cada componente y su interacción dentro de la red PKI. Al finalizar, se incorpora el Anexo 1 que detalla los lineamientos de seguridad aplicados para la operación y gestión de la infraestructura.

5. ARQUITECTURA LÓGICA Y FUNCIONAL

En este apartado se presenta el diagrama general del modelo de la arquitectura en relación con los sistemas de Producción y de Pruebas.

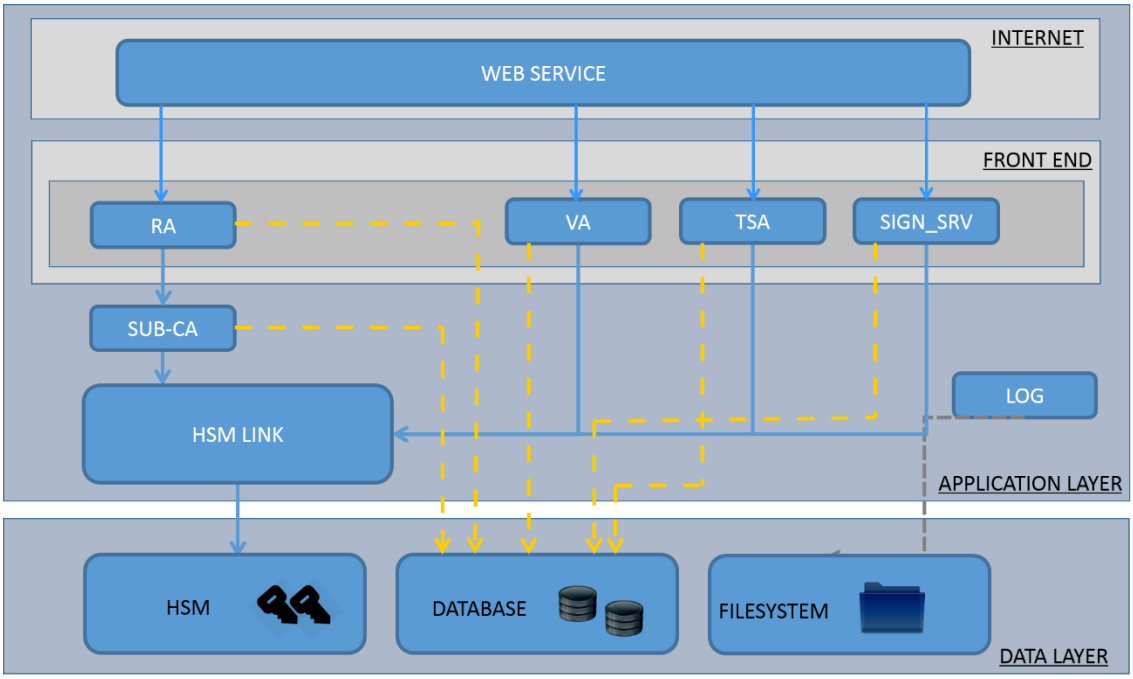


Figura 1 – Arquitectura Lógica y Funcional

- Ubicación y configuración de los entornos de Producción y Pruebas: Los Sistemas de Producción y Pruebas se encuentran alojados en el mismo Centro de Procesamiento de Datos (CPD), pero disponen de conexiones a internet diferenciadas y líneas de energía independientes, garantizando la separación lógica y operativa entre ambos entornos.

- Gestión de registros de actividad: Todos los registros de actividad del sistema son enviados al servicio concentrador de logs. Estos registros se almacenan en el sistema de archivos para su posterior análisis y cumplimiento de los lineamientos de seguridad.
- Acceso a la Autoridad de Registro (RA): La Autoridad de Registro (RA) será accesible a través de su interfaz gráfica (GUI). La gestión del ciclo de vida de los certificados se efectuará mediante una aplicación publicada en internet, que se conecta a la API de la RA para realizar las funciones de revocación, suspensión y reactivación de certificados.

6. ARQUITECTURA TÉCNICA Y ESQUEMA FÍSICO

La Infraestructura de Clave Pública (PKI) de La DIGER está compuesta por diversos nodos tecnológicos distribuidos en el Centro de Procesamiento de Datos Principal (CPD), organizados en dos segmentos lógicos claramente diferenciados, cada uno de los cuales cumple funciones específicas dentro de la PKI.

6.1 DESCRIPCIÓN

6.1.1 COMPONENTES DE LOS ENTORNOS DE PRODUCCIÓN Y DE PRUEBAS

Los entornos de Producción y de Pruebas están diseñados de manera simétrica y cuentan con los mismos componentes de hardware, organizados de acuerdo con la arquitectura técnica de la PKI.

6.1.2 COMPONENTES GENERALES:

- **Autoridad de Certificación Raíz (CA Raíz):** Componente físico operado en modo offline, equipado con un Hardware Security Module (HSM). Su función es emitir certificados exclusivamente para las Autoridades de Certificación Subordinadas (CA Sub).
- **Firewall:** Sistema de seguridad de red que supervisa y controla el tráfico entrante y saliente, conforme a políticas y reglas de seguridad predefinidas.
- **Switches:** En cada entorno se han implementado cuatro switches lógicos —externo (SWE) e interno (SWI)— para asegurar la conectividad segura y segmentada de los diversos componentes.

