Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Certificación Centralizada

Autor: Ing. Esp. Matías Román Vazquez Hess

Director de la Tesis: Ing. Pagola Hugo

Año de Presentación: 2019

Cohorte: 2014

Declaración Jurada de Origen de los Contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firma: [FIRMADO]
Nombres y Apellidos: Matías Román Vazquez Hess
DNI: 30.406.007

Resumen

Un certificado digital, es un archivo firmado electrónicamente por un tercero, considerado como una autoridad para el tipo de contenido vinculado en este, de forma de confirmar la identidad del firmante. De acuerdo a su propósito, la información contenida en un certificado identificara su tipo.

Ahora bien, cada día, es mayor la multiplicidad e interrelación que se presenta entre certificados e individuos, ya sean físicos o humanos dentro de las organizaciones. Lo que hace que la proliferación de estos es cada vez más común, pero no así los procesos o servicios que funcionan con estos y mucho menos su gestión, por las particularidades de cada escenario y la falta de conocimiento y expertise que implica ello.

Para reducir la probabilidad de tiempo indisponible, mediante una gestión completa y proactiva, brindando una herramienta concreta, tanto en la actualidad como en un futuro inmediato, de acuerdo a su disponibilidad, se plantea un enfoque práctico, abarcativo y sencillo, permitiendo la información necesaria para la toma de decisiones correspondiente, minimizando el conocimiento específico necesario para cada escenario particular; contribuyendo a solucionar un enorme problema presente en las organizaciones con necesidades diarias de operar utilizando certificados digitales con diversos fines, al más bajo costo y sin la necesidad de contar con personal específico para ello, en el menor tiempo posible, minimizando los riesgos y resguardando al máximo la información electrónica a operar.

Palabras clave: Certificados Digitales, Gestión, Gestión de certificados digitales, Open Source, bajo costo.

Índice

Prólogo vi
Nómina de abreviaturas y acrónimos vii
1. Cuerpo introductorio 1
1.1. Introducción 1
1.2. Objetivos 2
1.3. Alcance 2
1.4. Hipótesis 2
2. Cuerpo principal 3
2.1. Certificados Digitales 3
2.2. Gestión de certificados digitales 4
2.3. Escenarios de autenticación 5
2.4. Tipos de certificados 5
2.5. Estructura estándar de Certificados 5
2.6. Especificaciones del modelo 8
2.6.1. Denominación 8
2.6.2. Arquitectura 9
2.6.3. Diagrama de flujo de procesos 9
2.7. Diseño del prototipo experimental implementado 14
2.7.1. Limitaciones 14
2.7.2. Pruebas de concepto 14
2.7.3. Prerrequisitos 14
2.7.3.1. Requisitos de software 15
2.7.3.2. Requisitos de hardware 15
2.7.4. Operación 15
2.8. Casos de prueba 19
2.8.1. Entorno inicial de CA 19
2.8.1.1. Instalación 19
2.8.1.2. Pre requisitos 20
2.8.1.3. Inicio 21
2.8.1.4. Archivo de configuración global 21
2.8.1.5. Log 23
2.8.1.6. Creación de CA 24
2.8.1.7. Configuración de CA 29
2.8.1.8. Creación de clave cC CA 30
2.8.1.9. Denuncia de vínculo remoto 31
2.8.1.10. Despliegue de cC Sub-CA | RA 34

2.8.1.11. Despliegue de CA sobre cC Sub-CA | RA 35
2.8.1.12. Salir 37
2.8.2. Entorno de Sub-CA | RA....37
2.8.2.1. Pre requisitos 38
2.8.2.2. Inicio....39
2.8.2.3. Archivo de configuración global 39
2.8.2.4. Configurar Base de Datos 42
2.8.2.5. Configurar Correo Electrónico 43
2.8.2.6. Configurar Servidor Web 43
2.8.2.7. Configuraciones generales 44
2.8.2.8. Servidor Web....46
2.8.2.9. Consulta de CA 51
2.8.2.10. Creación de SUB-CA....53
2.8.2.11. Mecánica....59
2.8.2.12. Configuración de Sub-CA 60
2.8.2.13. Base de Datos plana SSL....62
2.8.2.14. Resguardo de Base de Datos....62
2.8.2.15. Consulta de CRL 64
2.8.2.16. Re carga de CRL....64
2.8.2.17. Gestión de certificados 68
2.8.2.17.1. Consulta de certificados cliente....68
2.8.2.17.2. Revocar certificados cliente 69
2.8.2.17.3. Nuevo certificado cliente 70
2.8.2.17.4. Creación de Cliente: Manual – Humano....70
2.8.2.17.5. Revocación de Cliente 75
2.8.2.17.6. Re carga de CRL con revocaciones....78
2.8.2.17.7. Distribución de Cliente: Manual – Puesto....82
2.8.2.17.8. Distribución de Cliente: CSR – Humano 87
2.8.2.17.9. Creación de certificado Servidor 92
2.8.2.18. Alertas y notificaciones....96
2.8.2.19. Certificados de terceros....104
2.8.2.19.1. CSR: Pedido de certificado 106
2.8.2.19.2. CSR: Recepción y composición de certificado final....110
2.8.2.20. Validaciones....113
2.8.2.21. Auditoria y manejo de errores....119
2.8.2.22. Modo aprendizaje de carga colectiva....122
2.9. Templates SSL....124

2.9.1. cC Sub-CA | RA - Puesto....124
2.10. Configuración global....127
2.10.1. Config.ini: cC Sub-CA | RA....127
2.11. Archivos dinámicos....133
2.12. Control de versiones....135
2.13. Aportes principales....135
2.14. Futuro....136
3. Conclusiones....137
4. Anexo....138
4.1. Ampliación de Configuración Global....138
4.1.1. Config.ini: cC CA....138
4.2. Ampliación de Templates SSL....140
4.2.1. cC Sub-CA | RA – Humano....141
4.2.2. cC Sub-CA | RA – Servidor....143
4.2.3. cC Sub-CA | RA – Monitoreo....145
4.2.4. cC Sub-CA | RA....146
4.2.5. cC CA....150
4.3. Tipos de uso de claves públicas....153
5. Índices específicos....154
5.1. Índice de Figuras....154
5.2. Índice de Tablas....161
6. Bibliografía general....162
7. Bibliografía específica....165

Prólogo

A Dios, quien es mi fortaleza en los momentos difíciles.

A mis Padres, Griselda y Carlos.

A todo aquel que me honra al leer estas páginas, dado que honra una parte de mí.

Matías R. Vz H.

Nómina de abreviaturas y acrónimos

Backend: Interfaz de administración

BASH, del inglés: Bourne-again Shell; en castellano: Interprete de órdenes y lenguaje de consola GNU/Linux

CA, del inglés: Certification Authority; en castellano: Autoridad Certificante

cC: centralizerCert

DS, del inglés: Date Stamp; en castellano: Sellado / Estampado de Fecha

DTS: Estampado de Fecha y Tiempo

Frontend: Interfaz de usuario

OS, del inglés: Operating System; en castellano: Sistema Operativo

PFX, del inglés: Personal Information Exchange; en castellano: son certificados que pueden contener tanto claves públicas y / o privadas. Define como almacenar objetos criptográficos en un archivo, para agrupar una determinada cadena de confianza

PKI, del inglés: Public Key Infraestructure; y del castellano: Infraestructura de Clave Pública.

RA: Autoridad de Registro

SSH, del inglés: Secure Shell; en castellano: Protocolo que implementa acceso remoto a un host por canal seguro mediante información cifrada

Sub-CA, del inglés: Subordinate CA; en castellano: Autoridad Certificante Subordinada o intermedia

TS, del inglés: Time Stamp; en castellano Sellado / Estampado de Tiempo

TSA, del inglés: Time Stamp Authority; en castellano: Autoridad de Sellado / Estampado de Tiempo

Uptime: Tiempo en línea

UTC, de inglés: Coordinated Universal Time; en castellano: Tiempo Universal Coordinado

VA, del inglés: Virtual Appliance; en castellano: Appliance Virtual

VM, del inglés: Virtual Machine; en castellano: Máquina Virtual

1. Cuerpo introductorio

1.1. Introducción

Desde hace tiempo, la necesidad de mejores y más sofisticadas medidas de seguridad es de primordial importancia, haciendo que hoy día la utilización de certificados digitales sea de uso común, para garantizar técnica y legalmente la identidad del firmante para ofrecer servicios seguros a través de la nube en su mayoría.

El formato estándar definido internacionalmente es ITU-T X.509, para garantizar su interoperabilidad, más allá de los diferentes usos que estos permiten. Lo que se pretende es analizar la problemática referente a la gestión de certificados digitales en organizaciones de pequeña y mediana envergadura.

Por ello, los sistemas simples de autenticación de usuarios por ejemplo, basados en usuario y contraseña, son insuficientes porque no proporcionan la suficiente granularidad entre los sistemas, pueden resultar tediosos, y ser fácilmente robados, compartidos y violados; lo cual no quiere decir que los certificados digitales no pueden ser vulnerados ni mucho menos, pero conjugando estos con sistemas más sofisticados de autenticación de usuarios como ser Infraestructura de Clave Pública [1] (PKI), proporcionan un incremento en los niveles de seguridad a expensas de la usabilidad y los costos que conllevan.

1.2. Objetivos

Evaluar la factibilidad y viabilidad analítica de una herramienta particular y efectiva orientada a pymes, evitando múltiples entornos descentralizados, heterogéneos e independientes de certificados digitales. Permitir cubrir la mayoría de los estadios y escenarios posibles existentes dentro un esquema de certificación, agrupando y centralizando la gestión de manera efectiva, con un diferencial único, modular, seguro y escalable, soportando la emisión, revocación, publicación, distribución y gestión eficaz de certificados digitales.

1.3. Alcance

Se realizará una prueba de concepto a fin de evaluar la problemática planteada, generando una CA root y una Sub-CA auto firmadas y customizables. Además, se plantea la posibilidad de permitir la gestión de certificados en un esquema centralizado y administrable, integrando múltiples plataformas, herramientas, motores y componentes open source [2] [3] permitiendo construir, disponibilizar y desplegar en pocos minutos bajo múltiples entornos de forma controlada diversos escenarios para la disponibilización de servicios a discreción.

1.4. Hipótesis

¿Es posible centralizar los certificados digitales de una organización pequeña o mediana sin el presupuesto necesario para la adquisición de más de una herramienta y sin personal especializado?

2. Cuerpo principal

2.1. Certificados Digitales

En la actualidad, debido al caudal de certificados digitales a manejar, es necesario la adquisición de alguna herramienta o solución que permita la administración de estos.

Ante tal situación, los centros de información tienden a desarrollar una serie de estrategias que centran su atención hacía un nuevo horizonte digital que permite la organización de esta gran masa de información, con el supuesto propósito de facilitar el acceso, aumentar la seguridad y reducir los tiempos; lo que permitiría una recuperación de forma práctica, eficiente y no invasiva fundamentalmente.

No se debe olvidar, la necesidad de restringir los accesos y comprobar que quien dice ser, es realmente él mismo, ya que la necesidad del mundo va de la mano con la evolución de las nuevas tecnologías y hace tiempo que los esquemas hiperconectados en la nube, para reconocer y confirmar la identidad de los usuarios en diversos esquemas como ser entre otros: banca, comercio electrónico, firma de documentos, o acceso a servicios; es de uso cotidiano.

Por lo cual, que el planteo a realizar es el de lograr limitar el accionar independiente, manual y particular de cada escenario, mitigando la falta de controles ya sea en la manipulación de certificados de terceros como propios tanto en su utilización como en su construcción generando una infraestructura de clave pública (PKI) propia. Ahora bien, para ello, se deberían poder anticipar vencimientos, como también detectar cambios en las fuentes de emisión, para los casos de aplicaciones con certificados estáticos por ejemplo (cacerts java [4]), dentro de organizaciones de pequeña y mediana estructura, con una inversión mínima de bajo coste.

Entonces, la gestión centralizada de certificados digitales utilizados en las organizaciones, permitiría la unificación de múltiples fuentes, de manera que se operen centralizadamente, dentro de un esquema controlado y seguro, de forma divisible por cada entorno según corresponda; ya bien agrupado o

distribuido, pero bajo la órbita del centralizador, unificando la toma de decisiones en un panel de control.

La centralización logra conseguir una serie de ventajas, dentro de las cuales podemos destacar:

- ✓ Confianza de única fuente: un único recurso despliega sobre el entorno correspondiente el escenario adecuado y customizado según corresponda, evitando su configuración e interacción manual.
- ✓ Control centralizado de permisos de acceso: puede limitarse el número de certificados a los que un usuario o servicio tiene acceso, y sobre qué páginas o servicios puede actuar, mediante el control centralizado del entorno.
- ✓ Monitoreo y trazabilidad: permite realizar un control y seguimiento tanto de los certificados como de su uso dependiendo el tipo de nivel de control.
- ✓ Control de pérdidas: permite mitigar las pérdidas de certificados al ubicarse en el almacén correspondiente con su política de resguardo según corresponda.
- ✓ Revocación, expiración y destrucción controlada: permite realizar la gestión correspondiente gracias a su organización unificada.
- ✓ Distribución: controlada desde que se procesa el pedido hasta que se entrega en la dirección electrónica del individuo interviniente.

2.2. Gestión de certificados digitales

Es el conjunto de acciones que permiten la realización de la actividad. Por ello, la gestión de certificados digitales, no es ni más ni menos que la planificación, construcción, ejecución y control de los pares de claves de criptografía asimétrica que, empleando las propiedades de las mismas, permiten identificar inequívocamente a una persona, entidad o website, mediante un certificado digital.

2.3. Escenarios de autenticación

Existen tres escenarios de autenticación en línea, en base al mecanismo empleado, definidos a continuación:

- Autenticación directa: Se basa en la interacción directa entre el servicio y el usuario. La mayoría de estos se basan en el intercambio de contraseñas y / o información adicional conocida por ambas partes.
- Autenticación federada: es un modelo en el cual un conjunto de servicios comparte y gestionan conjuntamente la información de sus usuarios.
- Autenticación certificada: Se basa en el empleo de certificados de clave pública, permitiendo autenticar sin la necesidad de un registro presencial, puesto que se confía en la información provista por el certificado presentado, siempre y cuando la legislación lo acompañe. Este método, trae aparejado el beneficio de poder relacionarse con terceros de forma transparente.

2.4. Tipos de certificados

De acuerdo a la finalidad solicitada por el firmante, se puede clasificar a los certificados, basándonos en la tipificación [5] realizada por el Instituto Nacional de Ciberseguridad de España denominado INCIBE, sobre certificados ordinarios clasificados como:

- Persona física, denominado en el presente documento como HUMANO
- Persona jurídica, denominado como PUESTO
- Individual o Corporativo, denominado como SERVIDOR y MONITOREO respectivamente

2.5. Estructura estándar de Certificados

X.509 es el estándar conocido para definir y establecer el contenido y estructura que tiene un certificado digital, definido en el RFC 5280 originario de 1988 y actualizado a su última versión (v3) en 2008.

La especificación de su estructura definidos principalmente en el apartado 4 [6] del RFC, muestran de forma gráfica la composición de certificados como se muestra a continuación, comparativamente

diferenciando sus campos entre las distintas versiones existentes con el paso del tiempo:

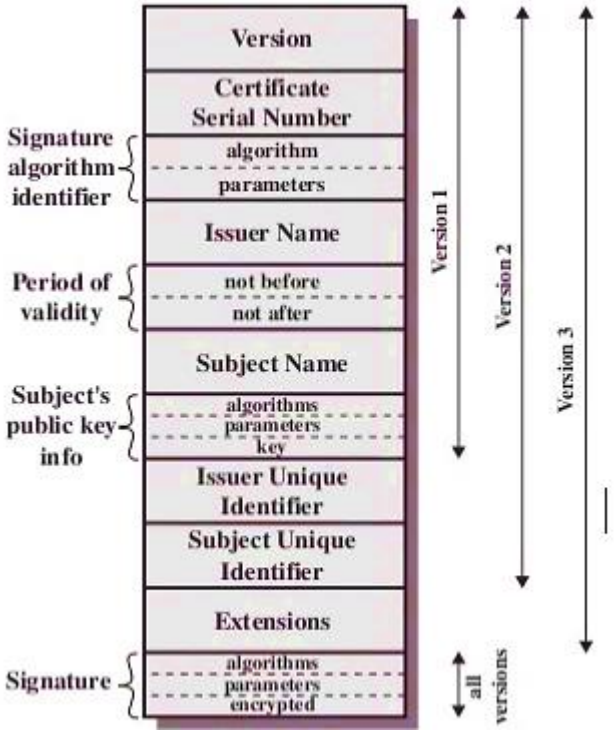

Figura 1. Estructura X.509 versión 3 de Certificados Digitales [7]

En la figura, se puede apreciar un conjunto de grupos, donde podemos destacar los siguientes:

- tbsCertificate: contiene la información de emisor, sujeto y validez como información adicional relacionada.
- signatureAlgoritm: contiene la información para identificar inequívocamente el algoritmo criptográfico empleado por la CA para firmar el certificado, como así también información opcional dependiendo del tipo de algoritmo utilizado.
- signatureValue: incorpora el contenido de la firma del certificado, y es el campo que asegura mediante la firma de la CA, que la información contenida en el campo tbsCertifcate es fidedigna, por ende, implementa la cadena de confianza.
- extensions: son un conjunto de campos y parámetros opcionales.

Ahora bien, si nos referimos al conjunto o bloque tbsCertificate, este contiene información fundamental de la Infraestructura de Clave Pública, de ahora en más denominada PKI; como así también otros campos de vital importancia detallados a continuación:

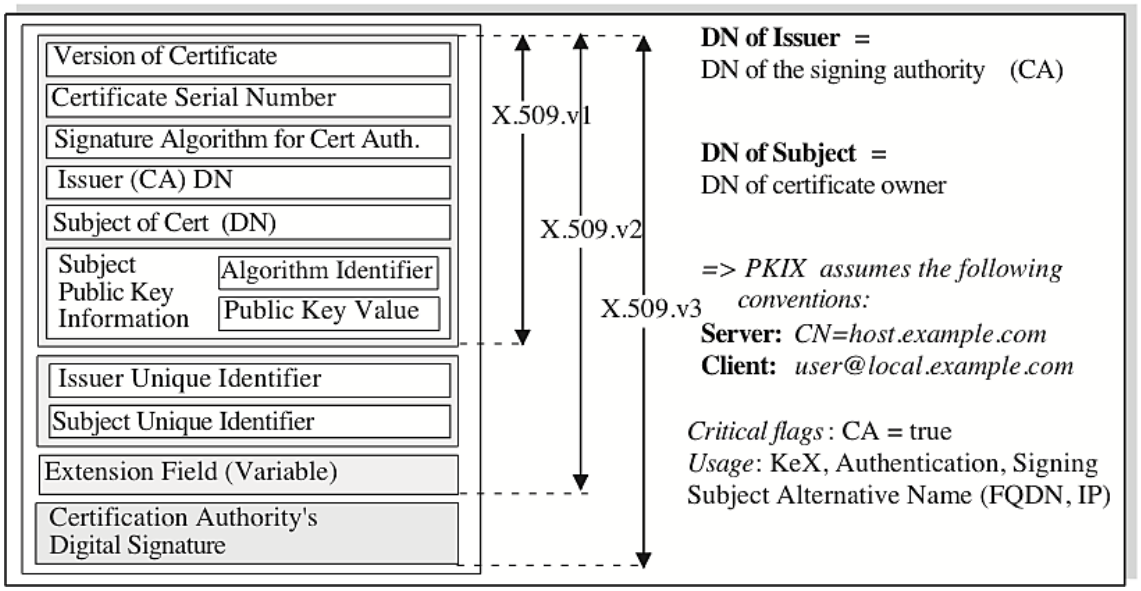

Figura 2. Detalle X.509 de Certificados Digitales [8]

- Versión / Version: contiene la versión del protocolo X.509 con la que fue construido el certificado.
- Número de Serie / Serial Number: contiene el número de serie expresado como numero entero positivo, que asigna la CA y que identifica al certificado unívocamente dentro de la cadena de confianza.
- Identificador del Algoritmo de Firma / Signature Algorithm Identifier: contiene el algoritmo de cifrado utilizado para generar la firma de quien suscribe.
- Emisor / Issuer: contiene la información de la Autoridad de Certificación que emitió el certificado.
- País / Country: país de la CA.
- Organización / Organization: nombre de la CA.
- Departamento / Organizational Unit: unidad organizativa o departamento de la CA.
- Provincia / State or Province Name: provincia de la CA.
- Nombre Común / Common Name (CN): subjet del certificado empleado.
- Localidad / Locality: localidad de la CA.
- Nota / Note: campos como title, surname, given name, initials, pseudonym o generation qualifier, entre otros, se definen dentro del campo emisor, pero no se suelen utilizar cuando quien emite el certificado es una CA.
- Validez / Validity: es un campo fundamental, dentro de una PKI, ya que es el tiempo en que se compromete la CA a disponer de información sobre la validez del certificado, es decir, la vida útil del certificado. Esta puede ser

codificada empleando dos mecanismos: UTC Time [9] o Generalized Time [10].

- Suscriptor / Subject: incorpora los datos del usuario final, por lo que va directamente asociado a la clave pública contenida en el mismo certificado. Análogamente, como en el caso anterior, nos detendremos únicamente en los campos fundamentales y de uso extendido, habiendo una especificación extensa de posibles campos para este punto.