6.1.3 COMPONENTES EN LOS SERVIDORES DEL ENTORNO DMZ:

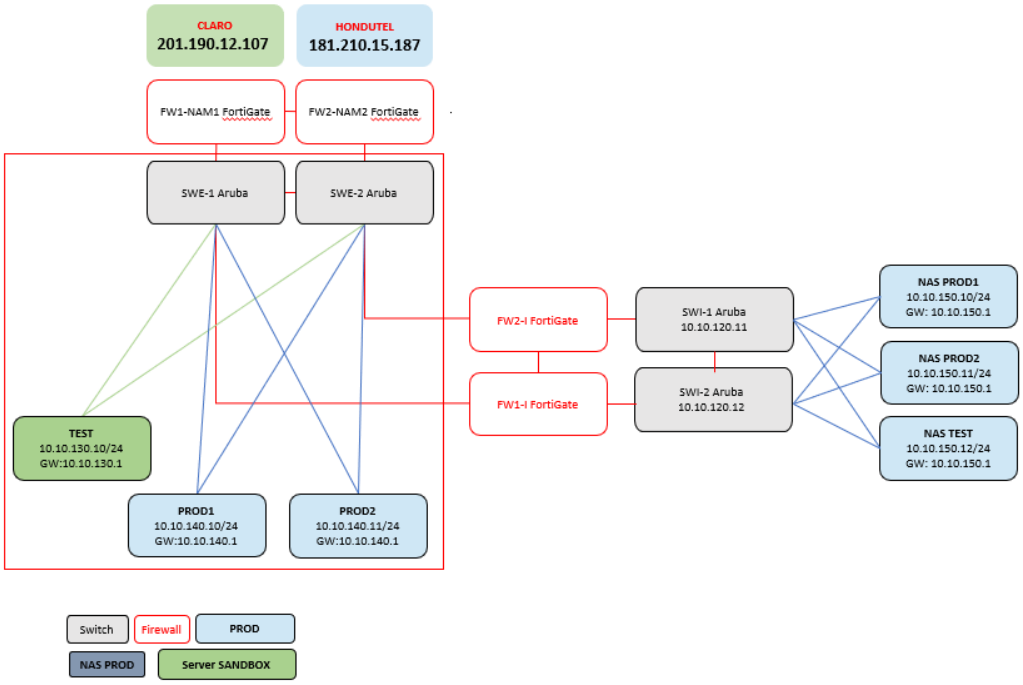
- **Autoridad de Registro (RA - Registration Authority):** Aplicación de front-end de la Autoridad de Certificación que permite a los operadores gestionar el ciclo de vida completo de los certificados digitales.
- **Autoridad de Validación (VA- Validation Authority):** Aplicación que proporciona servicios de validación en línea del estado de los certificados y facilita la gestión de revocación.
- **Autoridad de Certificación Subordinada (CA Sub):** Componente responsable de emitir certificados digitales para entidades finales, incluyendo servicios, organizaciones y usuarios individuales.

- Autoridad de Sellado de Tiempo (TSA- Time-Stamping Authority): Aplicación que emite sellos electrónicos de tiempo, asegurando la validez temporal de transacciones y documentos digitales.
- Hardware Security Module (HSM): Módulo criptográfico dedicado a la generación, protección y gestión de claves criptográficas.
- Servidor de Firma Centralizada: Plataforma de tipo enterprise, equipada con HSM incorporado, que almacena de forma segura las claves privadas de los usuarios. Facilita procesos de firma electrónica avanzada y firma longeva de documentos electrónicos con validez legal.

6.1.4 COMPONENTES EN LOS SERVIDORES DEL ENTORNO CORE PKI:

- NAS (Network Attached Storage): Sistema dedicado de almacenamiento conectado en red (NAS), utilizado para el resguardo seguro de datos críticos de la PKI.
- Base de Datos (DB): Sistema de gestión de base de datos que almacena de manera estructurada toda la información generada y administrada por la infraestructura.

La siguiente figura ilustra la arquitectura física y lógica de la Infraestructura de Clave Pública:



6.1.5 UBICACIÓN DEL CENTRO DE DATOS PKI HONDURAS

La infraestructura de la Infraestructura de Clave Pública (PKI) de la Dirección de Gestión por Resultados (DIGER) se encuentra alojada en el Centro de Procesamiento de Datos (CPD) ubicado en el edificio sede de la DIGER, en Boulevard Fuerzas Armadas, contiguo al Banco Central de Honduras, planta baja, en la ciudad de Tegucigalpa.

El CPD alberga tanto los sistemas de producción como los sistemas de pruebas, los cuales operan bajo medidas de seguridad física, lógica y ambiental diseñadas y documentadas en la correspondiente Declaración de Prácticas de Certificación (DPC) de La DIGER.

El entorno de producción corresponde al ambiente donde se prestan los servicios de certificación y se gestionan los datos de negocio esenciales que sustentan los servicios de confianza ofrecidos por La DIGER como Prestador de Servicios de Certificación (PSC).

Dicho entorno ha sido implementado con una arquitectura en alta disponibilidad (HA), que incluye balanceo de carga, y se compone de dos servidores físicos redundantes y dos sistemas de almacenamiento en red (NAS) con redundancia interna. La infraestructura está segmentada mediante redes dedicadas y configuraciones de seguridad específicas,

garantizando la separación lógica y la protección de los diferentes componentes, en concordancia con los principios de seguridad, transparencia y confidencialidad.

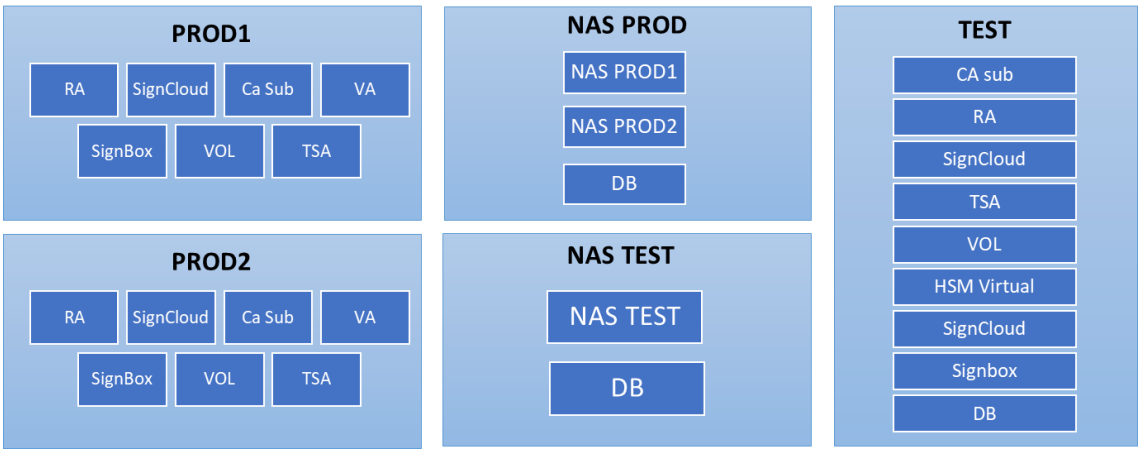


Ilustración 2: Composición de Nodo1

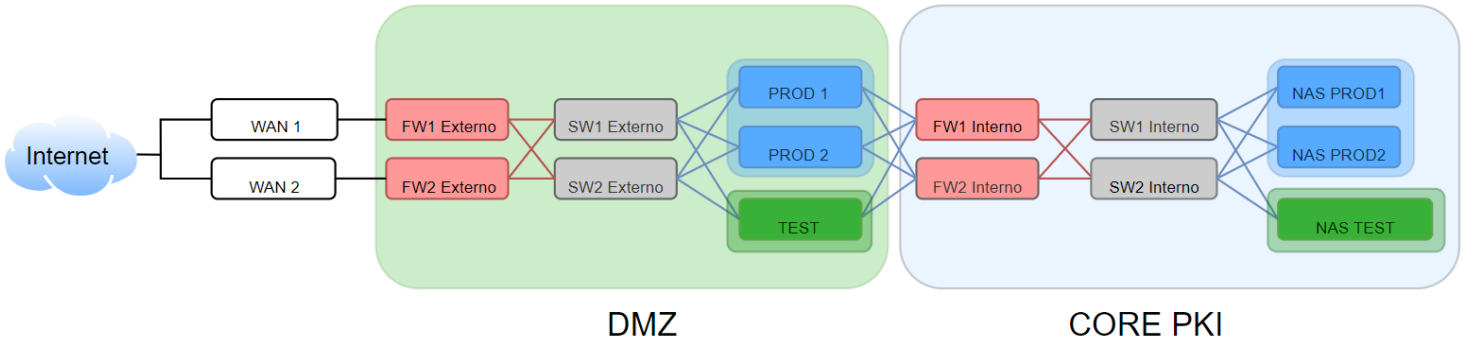


Ilustración 1: Esquema físico infraestructura Diger

7. HARDWARE

La infraestructura de la PKI de La DIGER utiliza como plataforma de cómputo principal dos servidores HP ProLiant DL320 Gen11 y un servidor HP ProLiant DL20 Gen11, seleccionados por su capacidad de procesamiento, densidad, rendimiento y facilidad de gestión en entornos de alta carga y arquitecturas virtualizadas en la nube.

Los servidores están configurados en chasis optimizados, operando bajo el sistema operativo

AlmaLinux OS 9, alineado con los requisitos de seguridad y estabilidad para infraestructuras críticas.

Los dos servidores HP ProLiant DL320 Gen11 están equipados con Hardware Security Modules (HSM) Entrust nShield 5S Base F3, los cuales realizan funciones de generación, protección y gestión segura de claves criptográficas en la infraestructura PKI.

Figura 5: HP Proliant DL320 Gen11 y HP Proliant DL20 Gen11

El Entrust nShield 5S Base F3 es un Hardware Security Module (HSM) de alto nivel de seguridad, diseñado para proteger claves criptográficas y ejecutar operaciones criptográficas críticas en un entorno de hardware resistente a manipulaciones (*tamper-resistant*).

El dispositivo, en formato tarjeta PCIe, permite la realización de operaciones de cifrado, firma electrónica y gestión de claves criptográficas en nombre de múltiples aplicaciones, incluyendo:

- Infraestructuras de Clave Pública (PKI).
- Sistemas de gestión de identidades.
- Cifrado a nivel de aplicación.
- Tokenización.
- Protocolos SSL/TLS.
- Firma de código.

El HSM cumple con los estándares internacionales de seguridad y está integrado en los servidores de la infraestructura PKI de La DIGER, proporcionando un entorno seguro para la generación, almacenamiento y uso de claves criptográficas.

Figura 4: HSM Entrust nShield 5S Base F3

7.1 PLATAFORMA DE LA CA RAÍZ

La Autoridad de Certificación Raíz (CA Raíz) de La DIGER opera en modo offline sobre una plataforma de hardware dedicada, compuesta por un equipo Lenovo ThinkPad Serie E con procesador Intel Celeron N3050 y sistema operativo AlmaLinux OS 9.

El sistema está equipado con un Hardware Security Module (HSM) Entrust nShield Edge F3 USB, el cual es utilizado exclusivamente para la emisión y firma de certificados destinados a las Autoridades de Certificación Subordinadas (CA Sub).

El Entrust nShield Edge F3 USB es un HSM de propósito general, diseñado para entornos de baja frecuencia de operaciones, que proporciona un entorno seguro (*tamper-resistant*) para la generación, almacenamiento y uso de claves criptográficas asociadas a la CA Raíz.

El dispositivo permite la ejecución segura de operaciones criptográficas (cifrado, firma electrónica, administración de claves) y está diseñado específicamente para escenarios como:

- Emisión de certificados para CAs Subordinadas.
- Firma de código.
- Operación de Autoridades de Certificación offline.

El HSM implementa mecanismos avanzados de control de acceso, autenticación multifactor basada en roles, y utiliza políticas de quórum para la autorización de operaciones críticas. Asimismo, automatiza procesos administrativos de alto riesgo y asegura la recuperación segura de claves, garantizando una fuerte separación de funciones dentro del perímetro físico del dispositivo.

Figure 6: Thales HSM nShield Edge USB

7.2 SEGMENTACIÓN DE RED Y ALIMENTACIÓN ELÉCTRICA

Con el fin de garantizar una separación adecuada de los diferentes dominios de red dentro de la infraestructura de la PKI, se emplean dos firewalls físicos Fortinet 100E, configurados en cuatro particiones lógicas (Virtual Domains - VDOMs): dos correspondientes a la zona externa de la red y dos a la zona interna. Esta arquitectura de firewall permite el aislamiento seguro de las distintas zonas operativas de la infraestructura, conforme a los principios de segmentación de red y control de tráfico definido en la política de seguridad.

En lo que respecta a la alimentación eléctrica, la infraestructura de Clave Pública (PKI) de La DIGER cuenta con una configuración redundante, conectada a través de dos Unidades de Alimentación Ininterrumpida (UPS) de 6 kVA cada una. Estas UPS están configuradas en redundancia y a su vez alimentadas por un circuito eléctrico protegido por una planta eléctrica de respaldo, garantizando la continuidad operativa de los sistemas críticos ante fallos en la red eléctrica principal.

La distribución y configuración detallada de las conexiones eléctricas entre los distintos componentes de la infraestructura se encuentran documentadas en el Anexo 1: Diagrama de Fuente Eléctrica.