Para finalizar la descripción de la estructura de un certificado X.509, detallamos las principales extensiones utilizadas, teniendo en cuenta que los campos son opcionales:

- Authority Key Identifier: Identifica inequívocamente a la CA.
- Subject Key Identifier: Identifica inequívocamente al suscriptor.
- Key Usage: Especifica los usos válidos del certificado.
- Certificate Policies: Define las Políticas de Certificación.
- Basic Constraints: Incluye información específica que indica si el certificado es de CA, lo que permitiría emplearlo para firmar otros certificados, por ejemplo.
- CRL Distribution Points: URL donde se puede obtener la CRL.
- Authority Information Access: Ruta de acceso al servicio de validación OCSP de la CA.

2.6. Especificaciones del modelo

De acuerdo a las definiciones planteadas hasta el momento, y basado en el relevamiento de flujo de procesos, a continuación se detallaran las especificaciones del prototipo modelo a implementar, basado en el relevamiento de flujo de procesos y sus características analizadas.

2.6.1. Denominación

Se adopta la contracción cC para identificar el prototipo denominado ‘centralizerCert’, haciendo mención a un centralizar de certificados. Con el simple hecho de intentar identificar una sigla con un símbolo, que vincule el operador al utilizar la solución, se realizó el diseño de imagen o branding, generando un concepto cerrado como unidad, con mayor fuerza. Su diseño

es muy sencillo y sus colores, tipografía y forma intentan generar efectos psicológicos en sus usuarios, por lo que fue específicamente diseñado para lograr un vínculo, provocando su identificación con el símbolo y el concepto.

Figura 3. Logotipo de cC

2.6.2. Arquitectura

El mecanismo consta de un esquema de tres máquinas virtuales sobre la cual, la base mínima y necesaria para su operación consta de dos VM's las cuales mantienen distintos niveles de acceso y comunicación, siendo el último eslabón, una agrupación de equipos de acuerdo a las necesidades del negocio, el cual podrá ser prescindible realizando la interacción manual con este según corresponda.

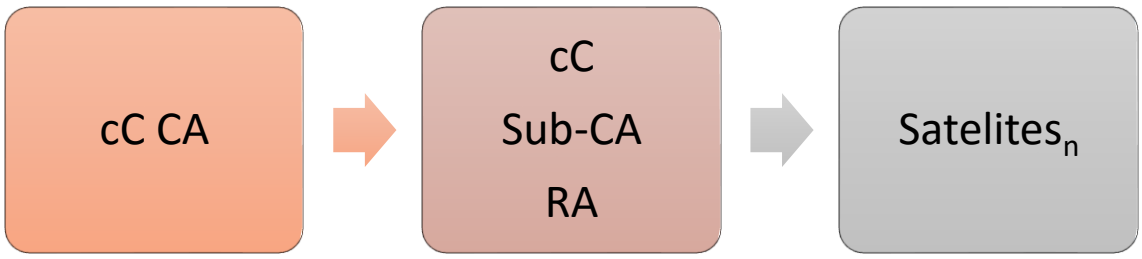

Figura 4. Diagrama en bloques de arquitectura cC

2.6.3. Diagrama de flujo de procesos

De acuerdo al modelo a implementar, se describen los procesos básicos generales diseñados:

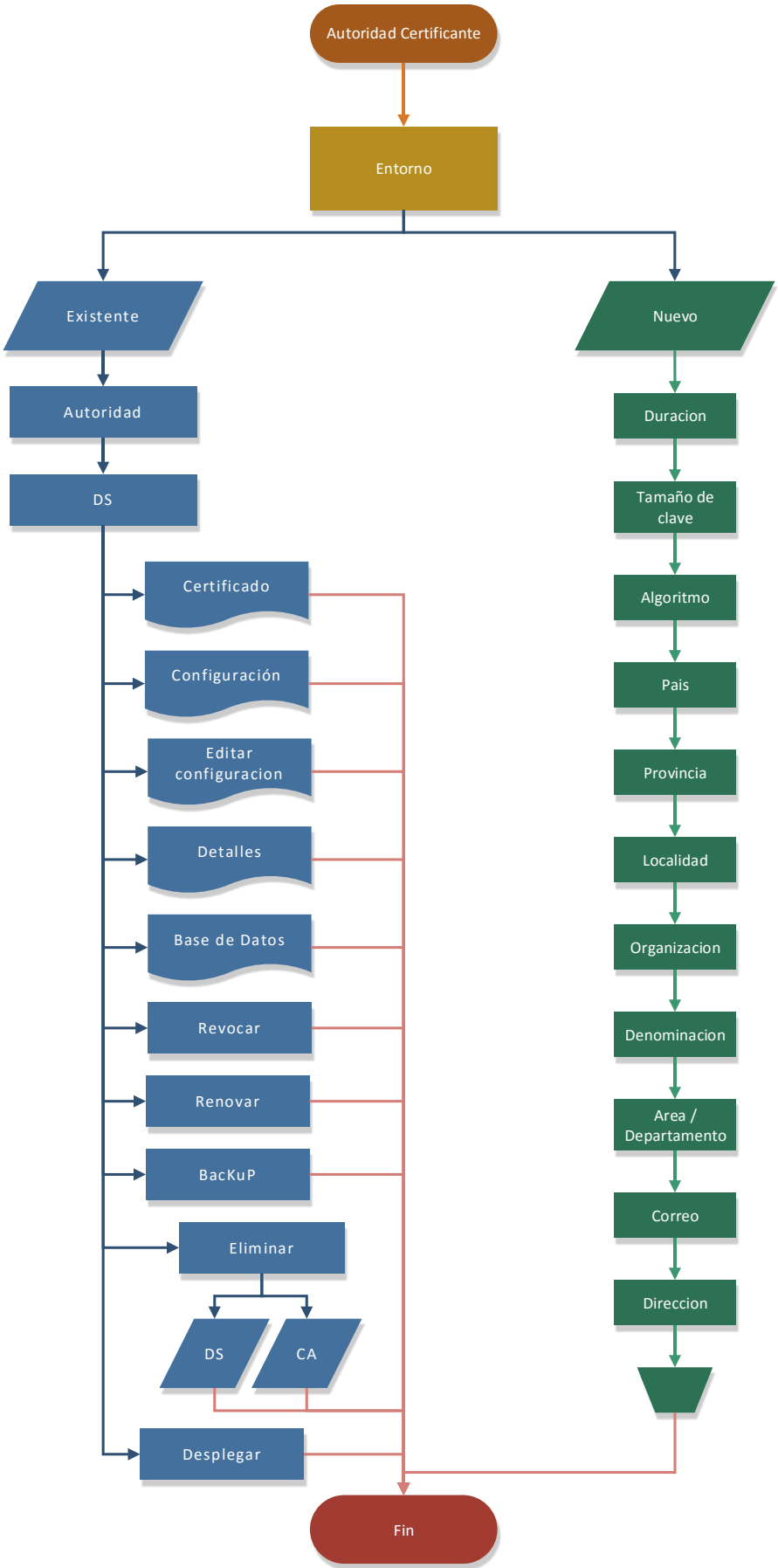

Figura 5. Diagrama de flujo general de CA

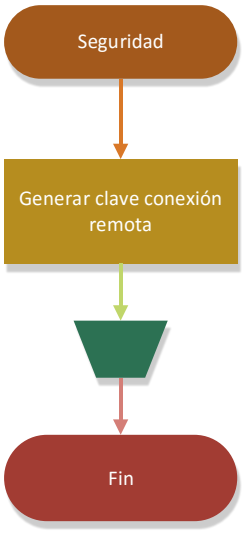

Figura 6. Diagrama de flujo general de clave de conexión de CA

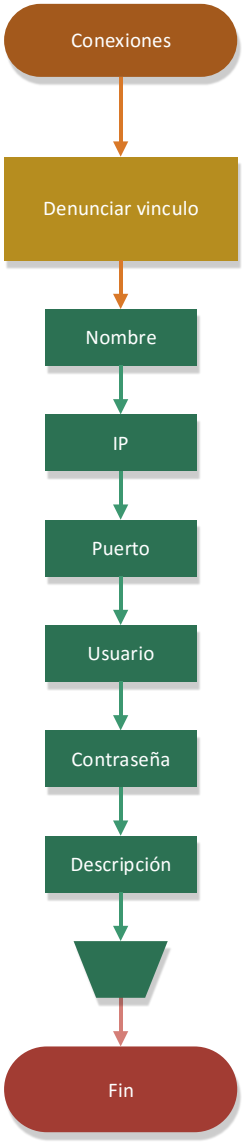

Figura 7. Diagrama de flujo general de vinculo CA – Sub-CA | RA

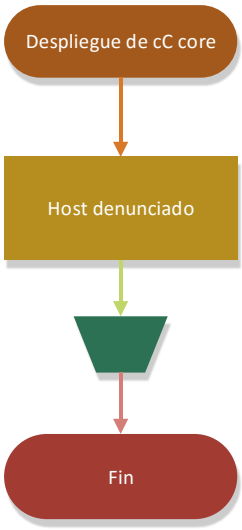

Figura 8. Diagrama de flujo general de despliegue de core desde CA

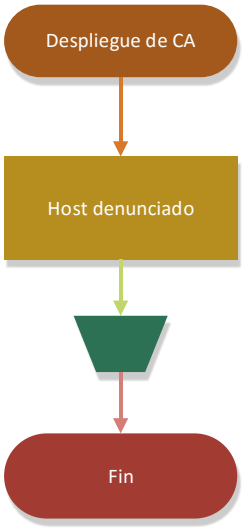

Figura 9. Diagrama de flujo general de despliegue de CA desde CA

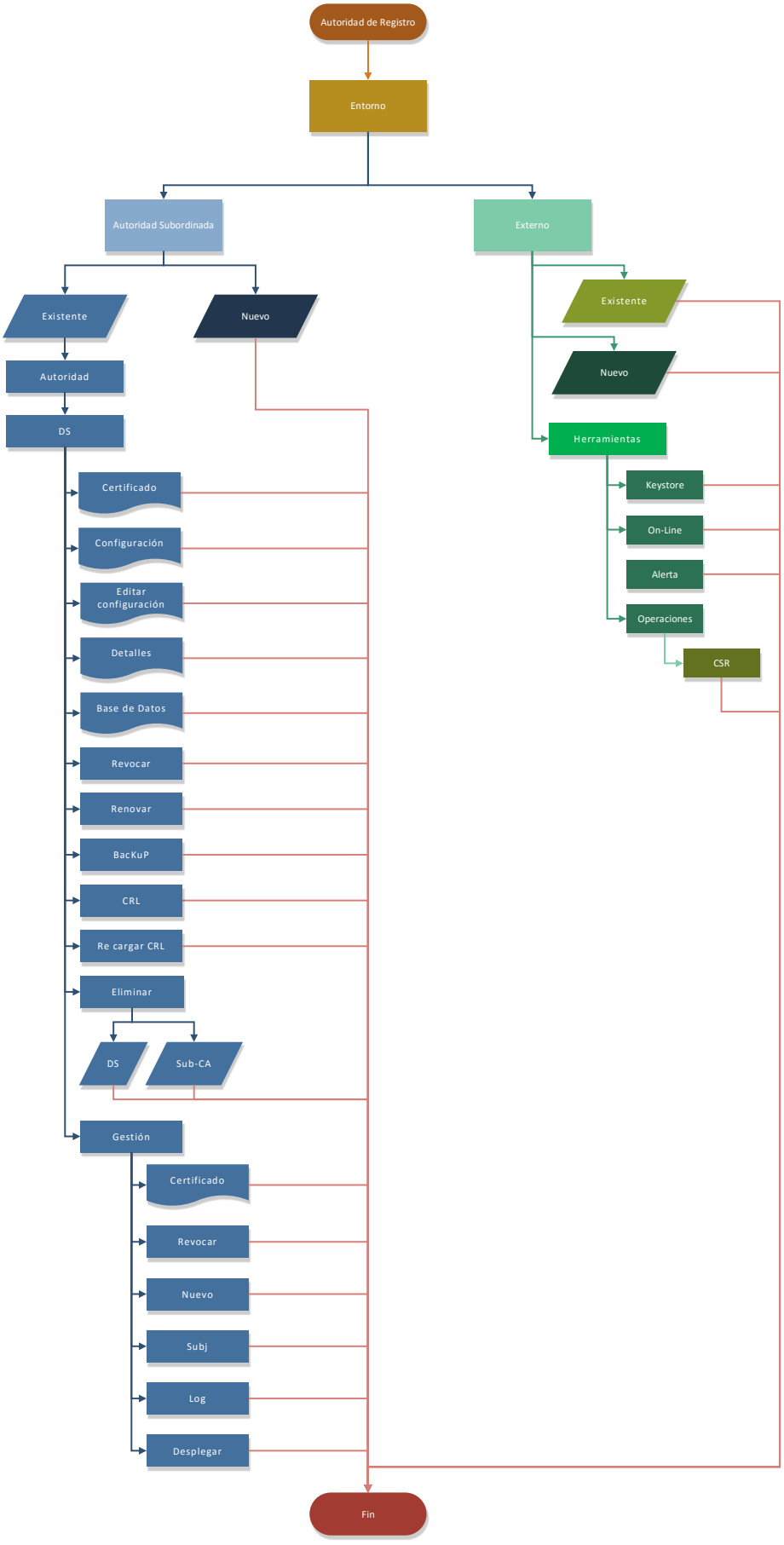

Figura 10. Diagrama de flujo general de RA

2.7. Diseño del prototipo experimental implementado

Con el fin de generar la infraestructura correspondiente para realizar las pruebas necesarias y verificar el modelo planteado, a continuación, se detalla la implementación intervenida, considerando además las buenas prácticas de uso y seguridad dentro de los lineamientos establecidos.

2.7.1. Limitaciones

Por las características del alcance y a fin de lograr una pronta aproximación a un modelo experimental para poder realizar el análisis de factibilidad, el presente prototipo no incluye ciertos pormenores de seguridad como ser: la securización de las máquinas virtuales y su infraestructura, informando que ante un pen test sobre estas, las mismas podrían llegar a incluir vulnerabilidades o debilidades a remediar.

2.7.2. Pruebas de concepto

Se definirán los casos para realizar las diferentes pruebas, siendo que las mismas fueron diseñadas y realizadas para comprobar las diferencias reales y ciertas dadas en la comparación realizada, obteniendo resultados cualitativos que permiten apreciar la diferencia en cada situación y su exposición según corresponda para su posterior análisis.

Por ende, la presente investigación nos permite identificar, cuantificar y clasificar los efectos que se obtienen dentro del estudio realizado a continuación.

2.7.3. Prerrequisitos

Se enumera el entorno necesario como escenario para las pruebas a realizar a nivel de hardware y software.

2.7.3.1. Requisitos de software

Existen una variedad de aplicaciones que trabajan en conjunto. En este caso, se mencionan los productos específicos requeridos para el entorno planteado:

- cC CA:
  - **S.O.:** Centos v6.5 o superior (Se recomienda utilizar v7)
  - **Paquetes:** net-tools, nano, vim-enhanced, system-config-firewall-tui, system-config-keyboard, dpkg-reconfigure tzdata, system-config-language, openssl, sshpass
- cC Sub-CA:
  - **S.O.:** Centos v6.5 o superior (Se recomienda utilizar v7)
  - **Paquetes:** net-tools, nano, vim-enhanced, system-config-firewall-tui, system-config-keyboard, dpkg-reconfigure tzdata, system-config-language, openssl, sshpass, httpd, php, mysql, mutt, bind-utils

2.7.3.2. Requisitos de hardware

- VM / VA - CA:
  - 1 CPU
  - 1 GB Memoria
  - 16 GB Disco
  - vLan Adaptador de red
- VM / VA - Sub-CA:
  - 1 CPU
  - 1 GB Memoria o superior
  - 16 GB Disco o superior
  - vLan Adaptador de red

2.7.4. Operación

El prototipo cC, permite en muy pocos minutos generar una infraestructura de appliance virtuales, con un entorno flexible gracias a su archivo estructurado minuciosamente, de configuración inicial. Despliega su potencial basado en una arquitectura de templates de configuración SSL on-

premise (solución instalada físicamente, no en la nube). Esto potencia y permite customizar de forma simple y sencilla la solución. Gracias a su interfaz gráfica SSH especialmente diseñada, permite la operación de cualquier usuario (operador) sin mayores conocimientos, gracias a los menús tipo wizard creados especialmente, a través de scripting bash.

El archivo de configuración por cada VM, permite personalizar el core (núcleo), desde sus mensajes, leyendas, configuraciones específicas de logueos, visuales, como así también, entornos, templates y valores sugeridos. En el caso de cC Sub-CA | RA, la VM intermedia, incorpora además la posibilidad de parametrizar según corresponda: base de datos, web y correo, haciendo una solución más completa que cC CA, propia de su razón de ser, su esencia. La escalabilidad con la que cuenta el core, permite la posibilidad de incorporar nueva parametrización de bits, algoritmo, países, días, motivo de revocaciones, estados, y tipos de cliente entre otros, sin la necesidad de modificar una línea de código, aportando un diseño resistente al paso del tiempo.

El esquema plantea un mecanismo de comunicación unidireccional, como se vio en la sección Arquitectura, es decir, de una sola vía, en sentido cC CA hacia cC Sub-CA | RA, y esta última hacia los satélites correspondientes. Esto permite limitar y aislar la CA, con un uptime mínimo para su despliegue, lo que implicaría teóricamente una operación estimada de 2’30’’[1] (dos minutos y medio) aproximadamente cada x días, siendo x el tiempo de vida de la misma.

Una vez generada la CA, para avanzar al siguiente nivel, configurar la Sub-CA, y utilizar la RA, se debería previamente desde cC CA, generar la clave de conexión remota, además de denunciar el vínculo remoto para establecer la relación de confianza unidireccional en sentido CA - Sub-CA | RA, y así proceder a desplegar el core base de cC, para por último desplegar la CA y sacarla de servicio a esta última, bajando el servicio cC CA, hasta

[1] Considerando que la VM ya se encuentra instalada, y cC CA ya ha sido instalado; el tiempo estimado corresponderá a 2’30‘’, basado en las pruebas realizadas. En el caso de requerir una instalación de cero con el SO limpio y configurado (usuario, contraseña y conexión de red funcionales), y cC CA sin instalar, el tiempo estimado será de 5’ aproximadamente. Se deberá tener en cuenta que en caso de requerir una configuración diferencial a la pre configurada, los tiempos podrían incrementarse.

requerir anticipar su vida útil nuevamente o por otros motivos según corresponda.

Una vez inicializada la RA, es decir, cC Sub-CA | RA, y antes de continuar con la generación de la Sub-CA, ósea la CA intermedia o subordinada, debería configurarse la Base de Datos, el Correo Electrónico y el Servidor Web, con un simple y rápido wizard que se podrá abordar en los próximos apartados, a medida que se desarrolla el modelo.

Ahora sí, estaríamos en condiciones de acceder a la RA, la Autoridad de Registro, y crear la Sub-CA basada en la CA root desplegada, o bien gestionar certificado de terceros, como se podrá ver en los próximos apartados.

Al generar una nueva Autoridad Certificante Intermedia (Sub-CA), una vez desplegada la CA root en la Sub-CA | RA, esta se basa en la combinación del template correspondiente, y el mismo, en los valores sugeridos tanto del template que se utilizara, como de la configuración sugerida contenida dentro del archivo ini, el cual viene pre configurado por defecto, a lo que se suma la posibilidad de modificar las características comunes a demanda, las cuales una vez confirmadas, serán procesadas y generadas con la parametrización informada, logrando entornos agiles. La particularidad de estos, es la posibilidad de basarse en otros por ejemplo (templates o .ini). Entonces, se puede tener sin mayores esfuerzos, entornos disponibles y operativos al instante de, por ejemplo: producción, Testing y demo por mencionar alguno.

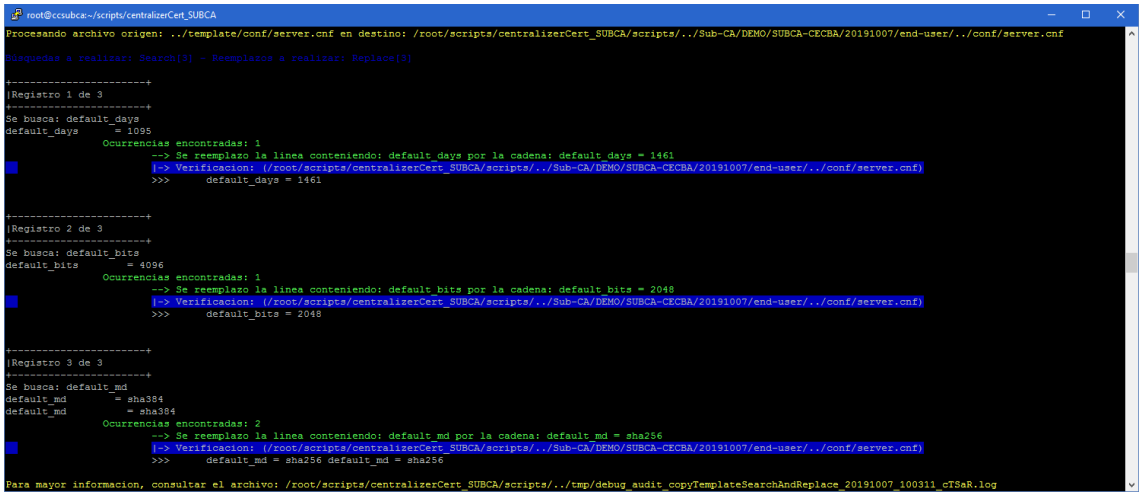

Figura 11. Ejemplo de búsqueda y reemplazo en template SSL

La imagen anterior, muestra cómo una vez introducida la información necesaria para crear en este caso, un certificado final de tipo servidor para autenticación web de cliente, se toma el template base SSL correspondiente, y conjugando este con los datos solicitados (parámetros sugeridos a través de su archivo de configuración global + datos ingresados a demanda según corresponda), se reemplazan puntos determinados del template, minuciosamente definidos, los cuales se pueden visualizar en la captura, para lograr componer y generar con sus parámetros específicos, dentro de un esquema univoco definido básicamente con la nomenclatura: Entorno | Sub-CA | DS.