8. AUTORIDAD DE CERTIFICACIÓN RAÍZ (CA RAÍZ)

La Autoridad de Certificación Raíz (CA Raíz) de La DIGER opera en modo offline y está compuesta por dos equipos dedicados: uno destinado a operaciones regulares de la CA Raíz y otro reservado para el mantenimiento de compatibilidad con sistemas históricos o legados. Estos sistemas tienen como función exclusiva la emisión y firma de certificados para las Autoridades de Certificación Subordinadas (CA Sub), conforme a la jerarquía de confianza establecida en la infraestructura PKI de La DIGER.

A continuación, se presenta un resumen de las especificaciones técnicas de los equipos que componen la plataforma de la CA Raíz:

Model	Lenovo ThinkPad Serie E
Serial Number / Service Tag	PF-599BE4
Processor	Intel Core i5-1235U
Cores / Threads	10 núcleos (2 P-cores + 8 E-cores) / 12 hilos
CPU Frequency	Hasta 4.4 GHz (frecuencia turbo)
Level Cache	12 MB Intel Smart Cache
Power	Adaptador de 65W USB-C / Batería de 45Wh
Memory	8 GB DDR4 3200 MHz
Hard Drive	SSD M.2 NVMe PCIe 512 GB
Interfaces	1x USB-C 3.2 Gen 2 (con carga y DisplayPort), 2x USB-A, HDMI, RJ-45
OS	Alma Linux OS9

A continuación, se presenta un resumen de las especificaciones técnicas del dispositivo Hardware Security Module (HSM) Entrust nShield Edge F3 USB, utilizado en la plataforma de la Autoridad de Certificación Raíz (CA Raíz):

Model	ENTRUST NSHIELD EDGE F3
Serial Number / Service Tag	46-E12200
Application Program Interfaces (APIs)	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI y CNG, nCore, Web Services
Host connectivity	USB 1.x y 2.x (conector Mini USB)
Cryptography	Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160, HMAC, SEED, Triple DES Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit) Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC) including Brainpool and custom curves
Security compliance	NIST SP 800-131A Common Criteria EAL4+ (AVA_VAN.5)
Power	700mW

9. SERVIDORES DE PRODUCCIÓN

A continuación, se presentan las especificaciones técnicas del servidor de producción utilizado en la infraestructura PKI de La DIGER:

Model	HP Proliant DL320 Gen11
Serial Number / Service Tag	CZUD2902WJ CZUD2902WH
Processor	Intel®
Cores / Threads	12 Cores / 24 Threads
Processor speed	3,9 GHz máximo

Level Cache	De 22,50 a 300 MB L3
Power	750 Watt
Memory	2 TB por zócalo, un zócalo solo, al complementarse con memoria DDR5 de 128 GB.
Unit Type	Hasta 8+2 HDD SAS/SATA SFF o SSD SATA/SAS/NVMe U.2 o U.3
OS	Alma Linux OS9

A continuación, se presentan las especificaciones técnicas de los dispositivos Hardware Security Module (HSM) Entrust nShield 5S Base F3, instalados en los servidores de producción que soportan los servicios de la PKI de La DIGER, incluyendo la Autoridad de Certificación Subordinada (CA Sub), la Autoridad de Sellado de Tiempo (TSA), la Autoridad de Validación (VA) y la Autoridad de Registro (RA):

Model	ENTRUST NSHIELD 5S BASE F3
Serial Number / Service Tag	46-U51391 46-U51853
Application Program Interfaces (APIs)	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG
Host connectivity	PCI Express Version 2.0; Solo + connector: 1 lane, Solo XC connector: 4 lane
Cryptography	Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160, HMAC, SEED, Triple DES Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)

	Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC) including Brainpool and custom curves
Security compliance	Common Criteria EAL4+ (AVA_VAN.5) como QSCD
Power	24 Watt

10. SERVIDOR TEST

A continuación, se presentan las especificaciones técnicas del servidor del entorno de pruebas de la infraestructura PKI de La DIGER:

Model	HP Proliant DL20 Gen11
Serial Number / Service Tag	CZ2D29009M
Processor	Intel®
Cores / Threads	12 Cores / 24 Threads
CPU Frequency	3,9 GHz máximo
Level Cache	De 22,50 a 300 MB L3
Power	750 Watt
Memory	2 TB por zócalo, un zócalo solo, al complementarse con memoria DDR5 de 128 GB.
Hard Drive	Hasta 8+2 HDD SAS/SATA SFF o SSD SATA/SAS/NVMe U.2 o U.3

Interfaces	Alma Linux OS9
OS	Intel®

11. NAS PRODUCCIÓN, NAS TEST

A continuación, se presentan las especificaciones técnicas de los sistemas Network Attached Storage (NAS) Synology R1619xs+ desplegados en la infraestructura PKI de La DIGER, configurados de la siguiente manera:

- 2 unidades NAS Synology R1619xs+ destinadas al almacenamiento de backups y de la base de datos en el entorno de producción.
- 1 unidad NAS Synology R1619xs+ dedicada al almacenamiento en el entorno de pruebas.

Model	3 NAS Synology R1619xs+
Storage SAS	RAID 5 4 discos SATA de 4TB 7.2K RPM Almacenamiento disponible de 12TB
Storage NL-SAS	RAID 6 4 discos SATA de 4TB 7.2K RPM Almacenamiento disponible de 8TB

12. FIREWALL

A continuación, se describen las características y la segmentación de los dispositivos Firewall Fortinet 100E, utilizados en la infraestructura PKI de La DIGER.

Los firewalls Fortinet 100E están configurados para operar con dos instancias virtuales (Virtual Domains- VDOM), estableciendo una segmentación lógica que permite separar los flujos de tráfico de red, de acuerdo con los siguientes dominios:

VDOM Externo: Responsable de gestionar el tráfico proveniente de la zona pública y de la conexión con los switches externos.

VDOM Interno: Responsable de la gestión del tráfico interno, incluyendo la comunicación entre los servidores, los sistemas NAS y los switches internos.

Ambos VDOM están configurados con políticas de firewall estrictas y filtros de acceso definidos, asegurando un aislamiento seguro entre las distintas zonas de red.

13. SWITCHES

A continuación, se presentan las características de los switches de red Aruba IOn 1930 implementados en la infraestructura PKI de La DIGER, cuya función es proveer conectividad de red segura y segmentada entre los distintos componentes del sistema.

La configuración de switches es la siguiente:

- Zona Externa (DMZ): 2 switches Aruba IOn 1930, dedicados a la conectividad de los componentes en la zona DMZ, incluyendo los servidores de producción (PROD 1, PROD 2) y el servidor de pruebas.
- Zona Interna (Backend): 2 switches Aruba IOn 1930, dedicados a la conectividad interna entre los sistemas centrales de la PKI (Core PKI), específicamente los sistemas NAS de producción y de pruebas.

14. ESQUEMA DEL MUNDO DE SEGURIDAD

La arquitectura del Security World implementada en la infraestructura PKI de La DIGER ha sido diseñada para garantizar altos niveles de seguridad, disponibilidad y capacidad de recuperación en la gestión de claves criptográficas.

El diseño establece un modelo de operación con:

- Un Hardware Security Module (HSM) independiente para la Autoridad de Certificación Raíz (CA Raíz).
- Un HSM dedicado por cada Autoridad de Certificación Subordinada (CA Sub) y para las aplicaciones asociadas (TSA, VA, RA, Servidor de Firma Centralizada).

Los dispositivos Entrust nShield 5S Base F3 operan sobre la arquitectura Security World, que proporciona una administración unificada y garantiza la interoperabilidad entre múltiples HSM desplegados en el mismo entorno.

Durante la inicialización de los HSM, se establece la asociación lógica y la vinculación de confianza entre los dispositivos desplegados en el mismo entorno Security World, lo cual permite la creación y distribución de un conjunto de claves de infraestructura comunes, esenciales para la operación resiliente y la recuperación segura del sistema.

Estas claves de infraestructura son resguardadas de manera segura mediante un conjunto de tarjetas inteligentes denominado Administrator Card Set (ACS), gestionado bajo políticas de control de acceso con quórum.

En la infraestructura PKI de La DIGER se han definido dos entornos independientes de Security World:

- Uno dedicado a los sistemas de la CA Raíz.
- Otro utilizado por los sistemas de las CA Subordinadas.

Este diseño establece límites de administración claros y separados para cada tipo de CA (CA Raíz y CA Sub).

En el entorno de pruebas se utiliza un HSM virtual, configurado con el objetivo de facilitar la manejabilidad y la ejecución controlada de los casos de prueba definidos, sin comprometer la integridad de los Security World de producción.

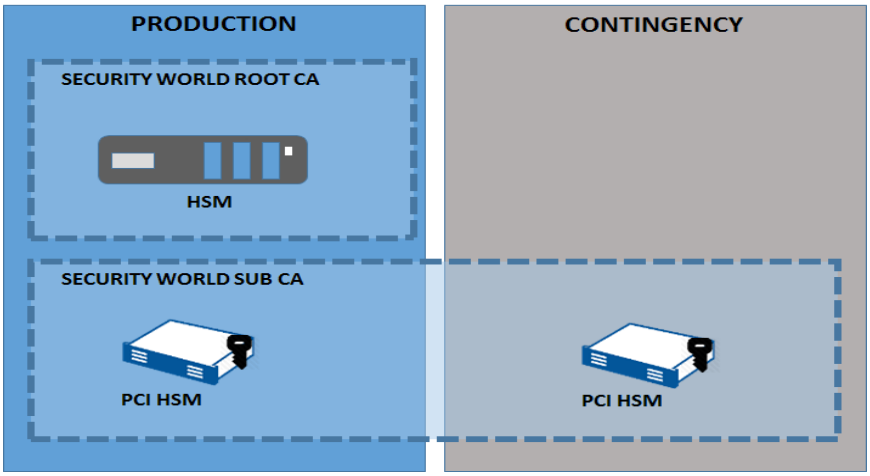


Figura 6- HSM Distribution

Uso de Tarjetas ACS / OCS y Quórum

Para alcanzar altos niveles de seguridad y control operativo, la arquitectura de la infraestructura PKI de La DIGER implementa un sistema de tarjetas inteligentes que habilita el uso de mecanismos de quórum para la autorización de operaciones sensibles en los Hardware Security Modules (HSM).

El conjunto de tarjetas de administración, denominado Administrator Card Set (ACS), soporta un modelo de quórum, en el cual se requiere un número mínimo de tarjetas (m) de un total configurado (n), utilizadas de manera conjunta, para autorizar operaciones críticas tales como la inicialización de un nuevo Security World, la recuperación de claves de infraestructura o la modificación de parámetros clave de seguridad.

Cada tarjeta ACS está protegida por un PIN, que debe ser autenticado en cada uso.
Los parámetros de configuración definidos para los sistemas de La DIGER son los siguientes:

CA Raíz:

- Número total de ACS: 6
- Quórum mínimo requerido: 3

CA Subordinada:

- Número total de ACS: 6

- Quórum mínimo requerido: 3

El uso del quórum de tarjetas ACS es requisito indispensable para la creación e inicialización de un nuevo Security World, así como para la recuperación de claves de infraestructura en caso de contingencia.
El funcionamiento operativo regular de los HSM está basado, adicionalmente, en un segundo conjunto de tarjetas inteligentes denominado Operator Card Set (OCS).

El conjunto OCS es generado durante la inicialización de los HSM, y tiene un propósito específico: habilitar la operación de descifrado de los Encrypted Data Blobs (blobs de datos cifrados) almacenados externamente en la base de datos asociada al HSM.
Cada tarjeta OCS está igualmente protegida por un PIN, y contiene credenciales necesarias para habilitar el uso interno de claves privadas dentro del perímetro seguro del HSM. Las claves privadas correspondientes permanecen cifradas mediante la clave maestra (Master Key) del HSM, de modo que todo descifrado de datos ocurre exclusivamente dentro del hardware del HSM, sin posibilidad de extracción de las claves a un entorno externo.

Este diseño garantiza un modelo de control de acceso fuerte, con separación de funciones, y asegura la integridad y confidencialidad de las claves críticas de la infraestructura PKI.