Una vez creada la Sub-CA, disponemos del certificado para firmar los certificados de clientes finales (usuarios + servidor) a fin de poder, por ejemplo, controlar el acceso a un servicio web determinado, o verificar y/o monitorear certificados de terceros, entre otras alternativas. Entonces, para poder generar los certificados de tipo cliente, existen tres (3) modos disponibles: manual, por lote o mediante CSR. A grandes rasgos el método manual y por lote, genera certificados finales de tipo pfx[14] [15] de distribución directa al usuario. La diferencia entre estos es que el manual es único y el método por lote permite generar N, basado en el aprendizaje; mientras que el modo CSR, permite incorporar mediante una Solicitud de Certificado recibida por el usuario interviniente, es decir, el usuario envía la clave pública, basado en la especificación indicada según corresponda, a fin de que en base a esta, generemos su par de claves, para que luego componga su certificado aumentando así el nivel de seguridad, evitando generar las claves del usuario y su distribución directa como archivo final, en el caso de los pfx[14] [15].

Para que la infraestructura se mantenga disponible, se debe generar el servidor, a fin de que acepte las peticiones, y recargar la CRL periódicamente con las novedades de los certificados revocados, expirados o vigentes. Operaciones que pueden realizarse sobre certificados clientes para básicamente limitar su utilización a grandes rasgos.

Una vez montado, operativo y publicado, será necesaria la gestión en el tiempo del parque de certificados administrados. En este caso, además de los propios se pretende poder administrar certificados de terceros, con el fin de anticipar vencimientos, y monitorear cambios en las fuentes para así evitar

la indisponibilización de servicios publicados que utilicen estos certificados que han sido modificados. Además, es necesario disponer de los mecanismos necesarios para la creación y revocación de certificados propios, como así también mecanismos de alerta. Panel centralizado para toma de decisiones y la facilidad de implementación de certificados en general bajo diversos esquemas, ambientes e infraestructuras de forma simple y transparente para el operador. Por lo cual, y para ello, a continuación, se desarrollará de forma completa y progresiva en detalle, la operación descripta de forma general en el presente apartado.

2.8. Casos de prueba

A continuación, se detalla el set de pruebas y configuraciones a realizar congruente con el prototipo diseñado.

2.8.1. Entorno inicial de CA

Se muestran los datos involucrados en el proceso por orden de secuencia de encadenación:

2.8.1.1. Instalación

Se despliega el core de centralizerCert CA, por primera vez en la VM principal:

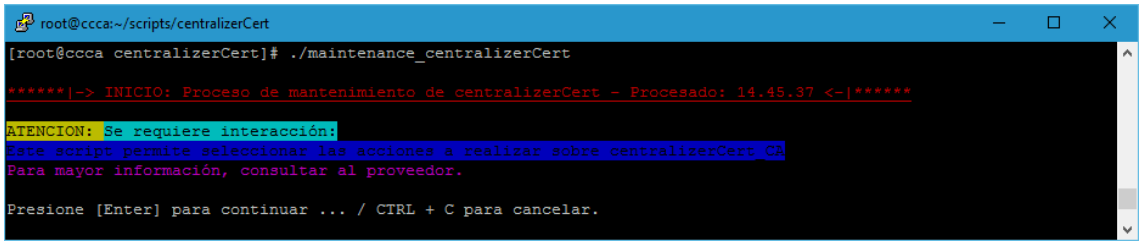

Figura 12. Paso 1 – Instalación de cC CA

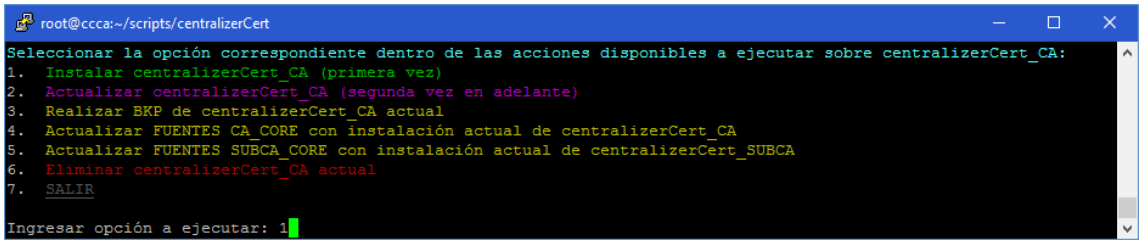

Figura 13. Paso 2 – Instalación de cC CA

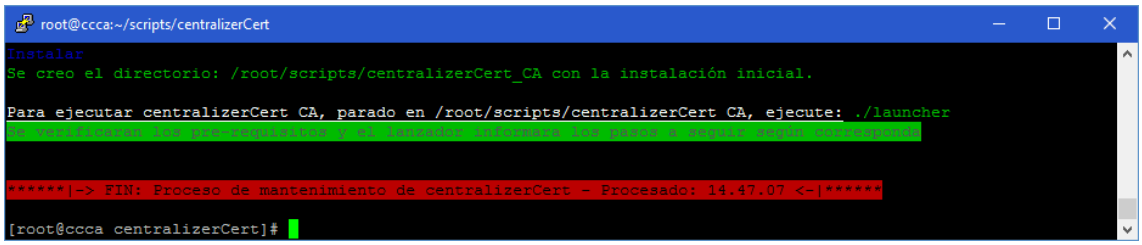

Figura 14. Paso 3 – Instalación de cC CA

2.8.1.2. Pre requisitos

Se inicializa por primera vez cC CA y se instalan los pre requisitos necesarios a fin de poder utilizar la tecnología, como se detalla a continuación paso a paso:

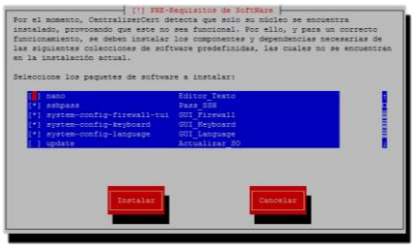

Figura 15. Paso 1 – Pre requisitos de cC CA

Figura 16. Paso 2 – Pre requisitos de cC CA

Figura 17. Paso 3 – Pre requisitos de cC CA

2.8.1.3. Inicio

Se inicia cC CA y su entorno operativo:

Figura 18. Paso 1 – Inicio de cC CA

Figura 19. Paso 2 – Inicio de cC CA

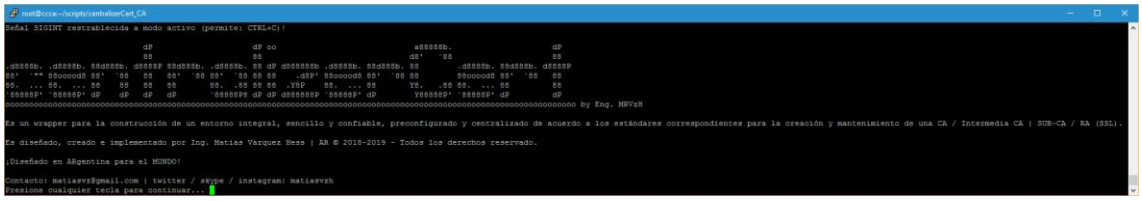

Figura 20. Paso 3 – Inicio de cC CA

2.8.1.4. Archivo de configuración global

Se visualiza el archivo pre configurado nativamente del core cC CA a continuación:

Figura 21. Paso 1 – Configuración global pre existente cC CA

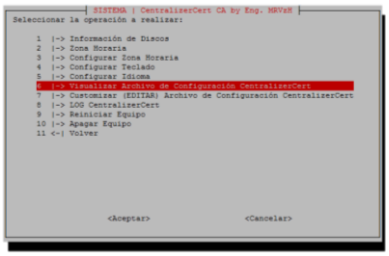

Figura 22. Paso 1 – Configuración global pre existente cC CA

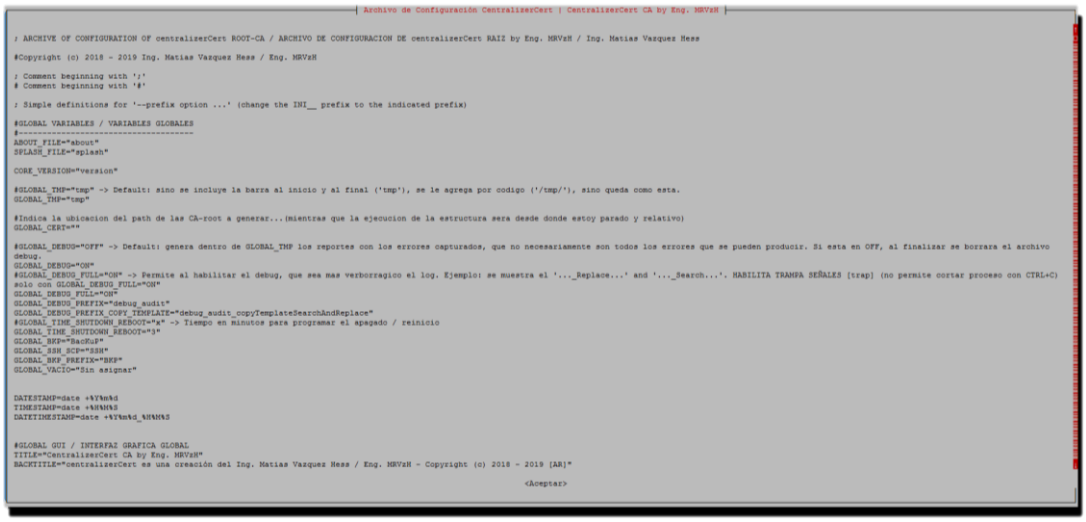

Figura 23. Paso 3 – Configuración global pre existente cC CA

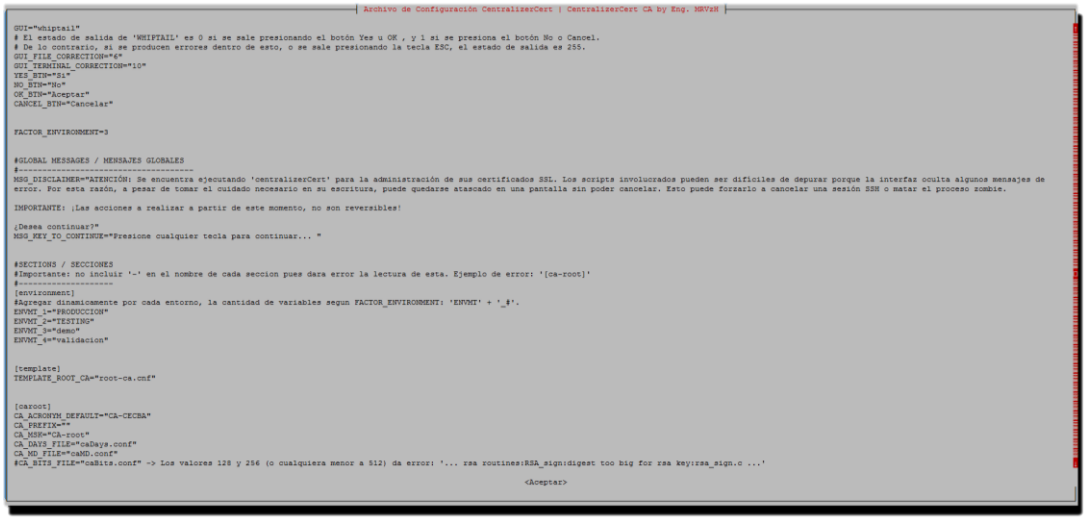

Figura 24. Paso 4 – Configuración global pre existente cC CA

Figura 25. Paso 5 – Configuración global pre existente cC CA

Para mayor información, respecto al archivo de configuración global de cC CA, ver: Ampliación de Configuración Global

2.8.1.5. Log

Se podrá visualizar el acceso al archivo histórico de cambios según corresponda:

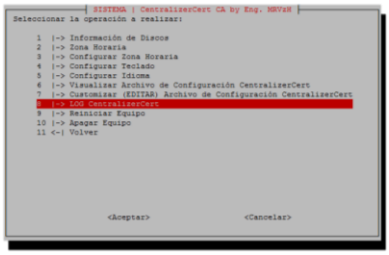

Figura 26. Paso 1 – Log cC CA

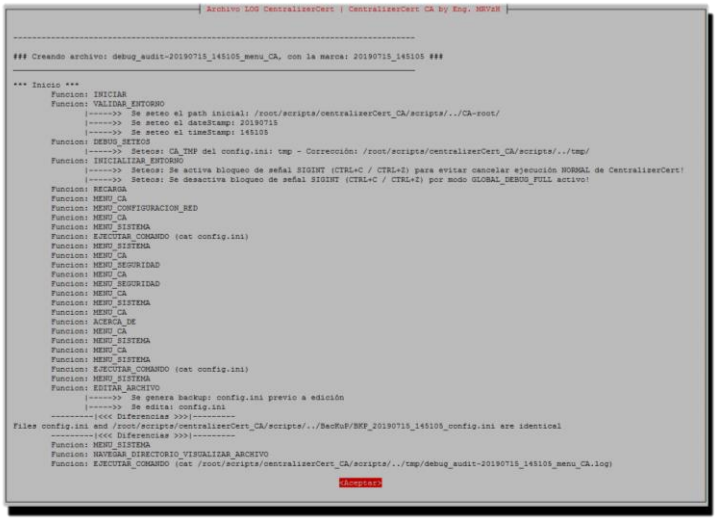

Figura 27. Paso 2 – Log cC CA

2.8.1.6. Creación de CA

Se crea la CA, como se puede observar en la VM principal, con la parametrización pre configurada, basado en sugerencias, templates e información ingresada a demanda:

Figura 28. Paso 1 – Creación de CA

Figura 29. Paso 2 – Creación de CA

Figura 30. Paso 3 – Creación de CA

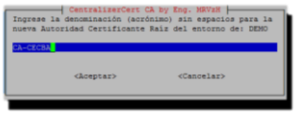

Figura 31. Paso 4 – Creación de CA

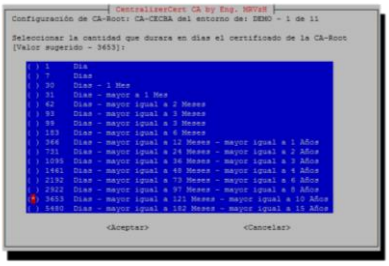

Figura 32. Paso 5 – Creación de CA

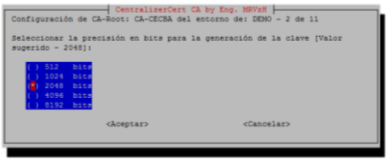

Figura 33. Paso 6 – Creación de CA

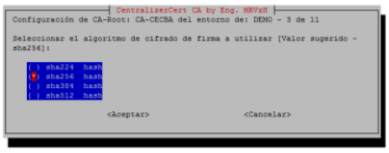

Figura 34. Paso 7 – Creación de CA

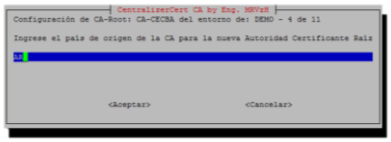

Figura 35. Paso 8 – Creación de CA

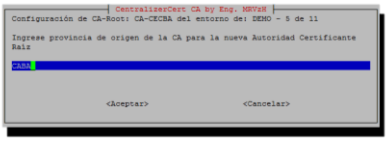

Figura 36. Paso 9 – Creación de CA

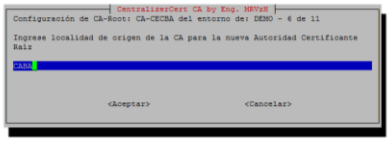

Figura 37. Paso 10 – Creación de CA

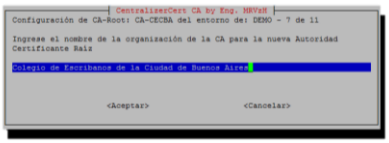

Figura 38. Paso 11 – Creación de CA

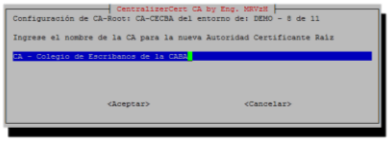

Figura 39. Paso 12 – Creación de CA

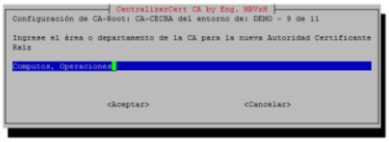

Figura 40. Paso 13 – Creación de CA

Figura 41. Paso 14 – Creación de CA

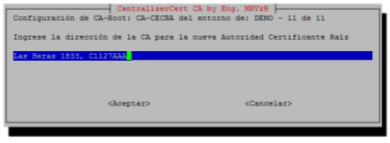

Figura 42. Paso 15 – Creación de CA

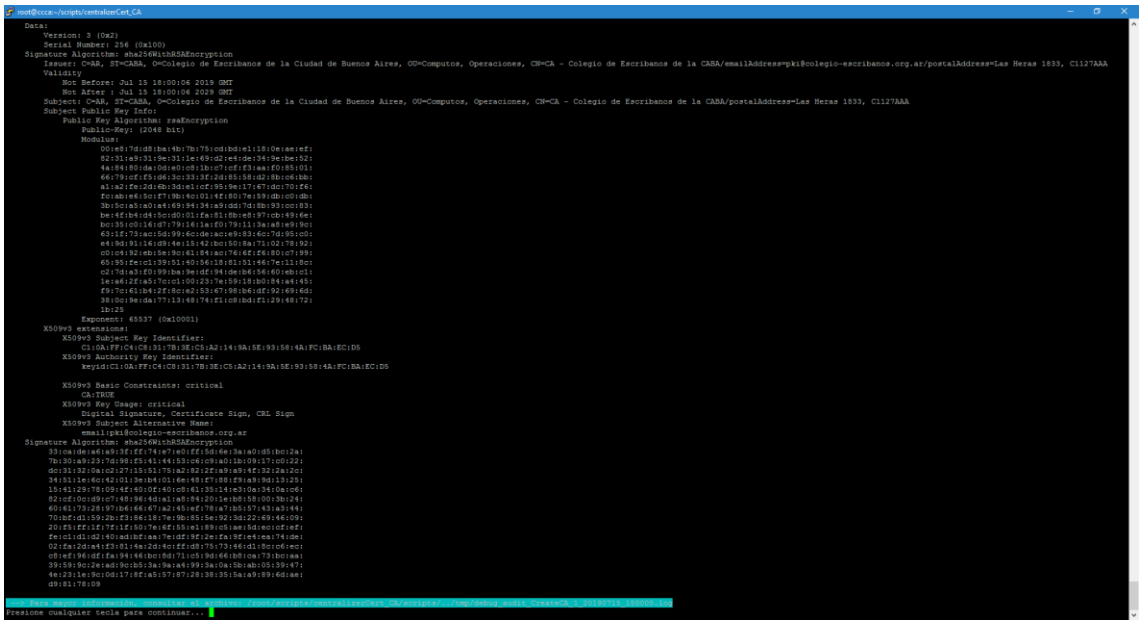

Figura 43. Paso 16 – Creación de CA

Figura 44. Paso 17 – Creación de CA

Figura 45. Paso 18 – Creación de CA

Figura 46. Paso 19 – Creación de CA

Figura 47. Paso 20 – Creación de CA

Figura 48. Paso 21 – Creación de CA

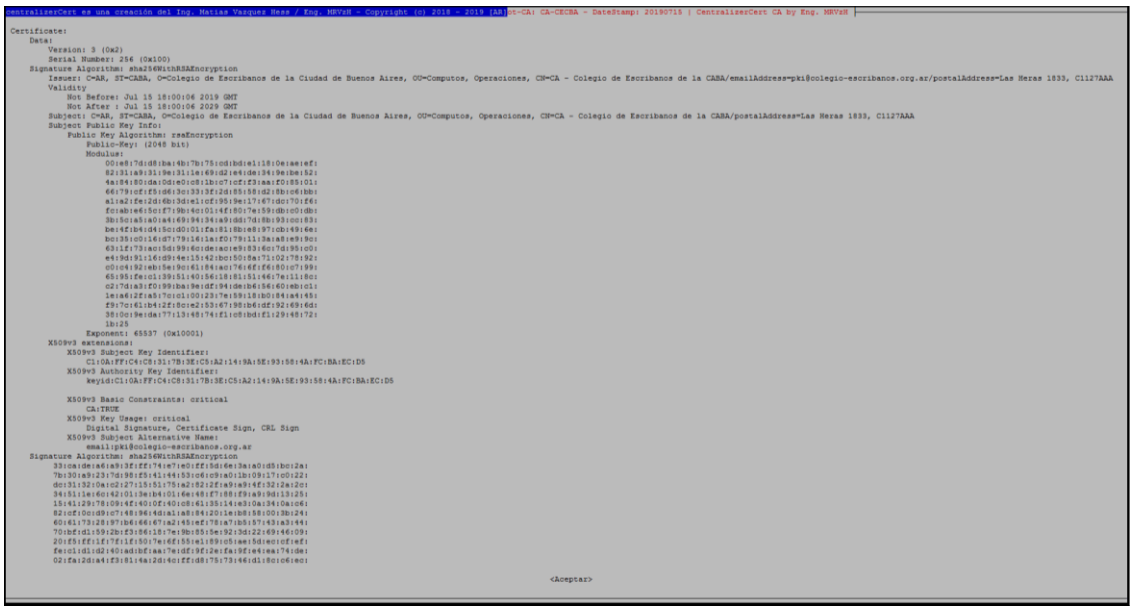

Figura 49. Paso 22 – Creación de CA

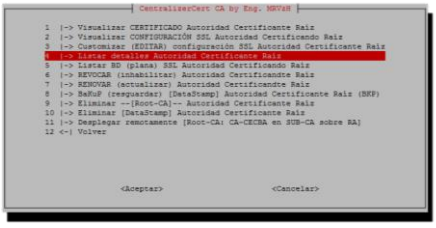

Figura 50. Paso 23 – Creación de CA

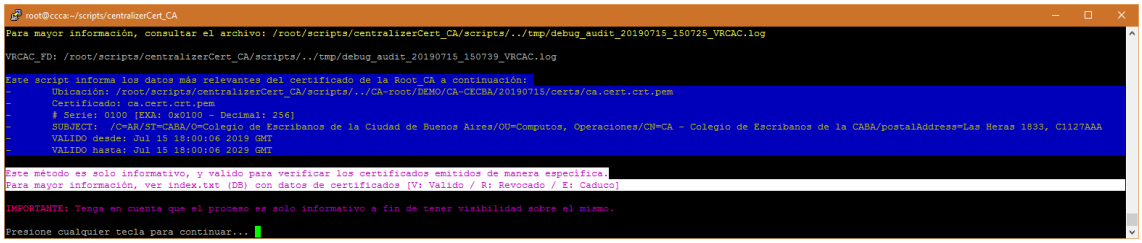

Figura 51. Paso 24 – Creación de CA

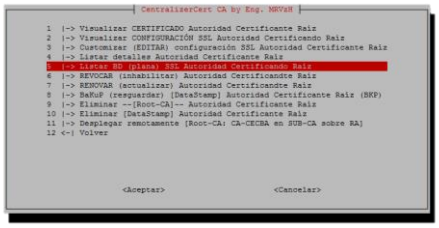

Figura 52. Paso 25 – Creación de CA

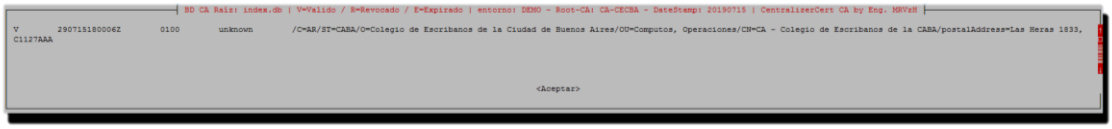

Figura 53. Paso 26 – Creación de CA

2.8.1.7. Configuración de CA

Basado en el template de cC CA, la pre configuración de parámetros sugeridos y los datos introducidos a demanda en el wizard anterior de creación de CA, observamos la parametrización final de la CA [11] sobre la cual se creó, basada en el template pre configurado y los parámetros base, lo cuales pueden customisarse en cualquier momento del ciclo de vida, con las implicancias del caso, es decir, si cambia el template de CA por ejemplo, para que los cambios surtan efecto, se deberá crear nuevamente la CA:

Figura 54. Paso 1 – Ver configuración SSL de CA

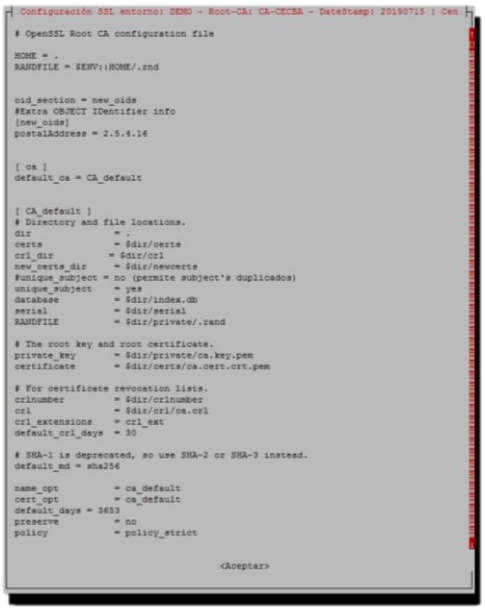

Figura 55. Paso 2 – SSL de CA

Figura 56. Paso 3 – SSL de CA

Figura 57. Paso 4 – SSL de CA

Figura 58. Paso 5 – SSL de CA

2.8.1.8. Creación de clave cC CA

Con el fin de poder vincular de forma unidireccional la VM principal conocida como CA, con la VM secundaria, como se evidencio en el apartado Arquitectura, se debe proceder a crear el par de claves necesario para establecer la relación de confianza entre y en sentido único de CA a Sub-CA | RA, como se puede observar a continuación:

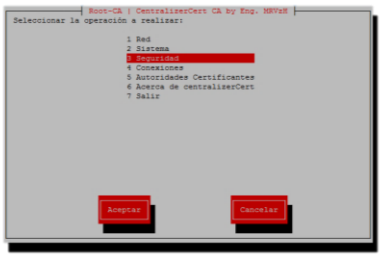

Figura 59. Paso 1 – Creación de clave de cC CA

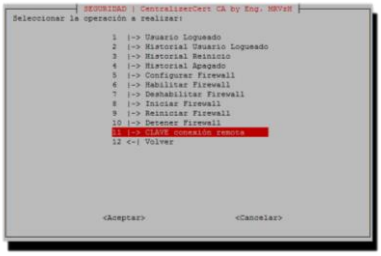

Figura 60. Paso 2 – Creación de clave cC CA

Figura 61. Paso 3 – Creación de clave cC CA

Figura 62. Paso 4 – Creación de clave cC CA

2.8.1.9. Denuncia de vínculo remoto

Para poder completar la relación de confianza, en este punto, es necesario proceder a denunciar el vínculo remoto, denominado equipo, por medio del cual se podrá establecer la relación unidireccional para su posterior sincronización:

Figura 63. Paso 1 – Denuncia de vinculo remoto desde cC CA

Figura 64. Paso 2 – Denuncia de vinculo remoto desde cC CA

Figura 65. Paso 3 – Denuncia de vinculo remoto desde cC CA

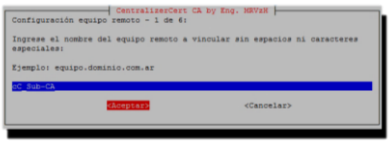

Figura 66. Paso 4 – Denuncia de vinculo remoto desde cC CA

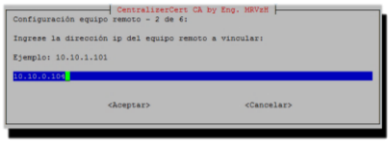

Figura 67. Paso 5 – Denuncia de vinculo remoto desde cC CA

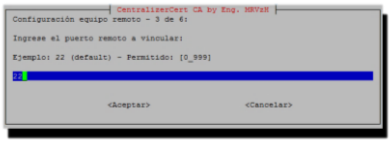

Figura 68. Paso 6 – Denuncia de vinculo remoto desde cC CA

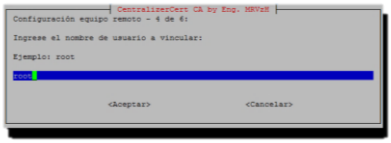

Figura 69. Paso 7 – Denuncia de vinculo remoto desde cC CA

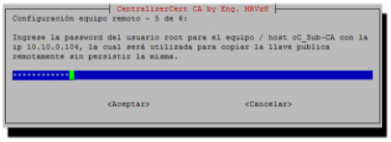

Figura 70. Paso 8 – Denuncia de vinculo remoto desde cC CA

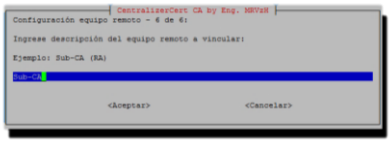

Figura 71. Paso 9 – Denuncia de vinculo remoto desde cC CA

Figura 72. Paso 10 – Denuncia de vinculo remoto desde cC CA

Sin haber podido incorporar automáticamente:

Figura 73. Paso 11A – Denuncia de vinculo remoto desde cC CA

Incorporado correctamente de manera automática:

Figura 74. Paso 11B – Denuncia de vinculo remoto desde cC CA

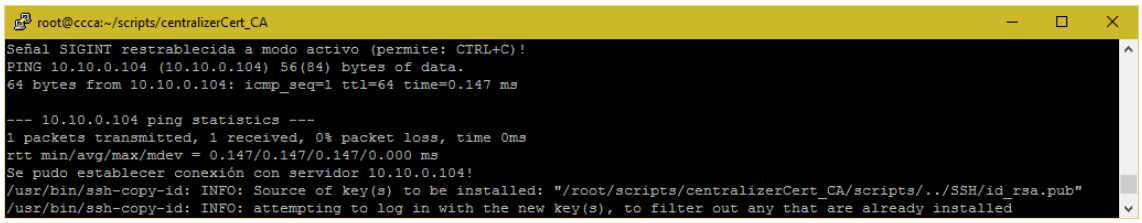

Figura 75. Paso 12 – Denuncia de vinculo remoto desde cC CA

Figura 76. Paso 13 – Denuncia de vinculo remoto desde cC CA

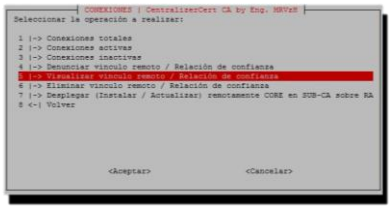

Figura 77. Paso 14 – Denuncia de vinculo remoto desde cC CA

Figura 78. Paso 15 – Denuncia de vinculo remoto desde cC CA

2.8.1.10. Despliegue de cC Sub-CA | RA

Se despliega el core de cC Sub-CA | RA remotamente desde cC CA hacia cC Sub-CA | RA, como se puede observar a continuación:

Figura 79. Paso 1 – Despliegue de core cC Sub-CA | RA desde cC CA

Figura 80. Paso 2 – Despliegue de core cC Sub-CA | RA desde cC CA

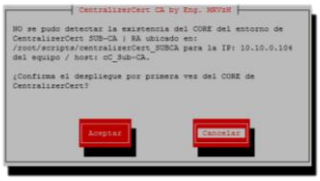

Figura 81. Paso 3 – Despliegue de core cC Sub-CA | RA desde cC CA

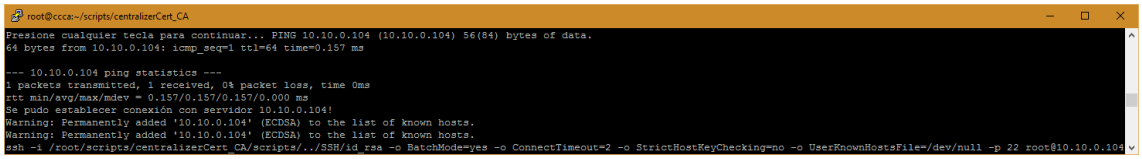

Figura 82. Paso 4 – Despliegue de core cC Sub-CA | RA desde cC CA

2.8.1.11. Despliegue de CA sobre cC Sub-CA | RA

Se despliega la CA root generada en y desde la cC CA hacia cC Sub-CA | RA como se puede observar desde la VM primaria a continuación, pasó a paso:

Figura 83. Paso 1 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 84. Paso 2 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 85. Paso 3 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 86. Paso 4 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 87. Paso 5 – Despliegue de CA base hacia cC Sub-CA | RA

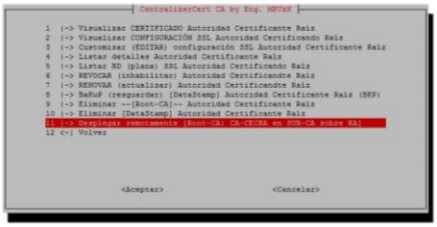

Figura 88. Paso 6 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 89. Paso 7 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 90. Paso 8 – Despliegue de CA base hacia cC Sub-CA | RA

Figura 91. Paso 9 – Despliegue de CA base hacia cC Sub-CA | RA

2.8.1.12. Salir

Para salir de cC CA, solo bastara desde el menú principal, ingresar a la opción de menú salir, y confirmar la acción, como se ve a continuación:

Figura 92. Paso 1 – Salir de cC CA

Figura 93. Paso 2 – Salir de cC CA

Figura 94. Paso 3 – Salir de cC CA

En este punto, y una vez finalizado el uso de cC CA, por cuestiones no solo operativas, sino también de seguridad, la recomendación es bajar el servicio, es decir, realizar un apagado controlado de la CA, con el fin de resguardar la misma, hasta tanto se cumpla su ciclo de vida; o en el peor de los casos, anticipándose a este, por un potencial riesgo determinado, el cual podría haber comprometido la CA.

2.8.2. Entorno de Sub-CA | RA

A continuación, se muestran los datos involucrados en el proceso:

2.8.2.1. Pre requisitos

Se inicializa por primera vez cC Sub-CA | RA y se instalan los pre requisitos necesarios a fin de poder utilizar la tecnología, como se muestra paso a paso:

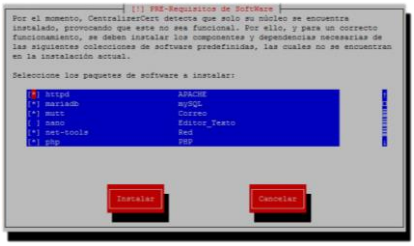

Figura 95. Paso 1 – Pre requisitos de cC Sub-CA

Figura 96. Paso 2 – Pre requisitos de cC Sub-CA

Figura 97. Paso 3 – Pre requisitos de cC Sub-CA

Figura 98. Paso 4 – Pre requisitos de cC Sub-CA

2.8.2.2. Inicio

Se inicia cC Sub-CA | RA y su entorno operativo:

Figura 99. Paso 1 – Inicio de cC Sub-CA | RA

Figura 100. Paso 2 – Inicio de cC Sub-CA | RA

Figura 101. Paso 3 – Inicio de cC Sub-CA | RA

2.8.2.3. Archivo de configuración global

Se visualiza el archivo pre configurado nativamente:

Figura 102. Paso 1 – Configuración global pre existente cC Sub-CA | RA

Figura 103. Paso 2 – Configuración global pre existente cC Sub-CA | RA

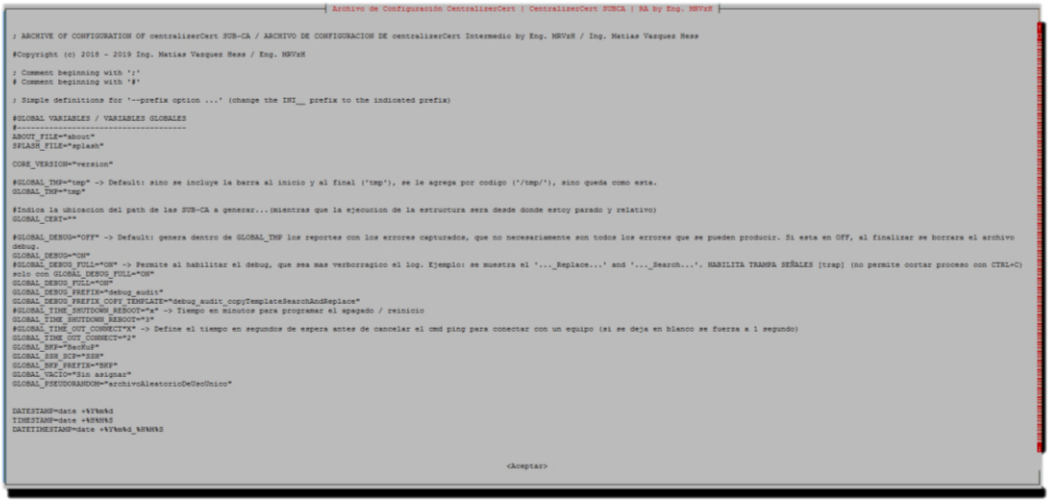

Figura 104. Paso 3 – Configuración global pre existente cC Sub-CA | RA

Figura 105. Paso 4 – Configuración global pre existente cC Sub-CA | RA

Figura 106. Paso 5 – Configuración global pre existente cC Sub-CA | RA

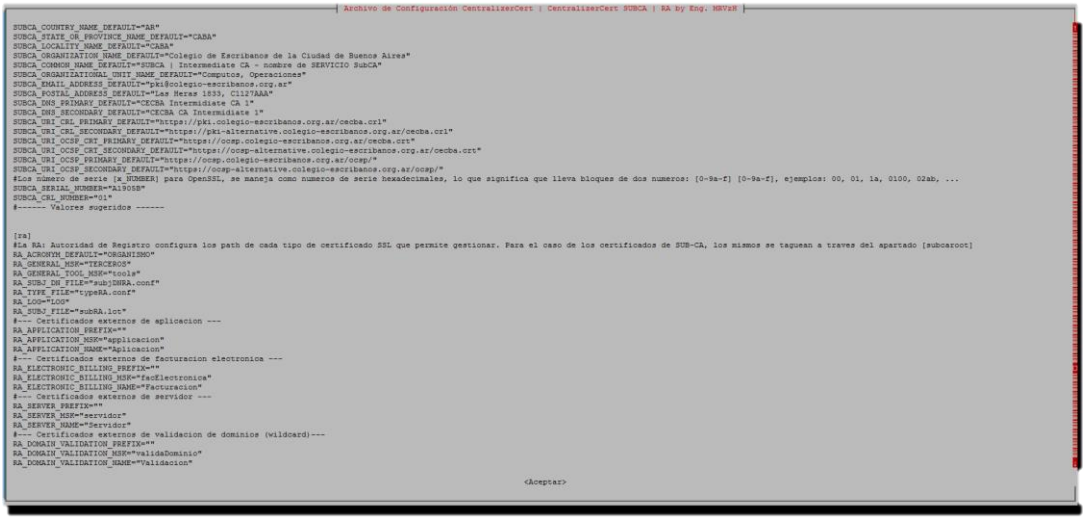

Figura 107. Paso 6 – Configuración global pre existente cC Sub-CA | RA

Figura 108. Paso 7 – Configuración global pre existente cC Sub-CA | RA

Para mayor información, respecto al detalle de cada entrada del archivo de configuración global de cC Sub-CA | RA, ver: Config.ini: cC Sub-CA | RA.

2.8.2.4. Configurar Base de Datos

De acuerdo a las funciones contenidas dentro del appliance desarrollado, se facilita la creación de la base de datos mediante un wizard muy simple y automatizado, que encapsula y delega la responsabilidad, como se podrá ver a continuación:

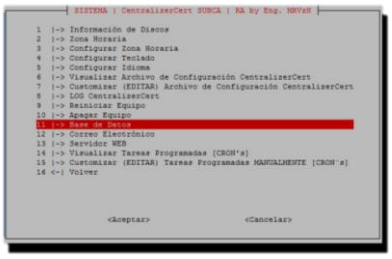

Figura 109. Paso 1 – Configurar base de datos de la RA

Figura 110. Paso 2 – Configurar base de datos de la RA

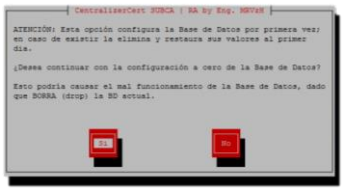

Figura 111. Paso 3 – Configurar base de datos de la RA

Figura 112. Paso 4 – Configurar base de datos de la RA

2.8.2.5. Configurar Correo Electrónico

De acuerdo a las funciones contenidas dentro del appliance desarrollado, se facilita la creación del buzón de correo mediante un wizard muy simple y automatizado especialmente diseñado, que encapsula y delega la responsabilidad, como se podrá apreciar a continuación:

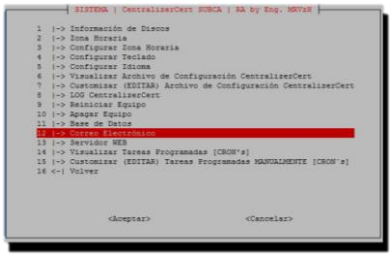

Figura 113. Paso 1 – Configurar correo electrónico de la RA

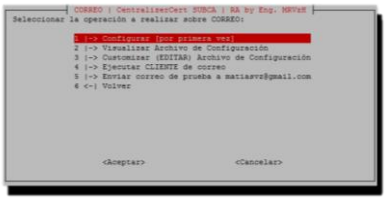

Figura 114. Paso 2 – Configurar correo electrónico de la RA

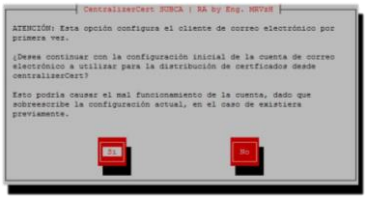

Figura 115. Paso 3 – Configurar correo electrónico de la RA

Figura 116. Paso 4 – Configurar correo electrónico de la RA

2.8.2.6. Configurar Servidor Web

De acuerdo a las funciones contenidas dentro del appliance desarrollado, se facilita la creación del servidor web mediante un wizard muy simple y automatizado, que encapsula y delega la responsabilidad, como se podrá visualizar:

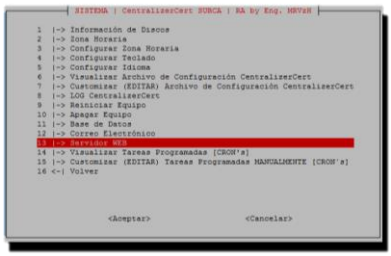

Figura 117. Paso 1 – Configurar servidor web de la RA

Figura 118. Paso 2 – Configurar servidor web de la RA

Figura 119. Paso 3 – Configurar servidor web de la RA

Figura 120. Paso 4 – Configurar servidor web de la RA

2.8.2.7. Configuraciones generales

Obedeciendo a las funciones contenidas dentro de la VM, se facilita la gestión de servicios existentes dentro del appliance virtual, mediante menú intuitivo, simple y automatizado. En el cual y para disponer de un entorno funcional, se deberá detener y desactivar el firewall como se muestra seguido a fin de acceder y visualizar correctamente el servidor web incorporado:

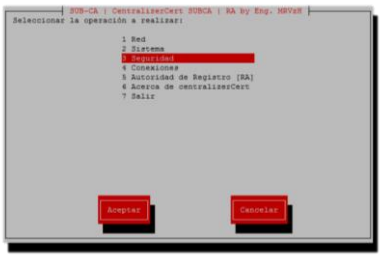

Figura 121. Paso 1 – Configuraciones generales cC Sub-CA | RA

Figura 122. Paso 2 – Configuraciones generales cC Sub-CA | RA

Figura 123. Paso 3 – Configuraciones generales cC Sub-CA | RA

Figura 124. Paso 4 – Configuraciones generales cC Sub-CA | RA

Figura 125. Paso 5 – Configuraciones generales cC Sub-CA | RA

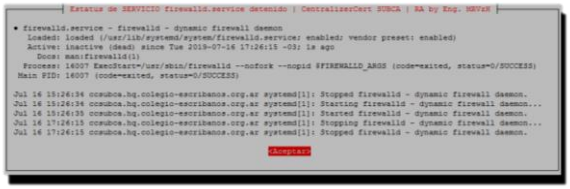

Figura 126. Paso 6 – Configuraciones generales cC Sub-CA | RA

2.8.2.8. Servidor Web

Una vez configurado el entorno como fue desarrollado, siguiendo su correspondiente hilo de secuencia, nos encontramos en condiciones de acceder al servidor apache, embebido en el appliance virtual, como se observara a continuación. El mismo por cuestiones de seguridad no muestra datos sensibles, y solo permite visualizar la información contenida, explotando la misma para la toma de decisiones. Es importante mencionar, que se limitan las operaciones WEB sobre cC Sub-CA | RA, siendo sus únicas acciones permitidas, la gestión de usuarios y alertas:

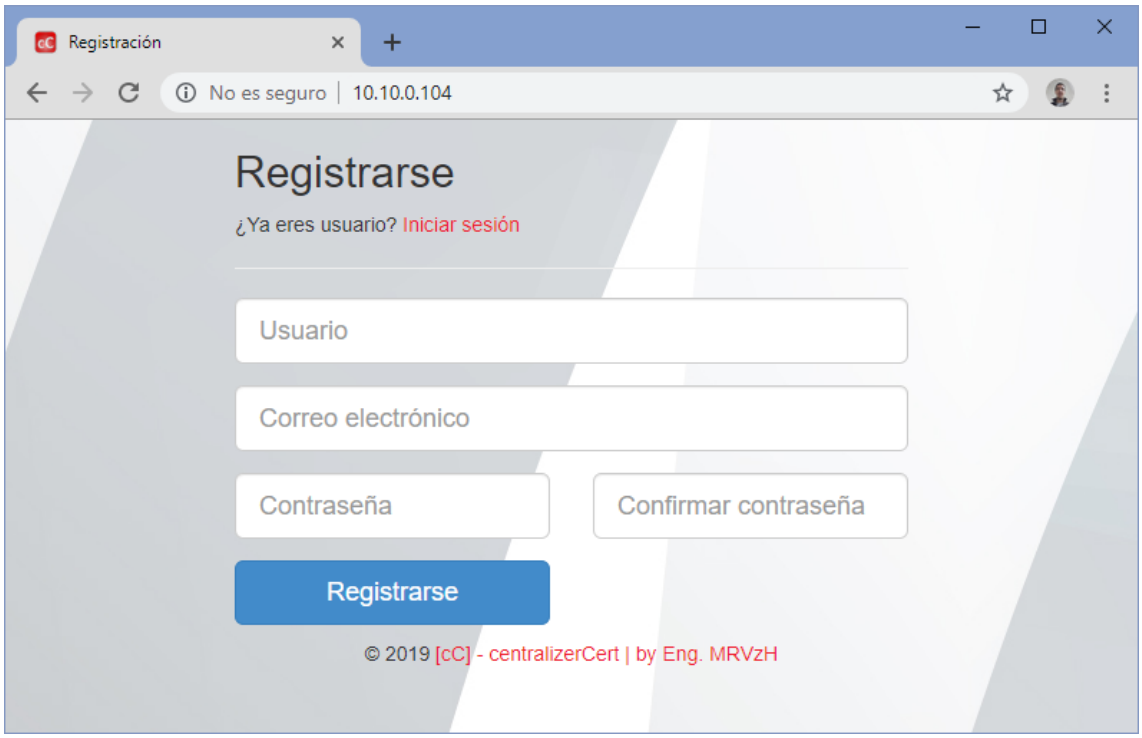

Figura 127. Paso 1 – Servidor web cC Sub-CA | RA – Registro de usuario

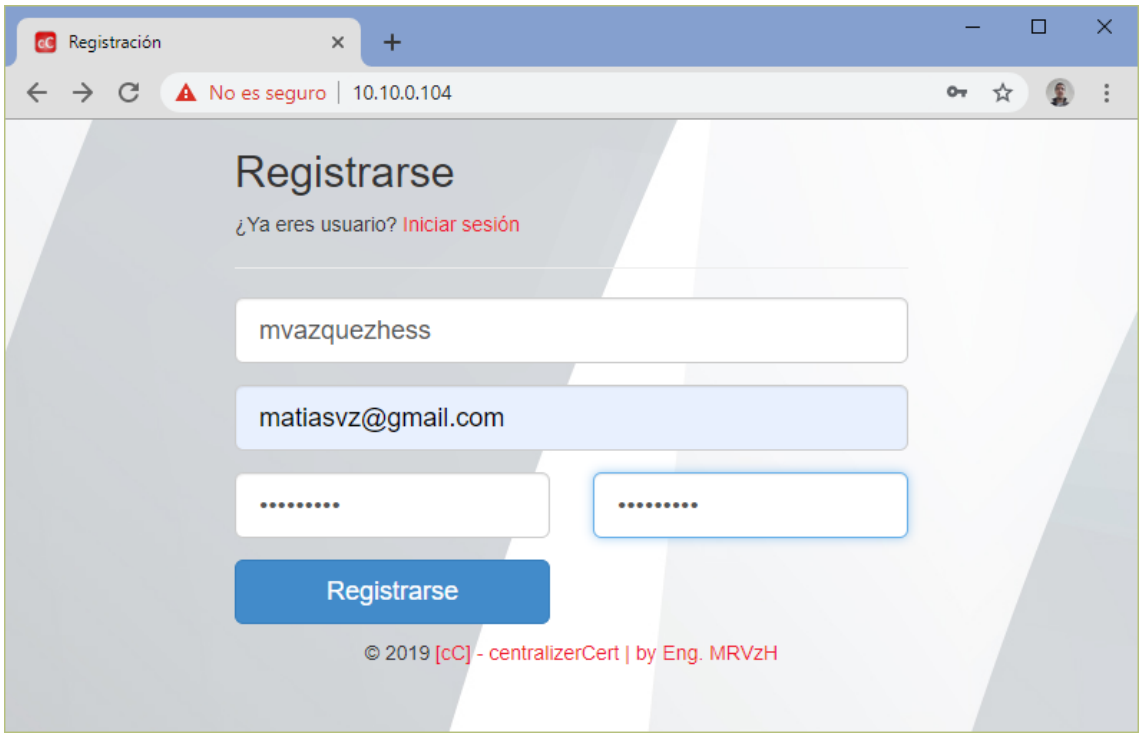

Figura 128. Paso 2 – Servidor web cC Sub-CA | RA – Registro de usuario

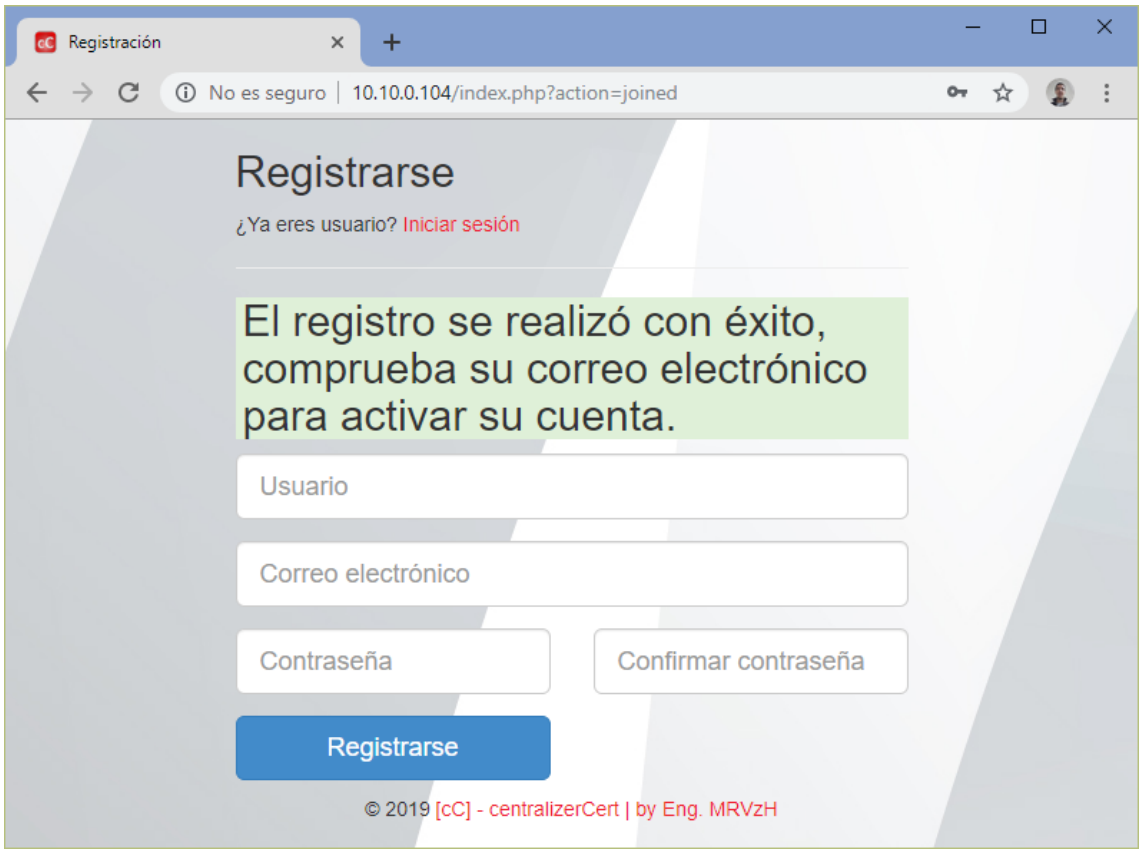

Figura 129. Paso 3 – Servidor web cC Sub-CA | RA – Registro de usuario

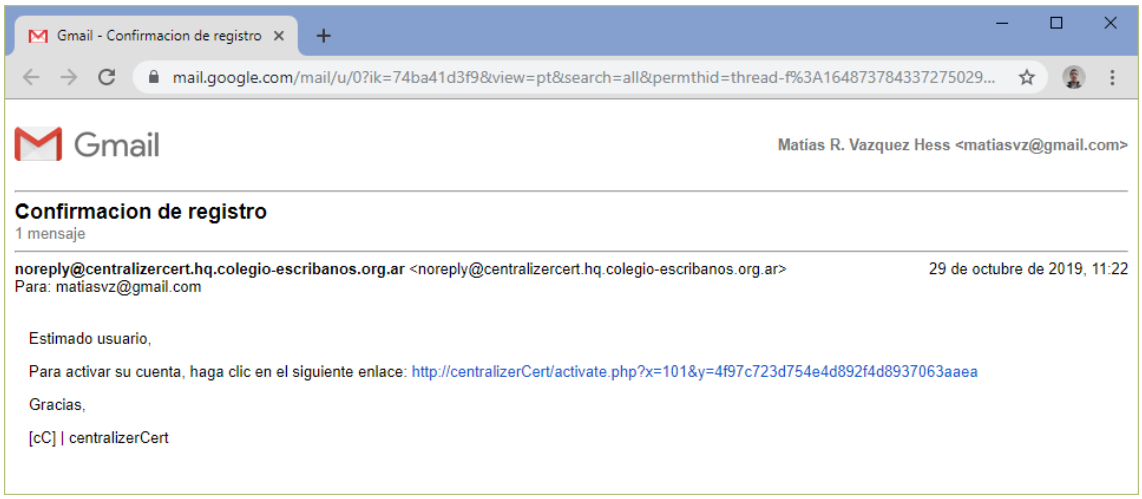

Figura 130. Paso 4 – Servidor web cC Sub-CA | RA – Recepcion de correo de registro

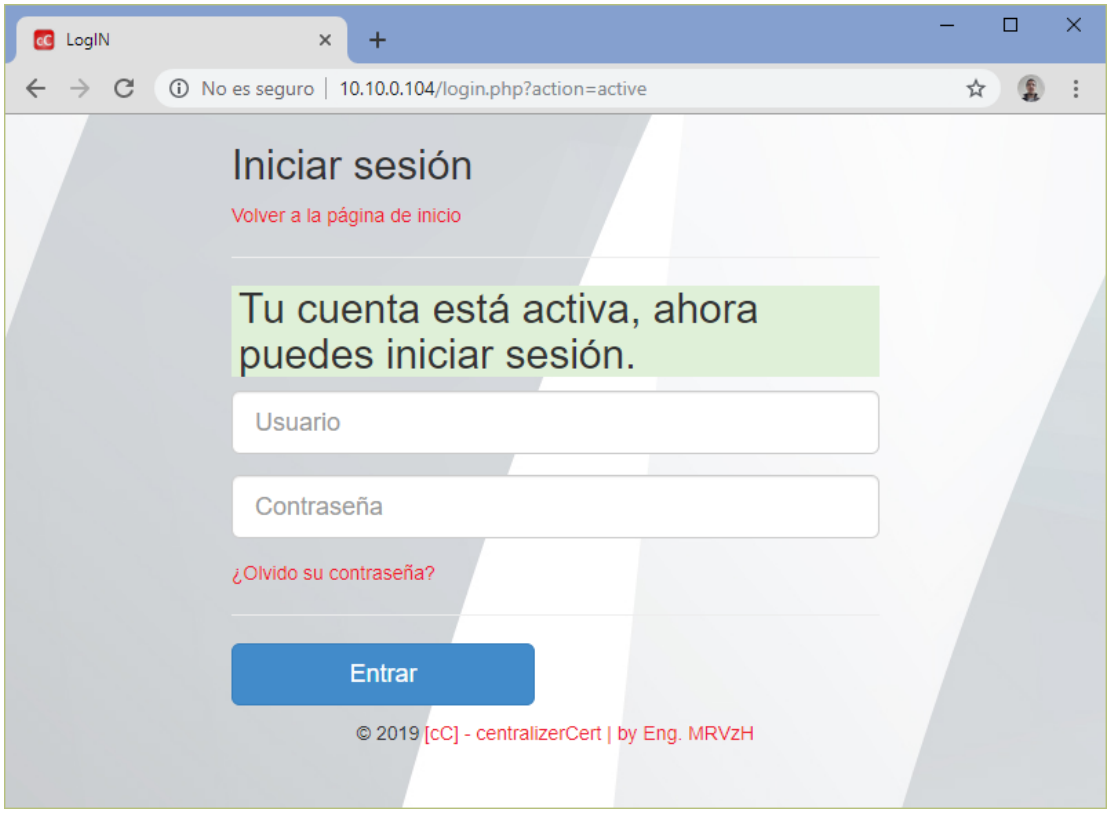

Figura 131. Paso 5 – Servidor web cC Sub-CA | RA – Activación de cuenta con enlace

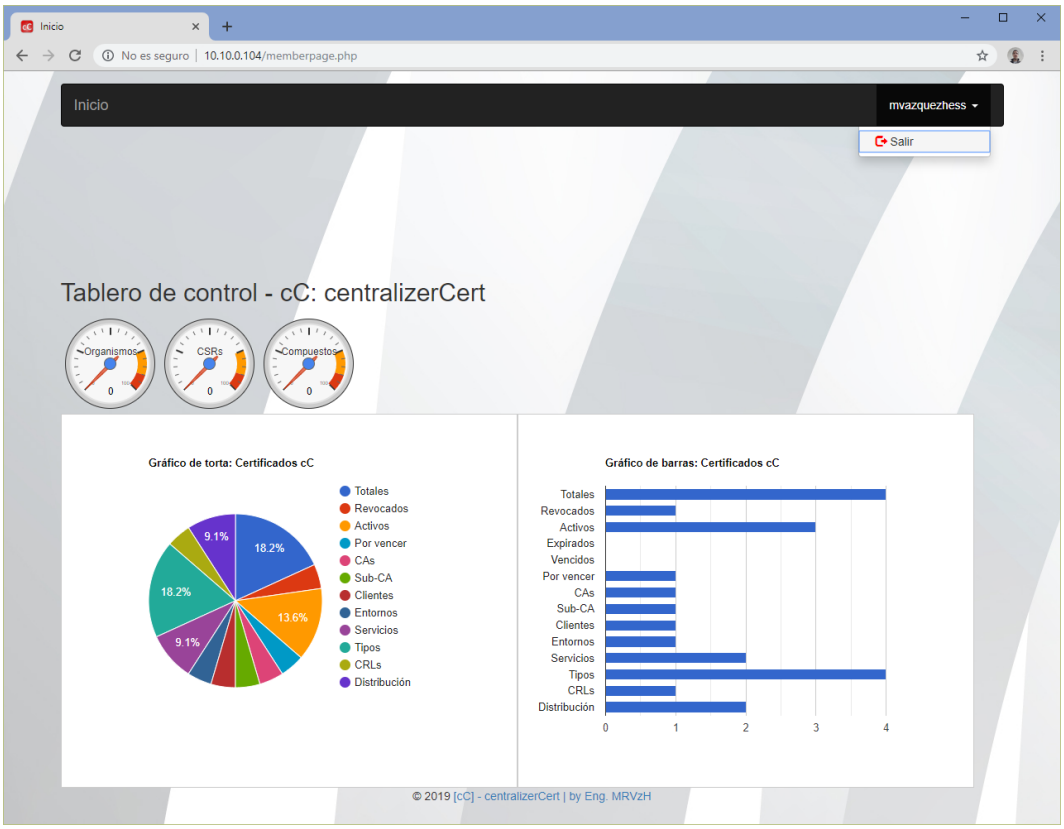

Figura 132. Paso 6 – Servidor web cC Sub-CA | RA – Acceso usuario sin privilegios