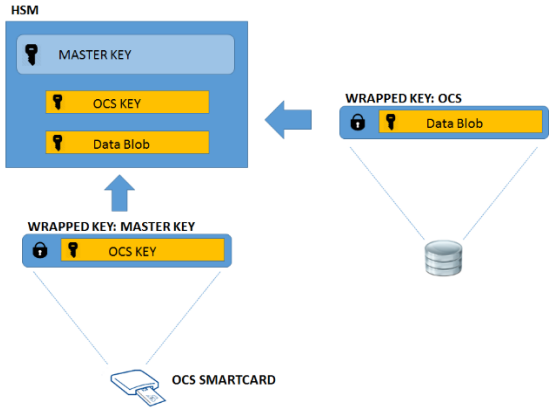


Figura 7 – Proceso de Protección del Data Blob

De acuerdo con el diseño de seguridad de la infraestructura PKI de La DIGER, la arquitectura del Security World y el uso de tarjetas inteligentes siguen dos principios fundamentales para la protección del entorno HSM:

- Toda clave está protegida mediante un sistema de claves jerárquico (protección en capas), de modo que cada clave se encuentra cifrada por otra clave.
- Ninguna clave en texto claro es exportada fuera del HSM; todas las operaciones criptográficas se realizan dentro del perímetro seguro del HSM.

  Adicionalmente, el conjunto de tarjetas Operator Card Set (OCS) implementa igualmente un mecanismo de control por quórum, conforme a las siguientes configuraciones:

CA Raíz:

- Número total de OCS: 6
- Quórum mínimo requerido: 1

CA Subordinada:

- Número total de OCS: 6
- Quórum mínimo requerido: 3

A continuación, se presentan las especificaciones de configuración de los dispositivos Hardware Security Module (HSM) Entrust nShield 5S Base F3 desplegados en el entorno de producción de la infraestructura PKI de La DIGER.

La siguiente tabla detalla, por entorno, el número de dispositivos HSM, el modelo, la configuración de tarjetas ACS y OCS, y su asociación al correspondiente Security World:

Entorno	Cantidad	Modelo	Number of ACS\QUORUM	Number of OCS\QUORUM	Security World
Producción 1	1	ENTRUST NSHIELD 5S BASE F3	3/6	1/6	CA Sub-Security World
Producción 2	1	ENTRUST NSHIELD 5S BASE F3	3/6	1/6	CA Sub-Security World

15. ANEXO 1- REQUERIMIENTOS DE SEGURIDAD

15.1 PROTECCIÓN Y DESCRIPCIÓN DE LOS CABLES DE LA PKI DE LA DIGER

La DIGER ha definido la arquitectura de interconexiones físicas de su infraestructura PKI, asegurando un cableado estructurado ordenado y debidamente protegido, tanto para la red de comunicaciones como para las conexiones de alimentación eléctrica que soportan el funcionamiento de los sistemas.

El diseño y gestión del cableado se realiza conforme a las buenas prácticas de seguridad física, asegurando la identificación, trazabilidad y segregación adecuada de los distintos tipos de conexión dentro del Centro de Procesamiento de Datos (CPD).

15.2 CABLEADO DE RED DE LA PKI DE LA DIGER

El cableado estructurado de red que interconecta los distintos componentes de la Infraestructura de Clave Pública (PKI) de La DIGER ha sido diseñado, implementado y documentado conforme a las buenas prácticas de seguridad de red.

Se ha elaborado un mapa de red formal que documenta las interconexiones físicas y lógicas entre los componentes que conforman la infraestructura PKI.

Dicho diseño se presenta en el siguiente diagrama de red, que forma parte de esta documentación:

Switch	Serie	Hostname	Puerto Switch	Hacia Dispositivo Final	Tipo de Puerto
Aruba InstanOn 1930	TW46LNT2PH	SW01-INTERNO	1	NAS-PROD1 (NIC1)	Ethernet 1G
			2	NAS-PROD2 (NIC1)	Ethernet 1G
			3	NAS-TEST (NIC1)	Ethernet 1G
			22	FORTINET01-Pto	Ethernet 1G
			23	LACP - SW02-INTERNO	DAC 1G
			24	LACP - SW02-INTERNO	DAC 1G
	TW46LNT2VJ	SW02-INTERNO	1	NAS-PROD1 (NIC2)	Ethernet 1G
			2	NAS-PROD2 (NIC2)	Ethernet 1G
			3	NAS-TEST (NIC2)	Ethernet 1G
			22	FORTINET02-Pto	Ethernet 1G
			23	LACP - SW01-INTERNO	DAC 1G
			24	LACP - SW01-INTERNO	DAC 1G
Aruba InstanOn 1930	TW46LNT2VV	SW01-EXTERNO	1	DMZ-PROD1 (NIC1)	Ethernet 1G
			2	DMZ-PROD2 (NIC1)	Ethernet 1G
			3	DMZ-TEST (NIC1)	Ethernet 1G
			4	DMZ-PROD1 (ILO)	Ethernet 1G
			22	FORTINET01-Pto	Ethernet 1G
			23	LACP - SW02-EXTERNO	DAC 1G
			24	LACP - SW02-EXTERNO	DAC 1G
	TW46LNT285	SW02-EXTERNO	1	DMZ-PROD1 (NIC2)	Ethernet 1G
			2	DMZ-PROD2 (NIC2)	Ethernet 1G
			3	DMZ-TEST (NIC2)	Ethernet 1G
			4	DMZ-PROD2 (ILO)	Ethernet 1G
			22	FORTINET02-Pto	Ethernet 1G
			23	LACP - SW01-EXTERNO	DAC 1G
			24	LACP - SW01-EXTERNO	DAC 1G

15.3 CABLEADO ELÉCTRICO DE LA PKI DE LA DIGER

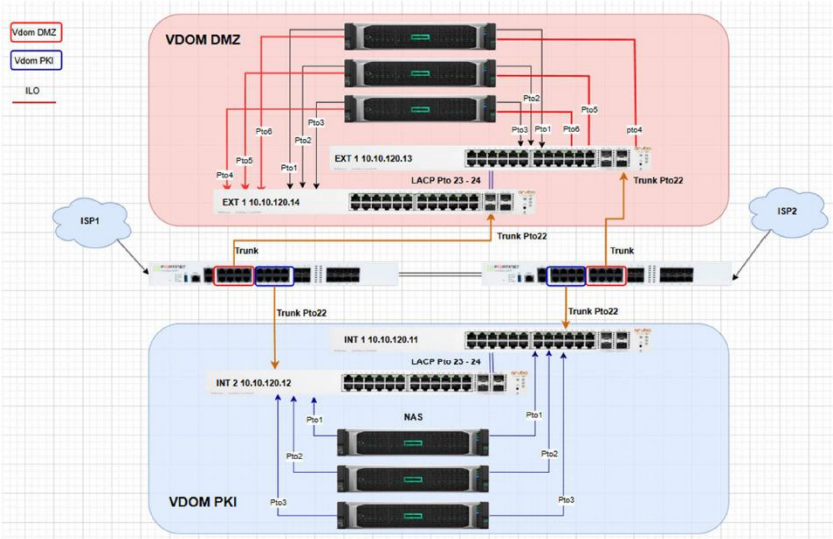
La Infraestructura de Clave Pública (PKI) de la Dirección de Gestión por Resultados (DIGER) cuenta con una configuración de alimentación eléctrica redundante, provista a través de dos UPSs independientes, suministradas por el Centro de Procesamiento de Datos (CPD) que alberga la infraestructura.

Este diseño garantiza la continuidad operativa de los sistemas críticos de la PKI en caso de incidentes o fallos en cualquiera de las fuentes eléctricas primarias.

El sistema de alimentación ha sido configurado para distribuir la energía entre los distintos componentes de la infraestructura PKI, conforme al diseño establecido en el diagrama de fuente eléctrica que se presenta a continuación:

UPS 1/ PDU A (Conector)	Componente Funcional de la PKI	UPS 2/ PDU B (Conector)
P1	SW01- INTERNO	
	SW02- INTERNO	P1
P2	SW01- EXTERNO	
	SW02- EXTERNO	P2
P3	FORTIGATE 100F A	P3
P4	FORTIGATE 100F B	P4
P5	DMZ-TEST	P5
P6	DMZ-PROD1	P6
P7	DMZ-PROD2	P7
P8	NAS-PROD1	P8
P9	NAS-PROD2	P9
P10	NAS-TEST	P10

15.4 SEGURIDAD DE RED DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA DE LA DIGER



15.5 SEGMENTACIÓN FÍSICA Y LÓGICA DE LA PKI DE DIGER

- **Subred de Servicios:** utilizada para la comunicación de servicios esenciales.
- **Subred para Firewalls y Switches:** destinada a la gestión y comunicación segura de los dispositivos de red.
- **Subred para Servidores y NAS de Producción:** conecta los servidores en configuración redundante y los dispositivos de almacenamiento.
- **Subred para Servidor y NAS de Pruebas:** asegura el aislamiento del entorno de pruebas respecto al entorno de producción.

La Infraestructura de Clave Pública (PKI) de La DIGER, que soporta la prestación de los servicios de confianza, se estructura en dos áreas lógicas principales: Frontend y Backend.

De acuerdo con la arquitectura definida, la zona física Backend, que alberga los sistemas principales de la PKI, permite aislar los componentes críticos mediante el uso de subredes Docker dedicadas, separadas e independientes.

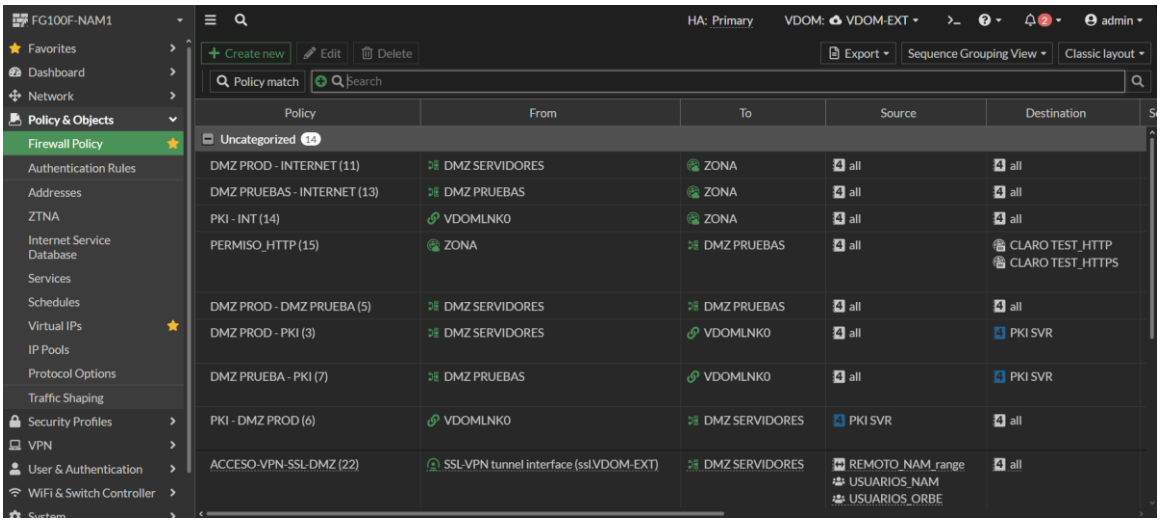
Los principales componentes de la PKI se alojan en estas redes dedicadas, y, gracias a la configuración de las políticas de cortafuegos, únicamente se expone el puerto 443, protegido

con cifrado TLS v1.3 y autenticación mutua (cliente y servidor), requerido para el funcionamiento de los servicios de confianza (TSP – Trusted Service Provider).

Este enfoque de segmentación impide que los componentes de un servicio puedan comunicarse con los de otro, al estar alojados en segmentos de red virtual completamente separados. Las políticas de cortafuegos permiten exclusivamente la comunicación cifrada a través del puerto indicado, en la red física del Backend.

El único puerto expuesto en la red física del Backend está protegido mediante protocolo TLS v1.3 con autenticación mutua, garantizando que solo los componentes autorizados, provistos del correspondiente certificado de autenticación, pueden establecer comunicación segura.

15.6 REGLAS EXTERNAS



15.7 REGLAS INTERNAS

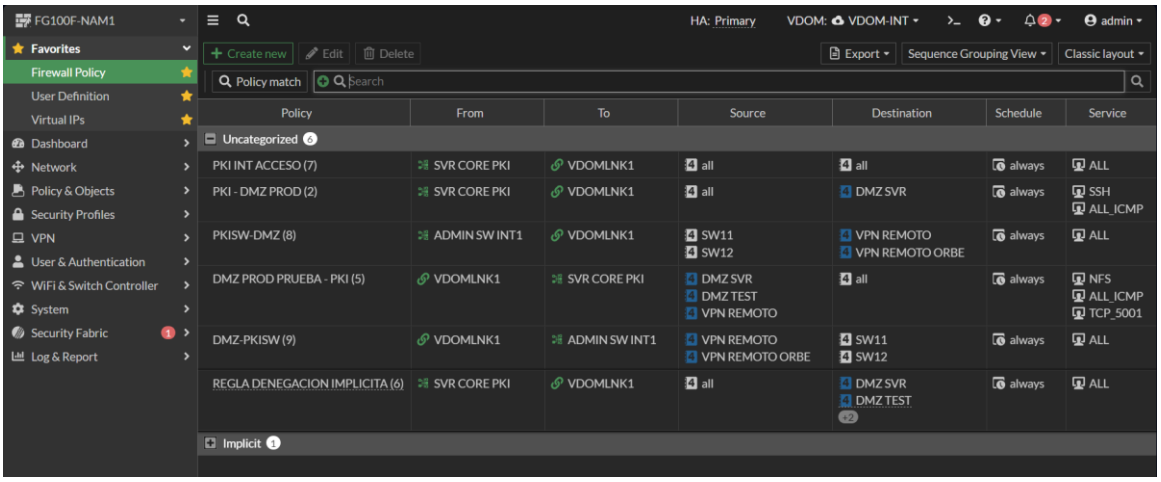


Figura 8 - configuración de las políticas del firewall respecto a la comunicación desde el Frontend al Backend.

La segmentación también se aplica al nivel de los archivos de datos: todos los archivos se crean utilizando cuentas de usuario dedicadas, y los procesos Docker se ejecutan mediante cuentas de sistema específicas.

Esta configuración impide cualquier acceso o interacción entre procesos (incluyendo sockets, pipes o archivos) de un servicio a otro.

El aislamiento de las redes Docker, en conjunto con la asignación de puertos dedicados por contenedor, garantiza que los sistemas críticos de la operación de la PKI se mantengan confinados en un entorno seguro y segregado.

15.8 CONFIGURACIÓN DE FIREWALL FORTINET 100F

El firewall Fortinet 100E implementado en la infraestructura PKI de La DIGER está configurado para optimizar la seguridad de red, garantizar la disponibilidad y habilitar una segmentación lógica robusta entre las distintas zonas operativas.

Las configuraciones implementadas son las siguientes:

SD-WAN:

- Activación y configuración de SD-WAN para optimización dinámica del tráfico hacia Internet.

- Uso de dos interfaces WAN conectadas a dos proveedores de servicios de Internet (ISP) distintos, para balanceo de carga y redundancia.
- Definición de políticas de enrutamiento dinámico que garantizan la selección de la mejor ruta en función del rendimiento y latencia de cada enlace.

Segmentación en VDOMs:

- Creación de instancias virtuales (Virtual Domains - VDOM) para separar zonas externas e internas.
- Aplicación de políticas diferenciadas para cada VDOM, asegurando aislamiento y control de acceso entre dominios.

Políticas de Seguridad:

- Implementación de reglas estrictas de entrada y salida entre los VDOM.
- Configuración de inspección profunda de paquetes (DPI) para tráfico crítico.
- Definición de listas de control de acceso (ACL) para limitar las conexiones entrantes y salientes.

Alta Disponibilidad (HA):

- Configuración del firewall en modo activo-pasivo, habilitando failover automático en caso de falla de uno de los nodos, conforme a las buenas prácticas de alta disponibilidad.

VPN y Acceso Remoto.

Creación de tres grupos de acceso VPN:

- Administradores de Infraestructura: Acceso completo a todos los dispositivos y servidores para administración y monitoreo.
- Partner de Soporte: Acceso restringido únicamente a los firewalls Fortinet, sin posibilidad de conexión a servidores u otros dispositivos de la red.
- Grupo de Auditoría: Acceso controlado a registros y herramientas de monitoreo, sin permisos de modificación en dispositivos críticos.

Aplicación de reglas de firewall específicas para garantizar la segmentación de cada grupo y evitar accesos no autorizados.

- Configuración de VPN SSL para acceso seguro de administradores.
- Control de acceso basado en roles para usuarios y dispositivos.

15.9 REGLAS DE FIREWALL

Regla	Origen	Destino	Puerto/Servicio	Acción
1	Zona Administrativa	Firewall/Switches	SSH (22), HTTPS (443), http NAS (5000), https NAS (5001)	Permitir
2	Servidores Producción	NAS Producción	NFS (2049)	Permitir
3	Servidores Producción	Internet	Salida HTTP/HTTPS 80/443	Permitir
4	Usuarios Internos	Servidores Producción	SSH (22)	Permitir
5	Servidor de Pruebas	NAS de Pruebas	NFS (2049),	Permitir
6	Zona Externa	Zona Interna	Cualquier puerto	Denegar
7	Todo	Todo	ICMP	Denegar

15.10 CONFIGURACIÓN DE SWITCHES ARUBA ION 1930

- Segmentación con VLANs:
  - VLAN 120: Firewalls/Switches
  - VLAN 130: DMZ Pruebas
  - VLAN 140: DMZ PROD
  - VLAN 150: PKI NAS
  - VLAN 160: VPN
- Spanning Tree Protocol (STP):
  - Implementación de Multiple Spanning Tree Protocol (MSTP) para optimizar el uso de los enlaces y reducir la sobrecarga de STP.
  - Configuración de instancias de MSTP:
    - Instancia 1: VLAN de Administración y Firewalls.
    - Instancia 2: VLANs de DMZ y Backend.
  - Establecimiento de prioridades adecuadas para definir el root bridge y evitar cambios innecesarios en la topología de red.
- Configuración de QoS (Calidad de Servicio):

- Priorización de tráfico crítico, como comunicaciones PKI y sincronización de NAS.

- Seguridad Adicional:
  - Port Security: Restricción de direcciones MAC en puertos críticos.
  - Des-habilitación de puertos no utilizados para reducir vectores de ataque.