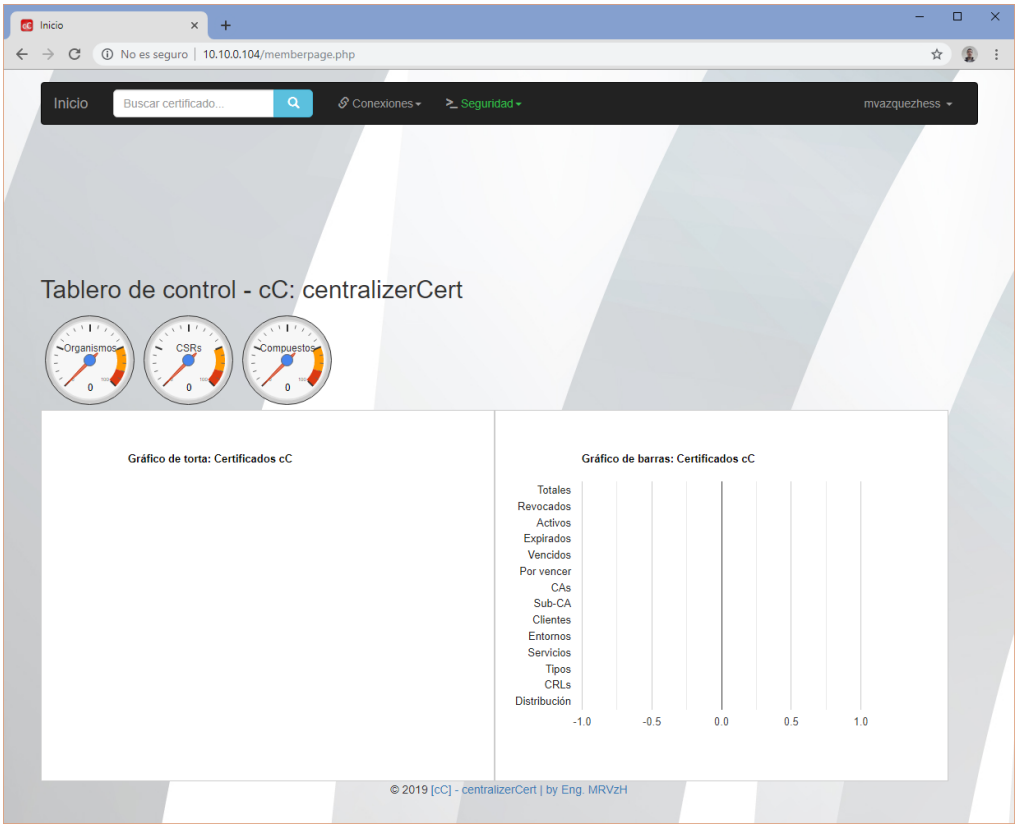

Figura 133. Paso 7 – Servidor web cC Sub-CA | RA – Acceso usuario administrador

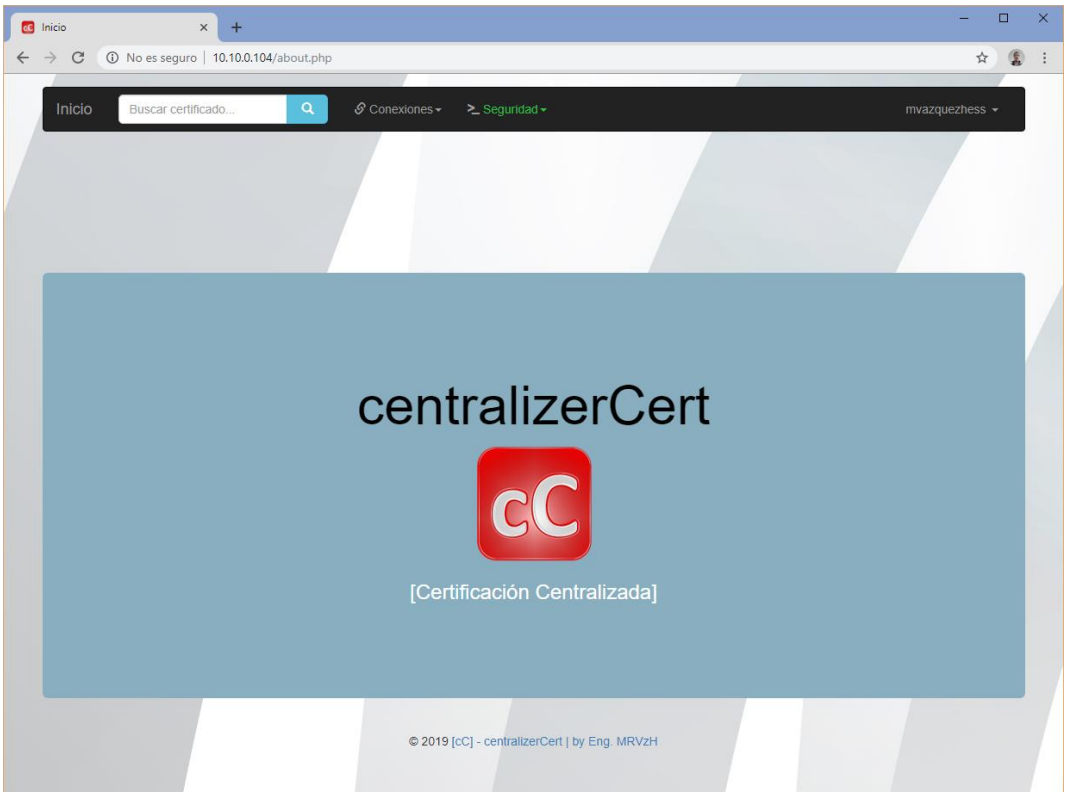

Figura 134. Paso 8 – Servidor web cC Sub-CA | RA – Acerca de cC

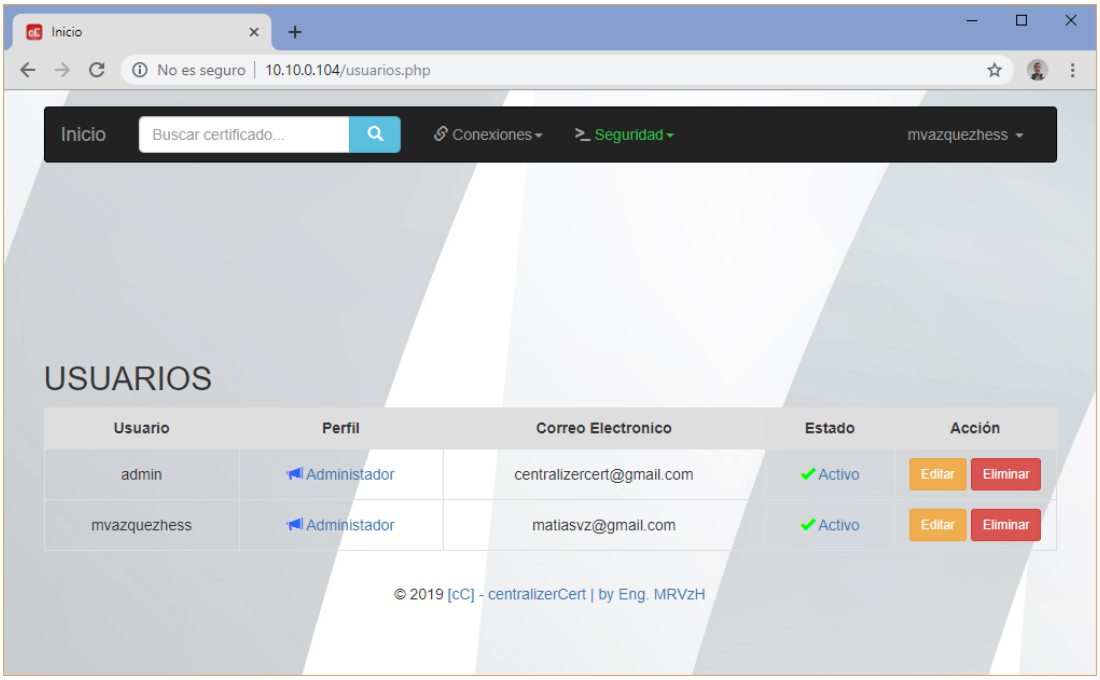

Figura 135. Paso 9 – Servidor web cC Sub-CA | RA - Usuarios

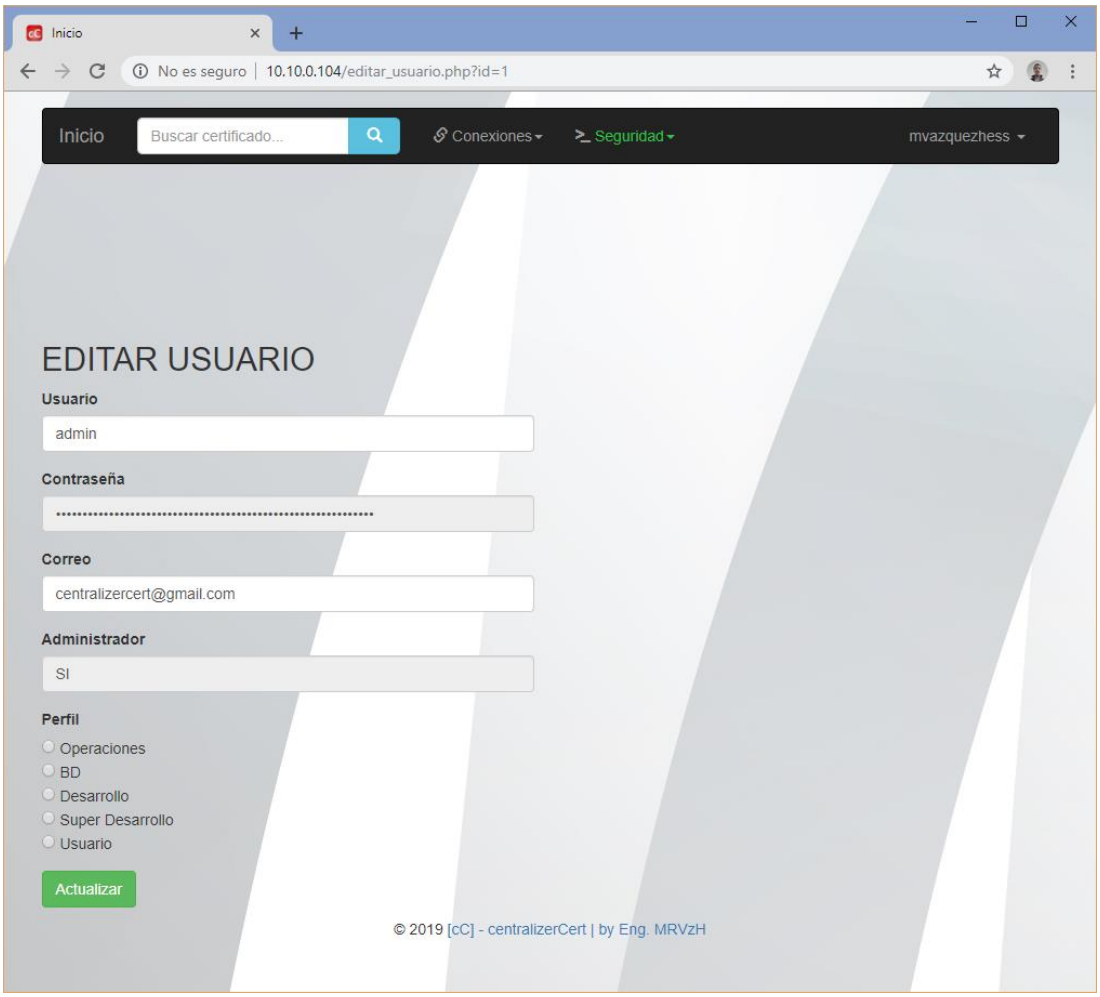

Figura 136. Paso 10 – Servidor web cC Sub-CA | RA - Usuario Administrador

2.8.2.9. Consulta de CA

Una vez configurado cC Sub-CA | RA, para comenzar a realizar operaciones sobre la Sub-CA, mediante la RA; se deberá consultar, para el caso de emisión de certificados, la existencia de CA's root, mediante el despliegue previo oportunamente realizado. Esto permitirá, basar la Sub-CA, como se visualiza a continuación, sobre una CA determinada, de acuerdo al universo de CA existentes por entorno desplegado desde cC CA previamente:

Figura 137. Paso 1 – Consulta de CA's disponibles desde RA

Figura 138. Paso 2 – Consulta de CA's disponibles desde RA

Figura 139. Paso 3 – Consulta de CA's disponibles desde RA

Figura 140. Paso 4 – Consulta de CA's disponibles desde RA

En el caso de no existir CA's root desplegadas previamente para el entorno en cuestión:

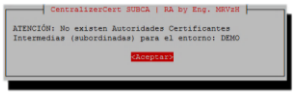

Figura 141. Paso 5A – Consulta de CA's disponibles desde RA

En el caso de existir CA's root desplegadas previamente para el entorno en cuestión:

Figura 142. Paso 5B – Consulta de CA's disponibles desde RA

Figura 143. Paso 6 – Consulta de CA's disponibles desde RA

2.8.2.10. Creación de SUB-CA

Ahora sí, estamos en condiciones de crear una nueva Sub-CA basados en una CA root, como veremos. Al igual que como se vio anteriormente sobre la CA, la Sub-CA utiliza el mismo concepto y se basa en la parametrización pre configurada, el template, las sugerencias del archivo global más la información introducida a demanda según corresponda. Esa conjunción dará como resultado:

Figura 144. Paso 1 – Creación de Sub-CA

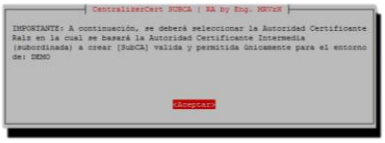

Figura 145. Paso 2 – Creación de Sub-CA

Figura 146. Paso 3 – Creación de Sub-CA

Figura 147. Paso 4 – Creación de Sub-CA

Figura 148. Paso 5 – Creación de Sub-CA

Figura 149. Paso 6 – Creación de Sub-CA

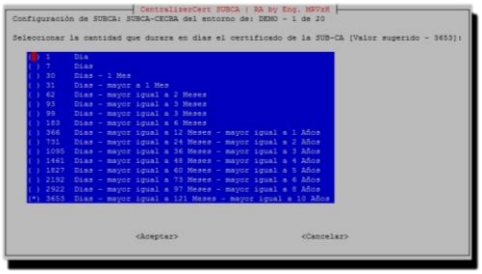

Figura 150. Paso 7 – Creación de Sub-CA

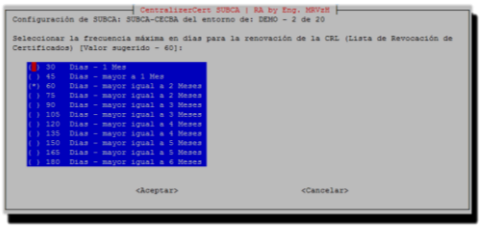

Figura 151. Paso 8 – Creación de Sub-CA

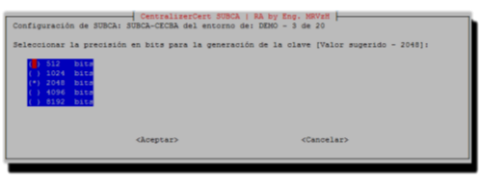

Figura 152. Paso 9 – Creación de Sub-CA

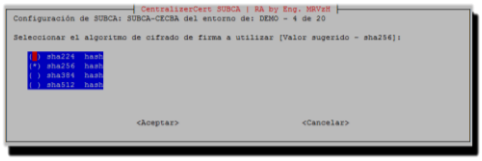

Figura 153. Paso 10 – Creación de Sub-CA

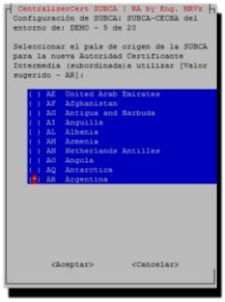

Figura 154. Paso 11 – Creación de Sub-CA

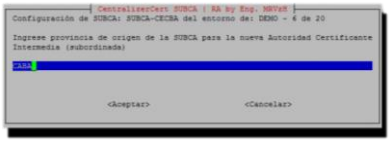

Figura 155. Paso 12 – Creación de Sub-CA

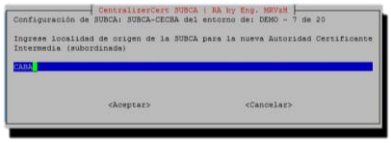

Figura 156. Paso 13 – Creación de Sub-CA

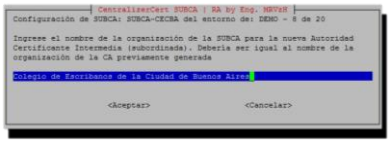

Figura 157. Paso 14 – Creación de Sub-CA

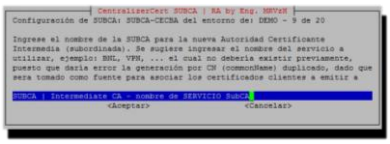

Figura 158. Paso 15 – Creación de Sub-CA

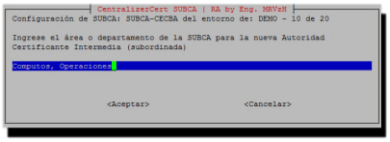

Figura 159. Paso 16 – Creación de Sub-CA

Figura 160. Paso 17 – Creación de Sub-CA

Figura 161. Paso 18 – Creación de Sub-CA

Figura 162. Paso 19 – Creación de Sub-CA

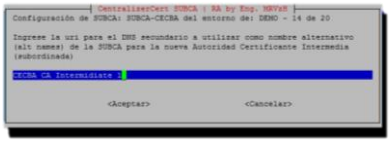

Figura 163. Paso 20 – Creación de Sub-CA

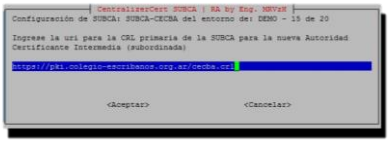

Figura 164. Paso 21 – Creación de Sub-CA

Figura 165. Paso 22 – Creación de Sub-CA

Figura 166. Paso 23 – Creación de Sub-CA

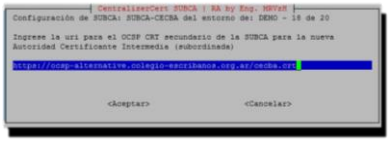

Figura 167. Paso 24 – Creación de Sub-CA

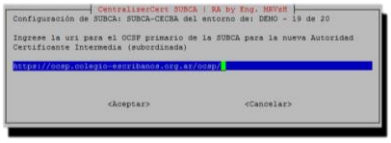

Figura 168. Paso 25 – Creación de Sub-CA

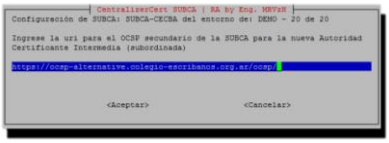

Figura 169. Paso 26 – Creación de Sub-CA

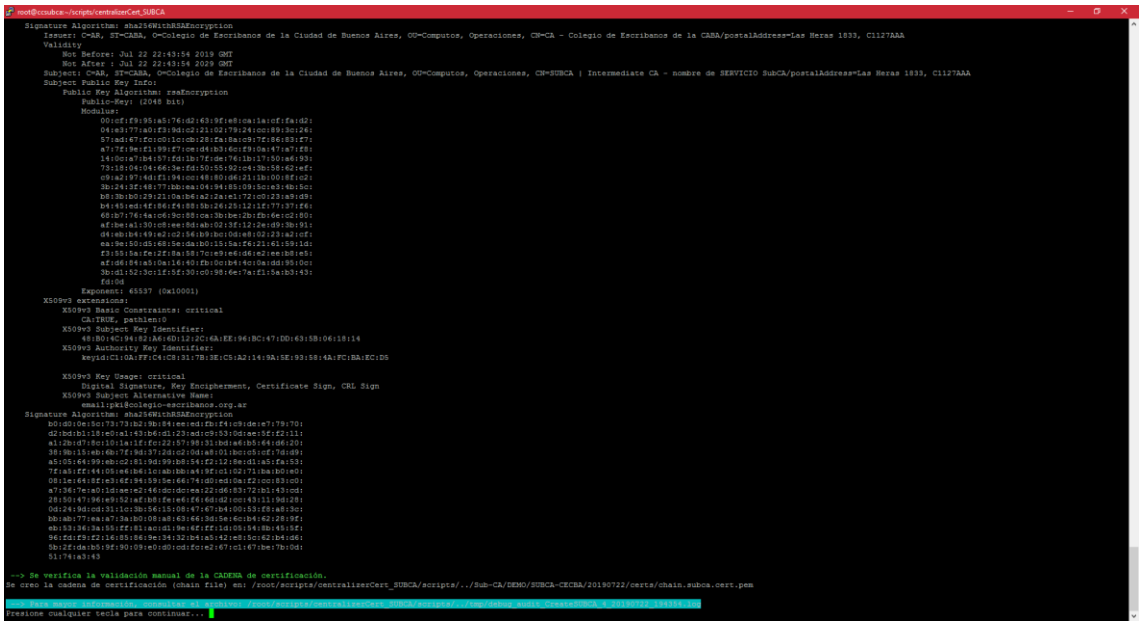

Figura 170. Paso 27 – Creación de Sub-CA

Figura 171. Paso 28 – Creación de Sub-CA

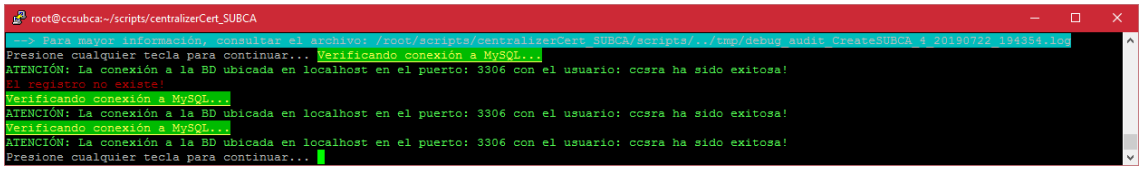

Figura 172. Paso 29 – Creación de Sub-CA

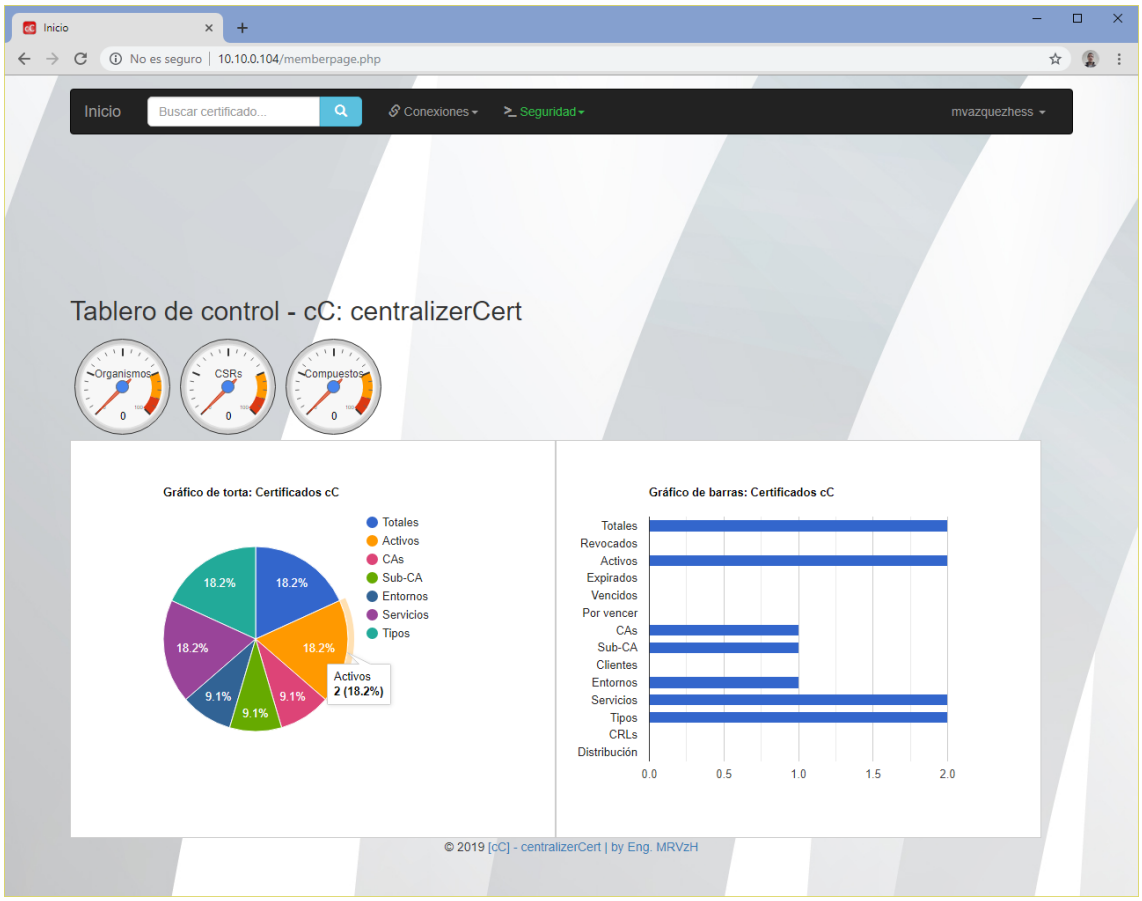

Figura 173. Paso 30 – Creación de Sub-CA

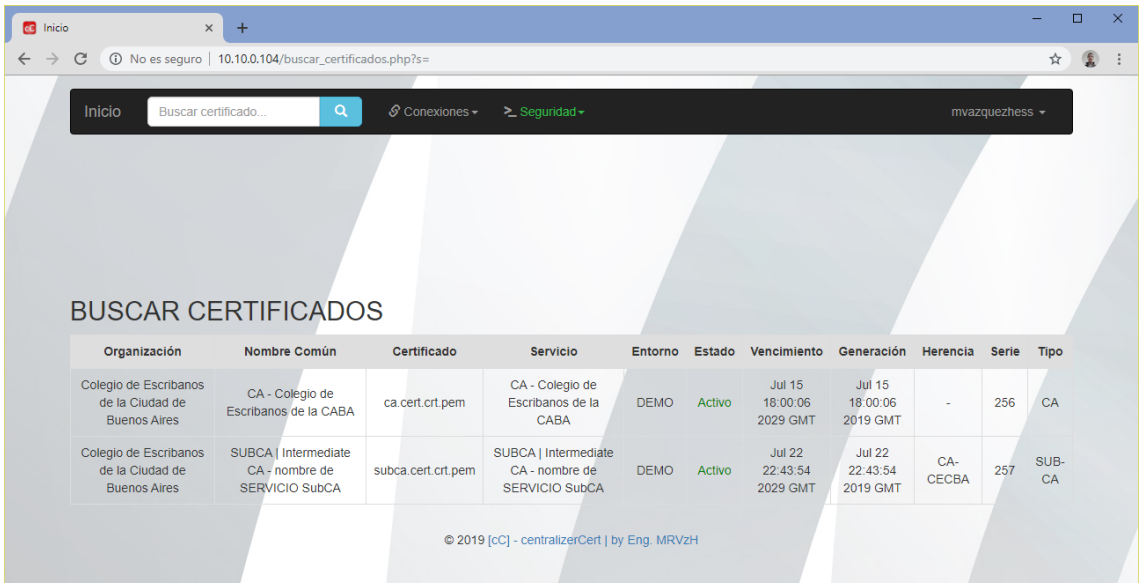

Figura 174. Paso 31 – Creación de Sub-CA

2.8.2.11. Mecánica

A continuación, se detalla el funcionamiento de los distintos estados que pueden tomar los certificados dentro de cC Sub-CA | RA:

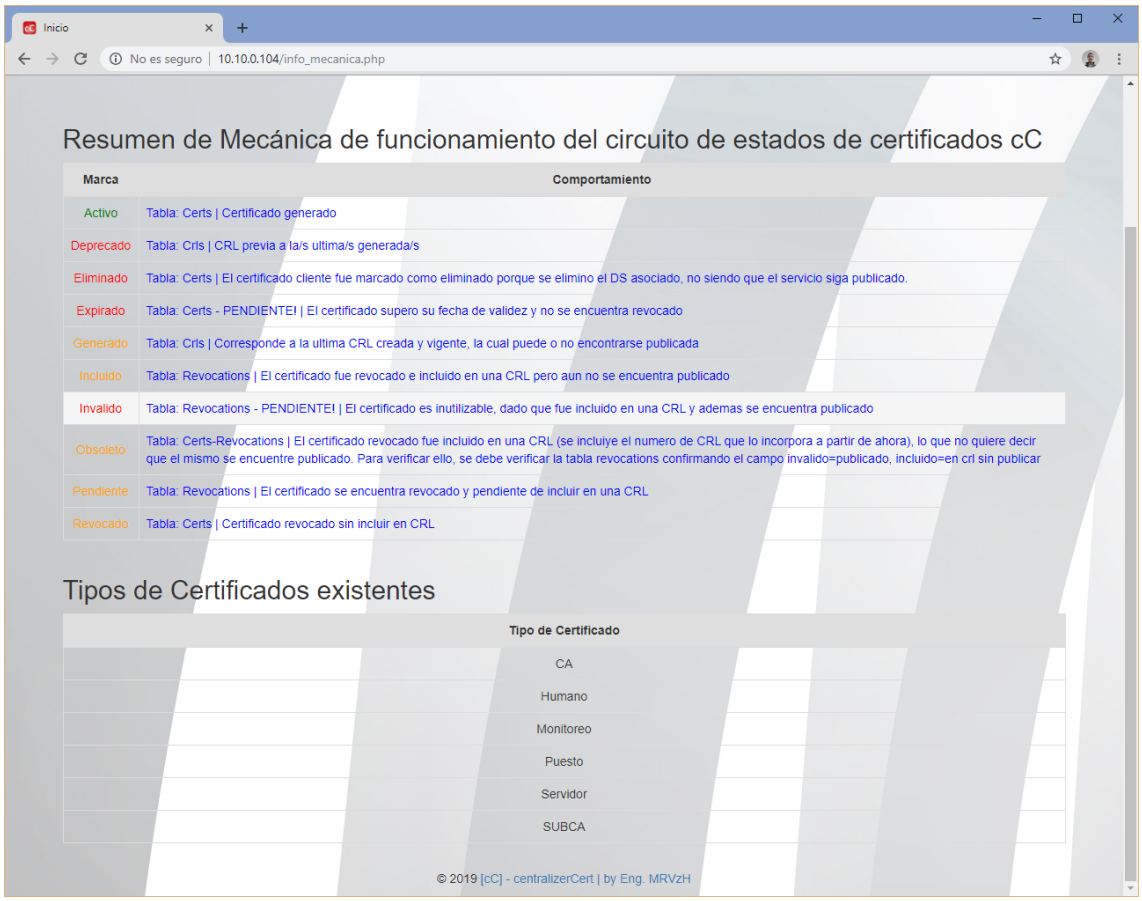

Figura 175. Mecánica de cC Sub-CA | RA

2.8.2.12. Configuración de Sub-CA

Basado en el template de la Sub-CA, la configuración de parámetros sugeridos pre cargada y los datos introducidos a demanda en el wizard de creación, generó la Sub-CA detallada a continuación:

Figura 176. Paso 1 – Ver configuración SSL de Sub-CA

Figura 177. Paso 2 – Ver configuración SSL de Sub-CA

Figura 178. Paso 3 – Ver configuración SSL de Sub-CA

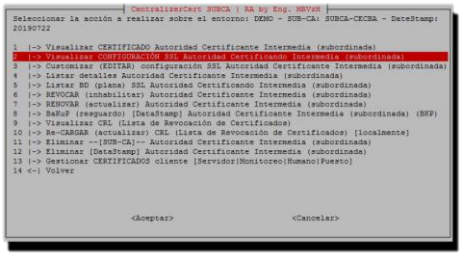

Figura 179. Paso 4 – Ver configuración SSL de Sub-CA

Figura 180. Paso 5 – SSL de Sub-CA

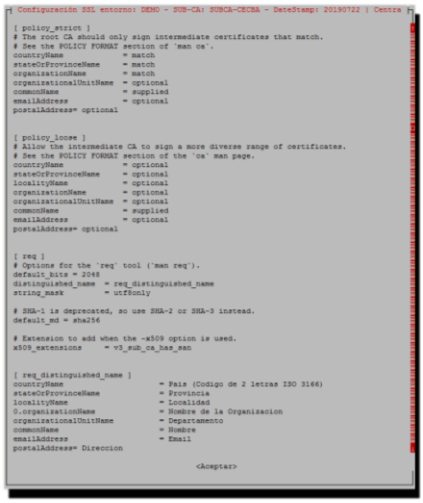

Figura 181. Paso 6 – SSL de Sub-CA

Figura 182. Paso 7 – SSL de Sub-CA

Figura 183. Paso 8 – SSL de Sub-CA

Figura 184. Paso 9 – SSL de Sub-CA

Figura 185. Paso 10 – SSL de Sub-CA

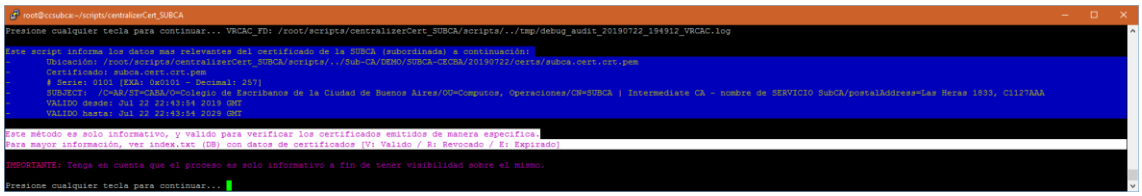

Figura 186. Paso 11 – Ver configuración SSL de Sub-CA

2.8.2.13. Base de Datos plana SSL

A continuación, se puede visualizar el corazón de SSL, correspondiente a la Sub-CA particular tomada como ejemplo, y el mecanismo para acceder al mismo:

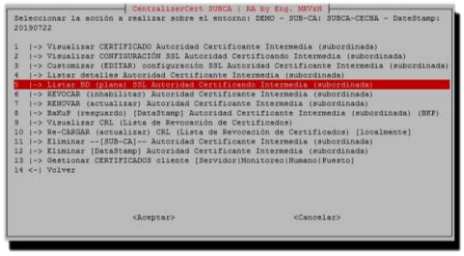

Figura 187. Paso 1 – BD plana SSL de Sub-CA

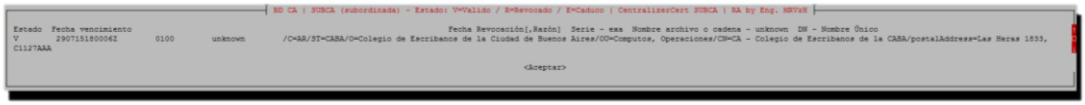

Figura 188. Paso 2 – BD plana SSL de Sub-CA

2.8.2.14. Resguardo de Base de Datos

Se encuentran disponibles, más de una alternativa de resguardo sobre mySQL, permitida mediante menú de cC Sub-CA | RA:

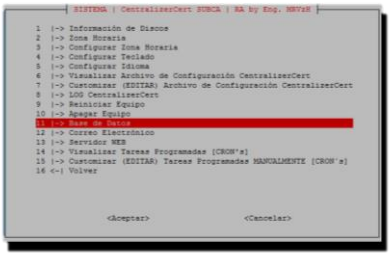

Figura 189. Paso 1 – Resguardo de BD de Sub-CA

Figura 190. Paso 2 – Resguardo de BD a demanda de Sub-CA

Figura 191. Paso 3 – Resguardo de BD a demanda de Sub-CA

Figura 192. Paso 4 – Resguardo de BD a demanda de Sub-CA

Figura 193. Paso 5 – Resguardo de BD programado de Sub-CA

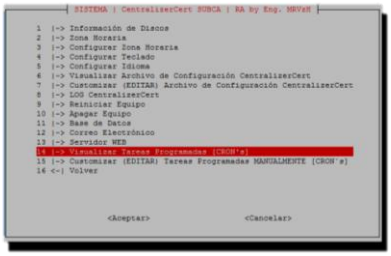

Figura 194. Paso 6 – Resguardo de BD programado de Sub-CA

Figura 195. Paso 6 – Resguardo de BD programado de Sub-CA

2.8.2.15. Consulta de CRL

A continuación, se visualiza la última lista de revocación disponible. Como es de esperar, y al no haberse creado aun, la misma no existe, como vemos a continuación:

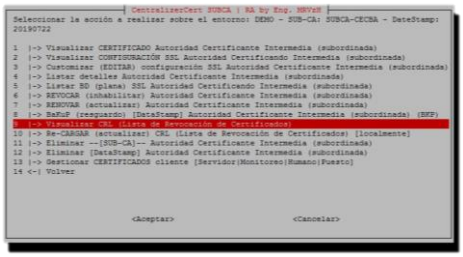

Figura 196. Paso 1 – Consulta de CRL de Sub-CA

Figura 197. Paso 2 – Consulta de CRL de Sub-CA

2.8.2.16. Re carga de CRL

En este punto, se podrá visualizar el proceso a ejecutar para re generar la lista de revocación de certificados [12] [13] para mantener operativo el servicio, de acuerdo al límite de días establecido. Este caso puntual, no incluirá certificados revocados, por no existir todavía estos:

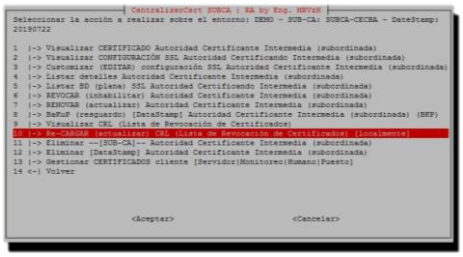

Figura 198. Paso 1 – Re carga de CRL de Sub-CA

Figura 199. Paso 2 – Re carga de CRL de Sub-CA

Figura 200. Paso 3 – Re carga de CRL de Sub-CA

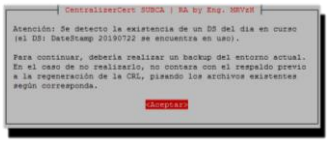

Figura 201. Paso 4 – Re carga de CRL de Sub-CA

Figura 202. Paso 5 – Re carga de CRL de Sub-CA

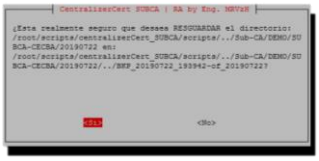

Figura 203. Paso 6 – Re carga de CRL de Sub-CA

Figura 204. Paso 7 – Re carga de CRL de Sub-CA

Figura 205. Paso 8 – Re carga de CRL de Sub-CA

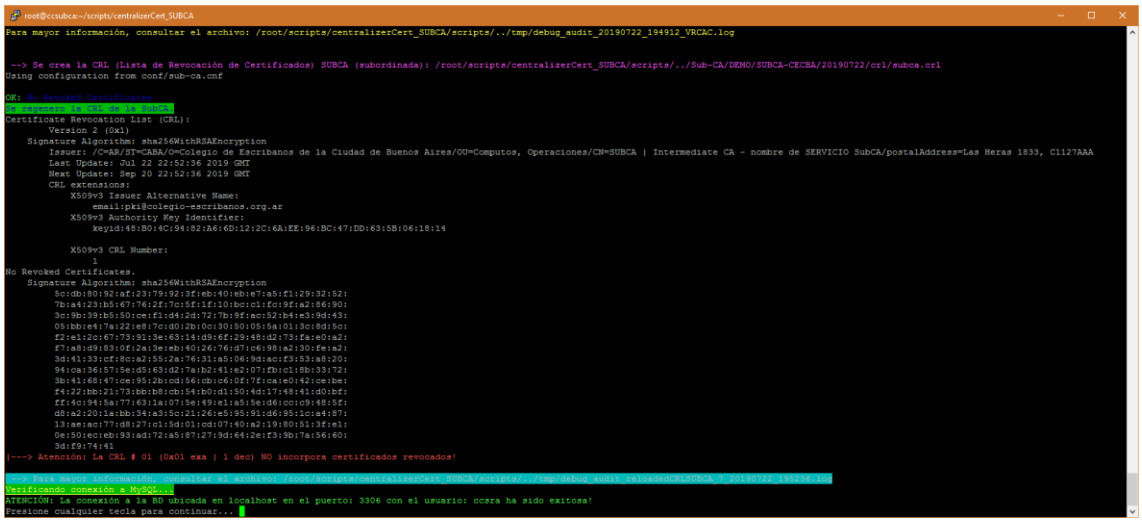

Figura 206. Paso 9 – Re carga de CRL de Sub-CA

Figura 207. Paso 10 – Re carga de CRL de Sub-CA

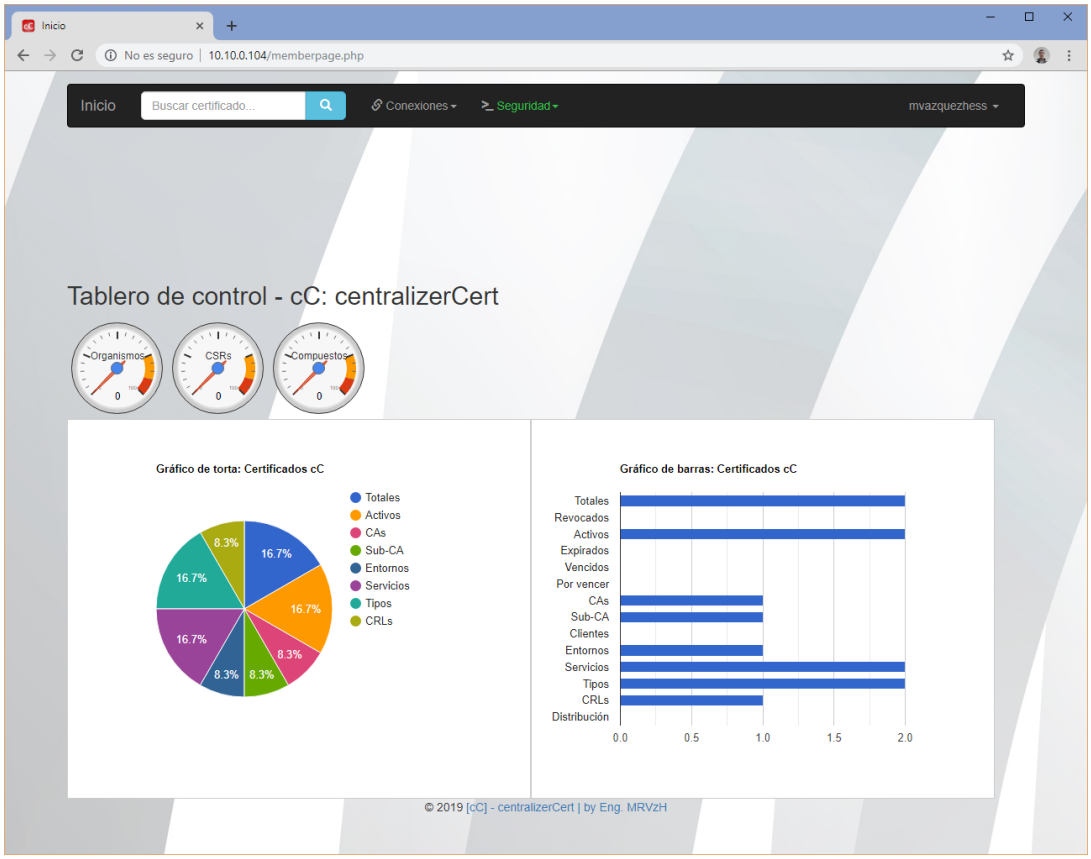

Figura 208. Paso 11 – Re carga de CRL de Sub-CA

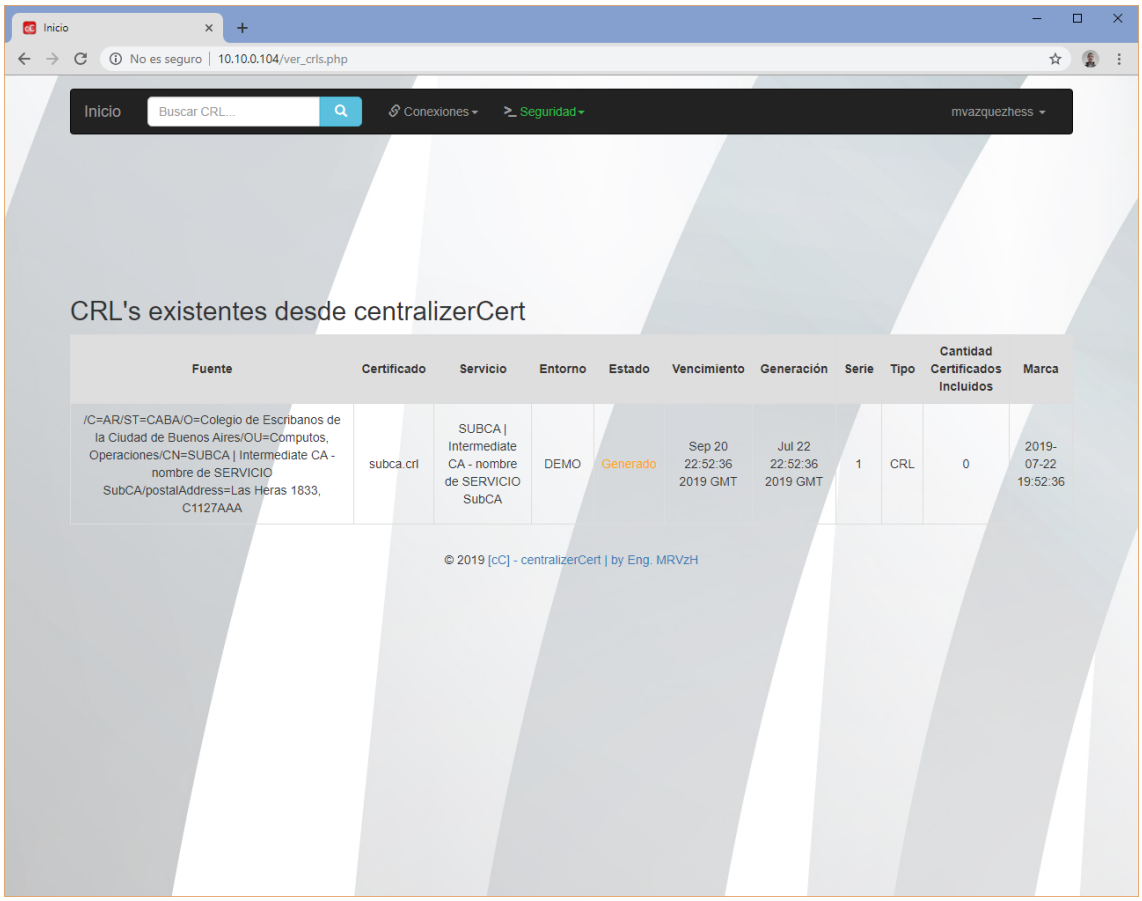

Figura 209. Paso 12 – Re carga de CRL de Sub-CA

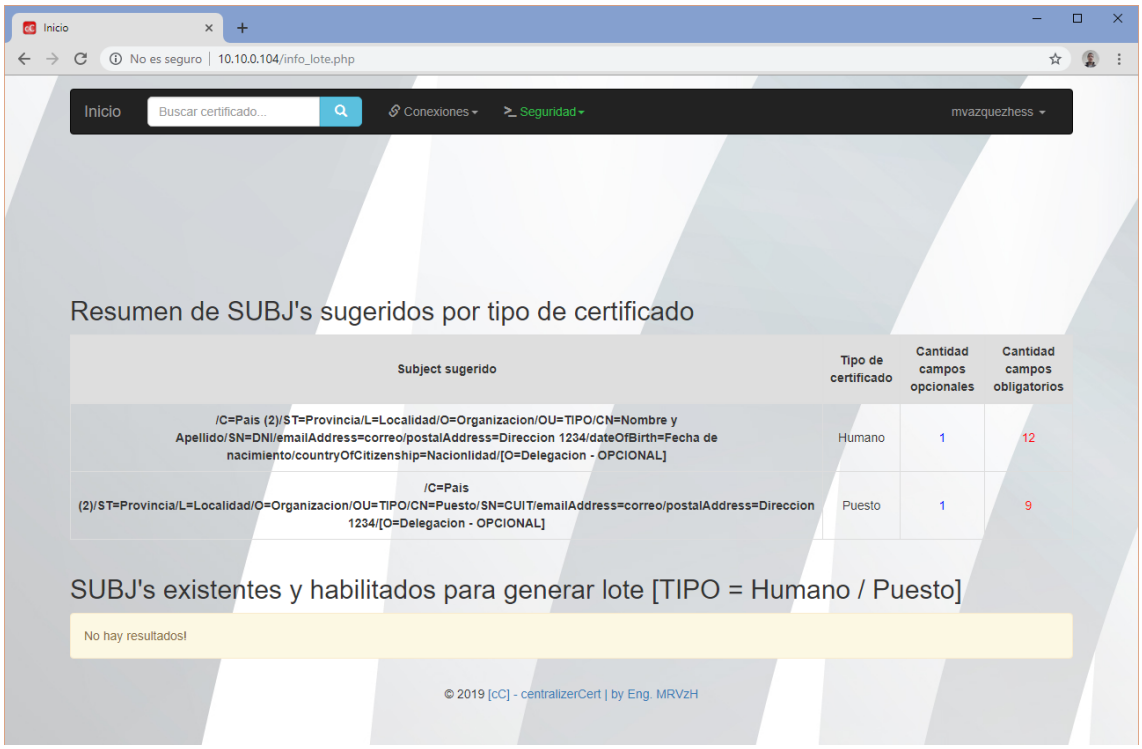

Figura 210. Paso 12 – Re carga de CRL de Sub-CA

2.8.2.17. Gestión de certificados

Corresponde al punto de entrada para la gestión de certificados cliente de la Sub-CA:

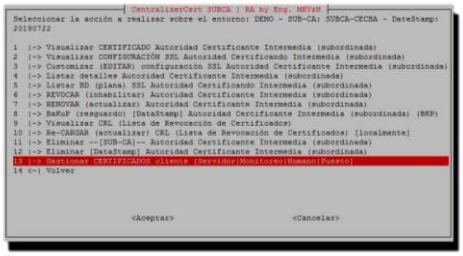

Figura 211. Gestión de Certificados cliente

2.8.2.17.1. Consulta de certificados cliente

Corresponde a los certificados emitidos por la Sub-CA, al momento de realizar la consulta, como se verá a continuación:

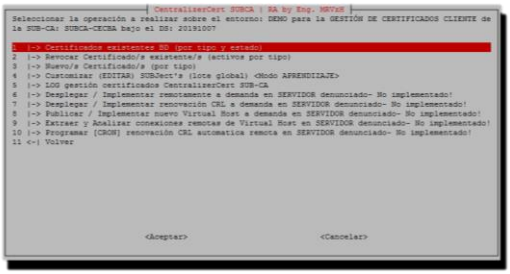

Figura 212. Paso 1 – Consulta de certificados cliente

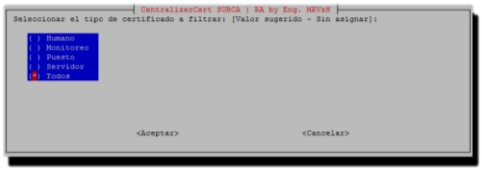

Figura 213. Paso 2 – Consulta de certificados cliente

Figura 214. Paso 3 – Consulta de certificados cliente

2.8.2.17.2. Revocar certificados cliente

Es la acción que permite revocar los certificados activos emitidos por la Sub-CA, al momento de ejecutar la operación. Existen dos modalidades: Manual o Lote, siendo la diferencia entre ambas su relación, es decir, el modo Manual soporta revocación 1:1, mientras que el modo por Lote, permite revocar con una multiplicidad 1:N. En este caso puntual, y dado el hilo de ejecución actual, en este momento no existe certificado previo alguno, por lo cual no se deberá poder realizar revocación alguna, como se verá a continuación, en cualquier modalidad:

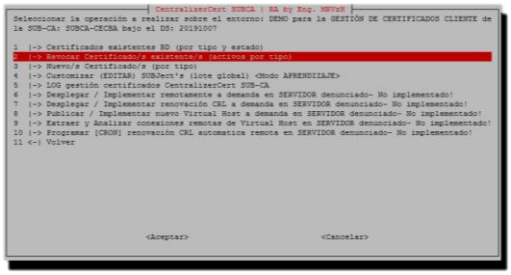

Figura 215. Paso 1 – Revocar certificados cliente

Figura 216. Paso 2 – Revocar certificados cliente

Figura 217. Paso 3 – Revocar certificados cliente

Figura 218. Paso 4 – Revocar certificados cliente

2.8.2.17.3. Nuevo certificado cliente

Es la acción que permite generar un nuevo certificado cliente a emitir por la Sub-CA activa, es decir, la Sub-CA sobre la cual se encuentra parado el operador al momento de ejecutar la operación. Esta modalidad, permite crear distintos tipos de certificados en diversas modalidades de emisión: Manual, Lote o CSR. Dependiendo de la modalidad, será el tipo de emisión soportada, como veremos en la tabla a continuación:

Modalidad	Tipo				Relación
Manual	Humano	Puesto	Monitoreo	Servidor	1:1
Lote	Humano	Puesto	-	-	1:N
CSR	Humano	Puesto	-	-	1:1

Tabla 1. Especificación de modalidades por tipo y multiplicidad

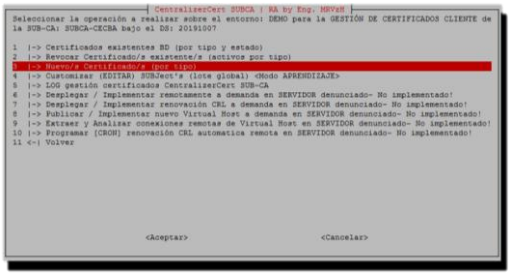

Figura 219. Nuevo certificado cliente por tipo

2.8.2.17.4. Creación de Cliente: Manual – Humano[2]

A continuación, se proceda a la creación de certificado en modalidad manual de tipo humano:

Figura 220. Paso 1 – Crear certificado cliente humano manual

[2] Se deberá tener en cuenta que el proceso de creación de certificados de cliente en modalidad diferente a CSR, implicará la distribución de este mediante correo electrónico en formato .PFX, el cual, en este caso puntual, será visto a posterior de forma completa en Distribución de Cliente: Manual – Puesto por ejemplo.

Figura 221. Paso 2 – Crear certificado cliente humano manual

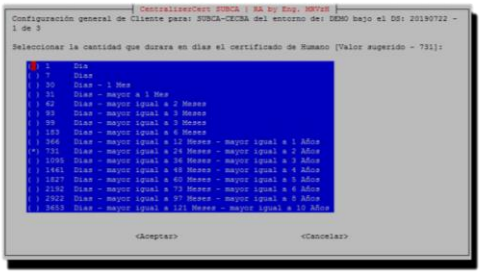

Figura 222. Paso 3 – Crear certificado cliente humano manual

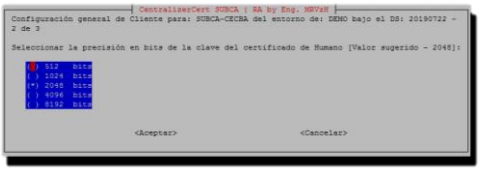

Figura 223. Paso 4 – Crear certificado cliente humano manual

Figura 224. Paso 5 – Crear certificado cliente humano manual

Figura 225. Paso 6 – Crear certificado cliente humano manual

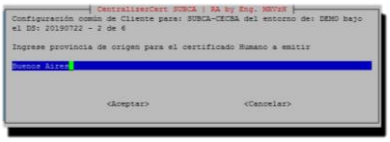

Figura 226. Paso 7 – Crear certificado cliente humano manual

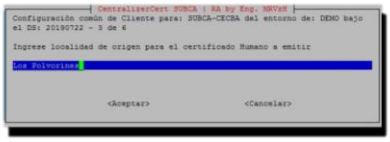

Figura 227. Paso 8 – Crear certificado cliente humano manual

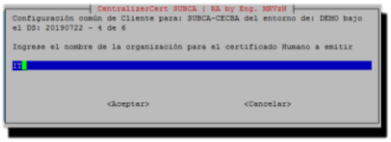

Figura 228. Paso 9 – Crear certificado cliente humano manual

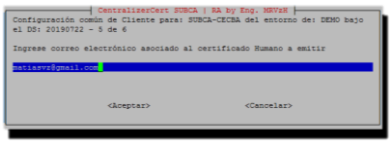

Figura 229. Paso 10 – Crear certificado cliente humano manual

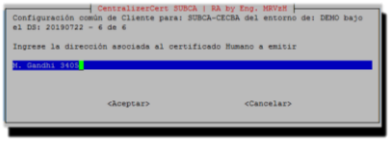

Figura 230. Paso 11 – Crear certificado cliente humano manual

Figura 231. Paso 12 – Crear certificado cliente humano manual

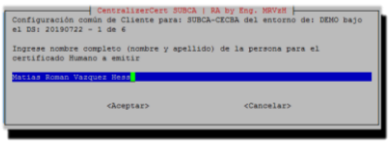

Figura 232. Paso 13 – Crear certificado cliente humano manual

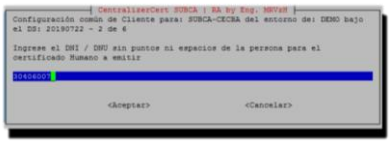

Figura 233. Paso 14 – Crear certificado cliente humano manual

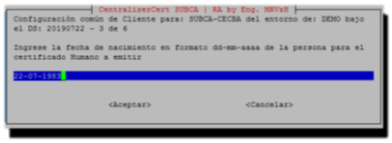

Figura 234. Paso 15 – Crear certificado cliente humano manual

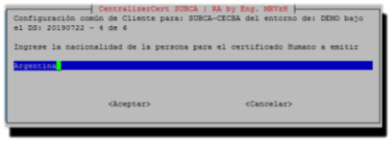

Figura 235. Paso 16 – Crear certificado cliente humano manual

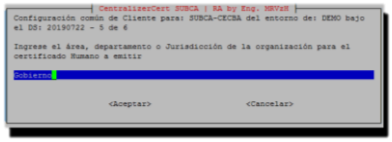

Figura 236. Paso 17 – Crear certificado cliente humano manual

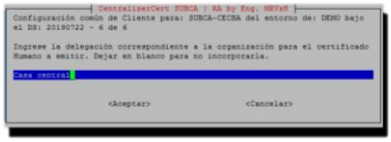

Figura 237. Paso 18 – Crear certificado cliente humano manual

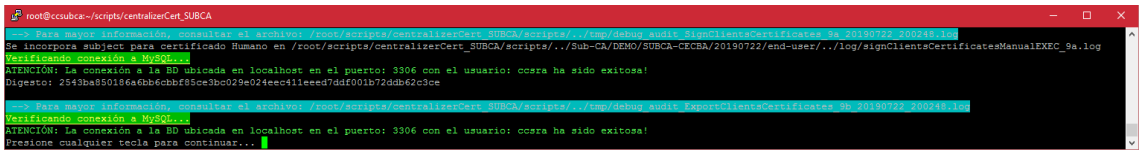

Figura 238. Paso 19 – Crear certificado cliente humano manual

Figura 239. Paso 20 – Crear certificado cliente humano manual

Figura 240. Paso 21 – Crear certificado cliente humano manual

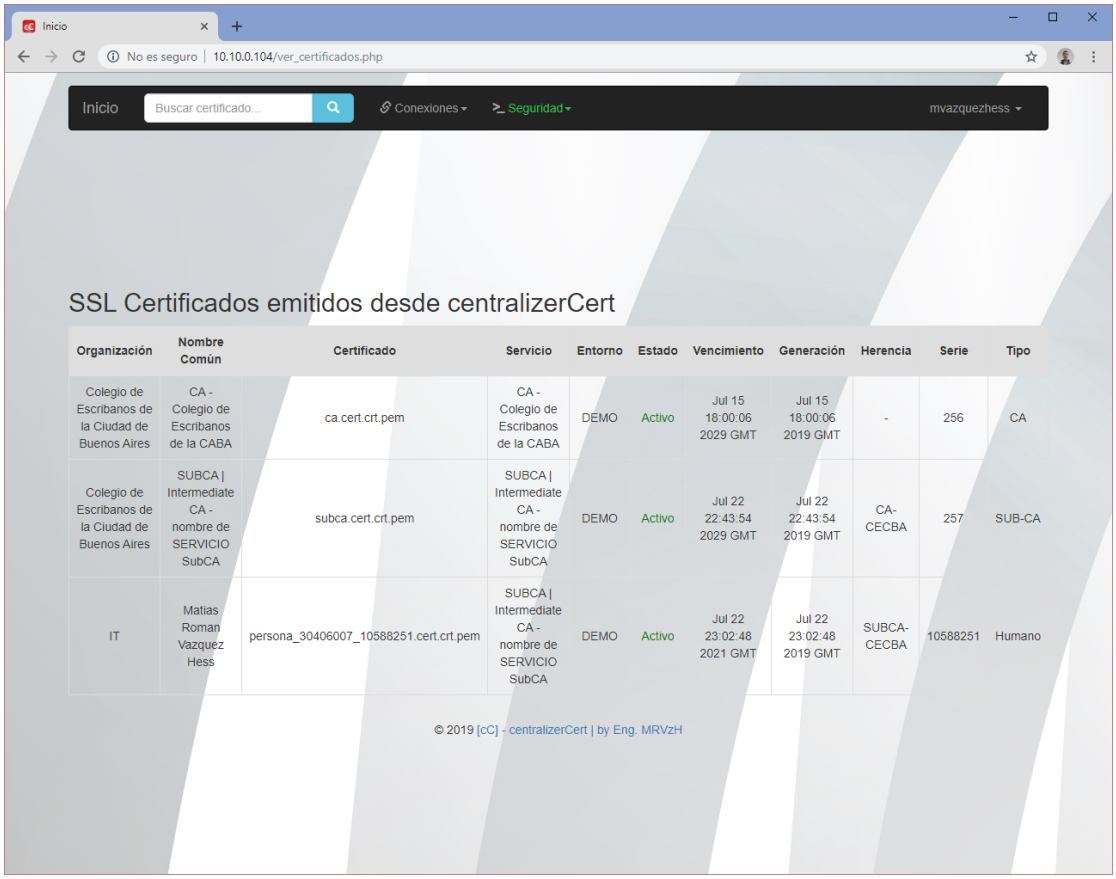

Figura 241. Paso 22 – Crear certificado cliente humano manual

2.8.2.17.5. Revocación de Cliente

En esta instancia, se revocará el certificado cliente anteriormente creado, como se podrá apreciar a continuación:

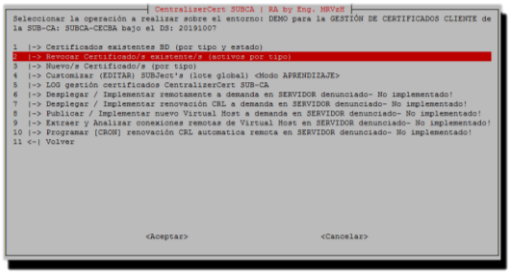

Figura 242. Paso 1 – Revocar certificado cliente humano manual

Figura 243. Paso 2 – Revocar certificado cliente humano manual

Figura 244. Paso 3 – Revocar certificado cliente humano manual

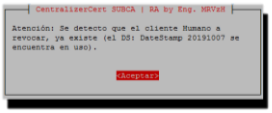

Figura 245. Paso 4 – Revocar certificado cliente humano manual

Figura 246. Paso 5 – Revocar certificado cliente humano manual

Figura 247. Paso 6 – Revocar certificado cliente humano manual

Figura 248. Paso 7 – Revocar certificado cliente humano manual

Figura 249. Paso 8 – Revocar certificado cliente humano manual

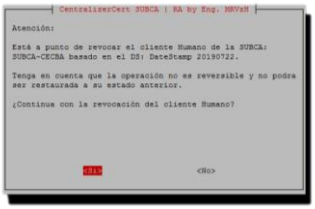

Figura 250. Paso 9 – Revocar certificado cliente humano manual

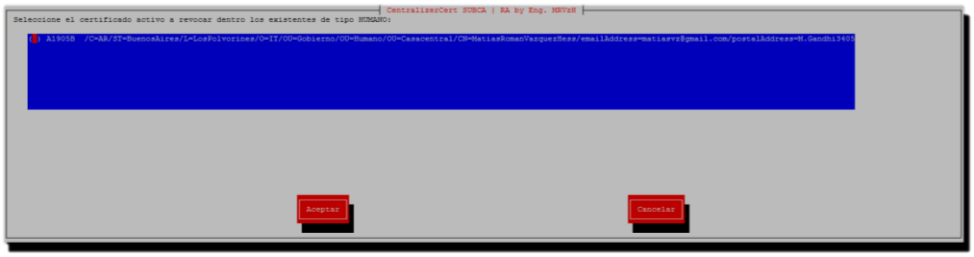

Figura 251. Paso 10 – Revocar certificado cliente humano manual

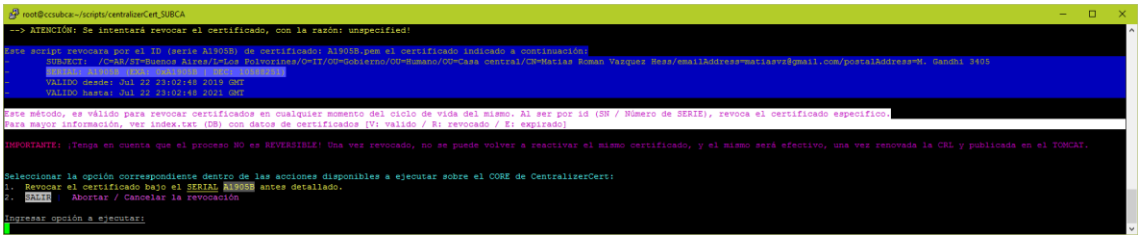

Figura 252. Paso 11 – Revocar certificado cliente humano manual

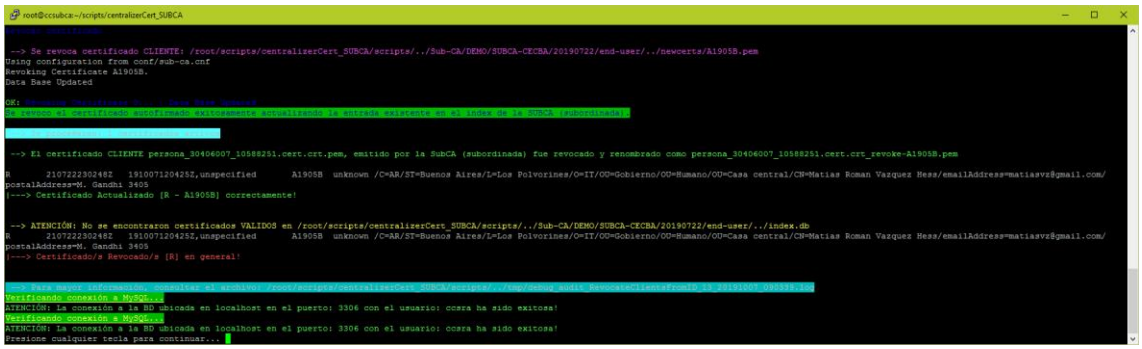

Figura 253. Paso 12 – Revocar certificado cliente humano manual

Figura 254. Paso 13 – Revocar certificado cliente humano manual

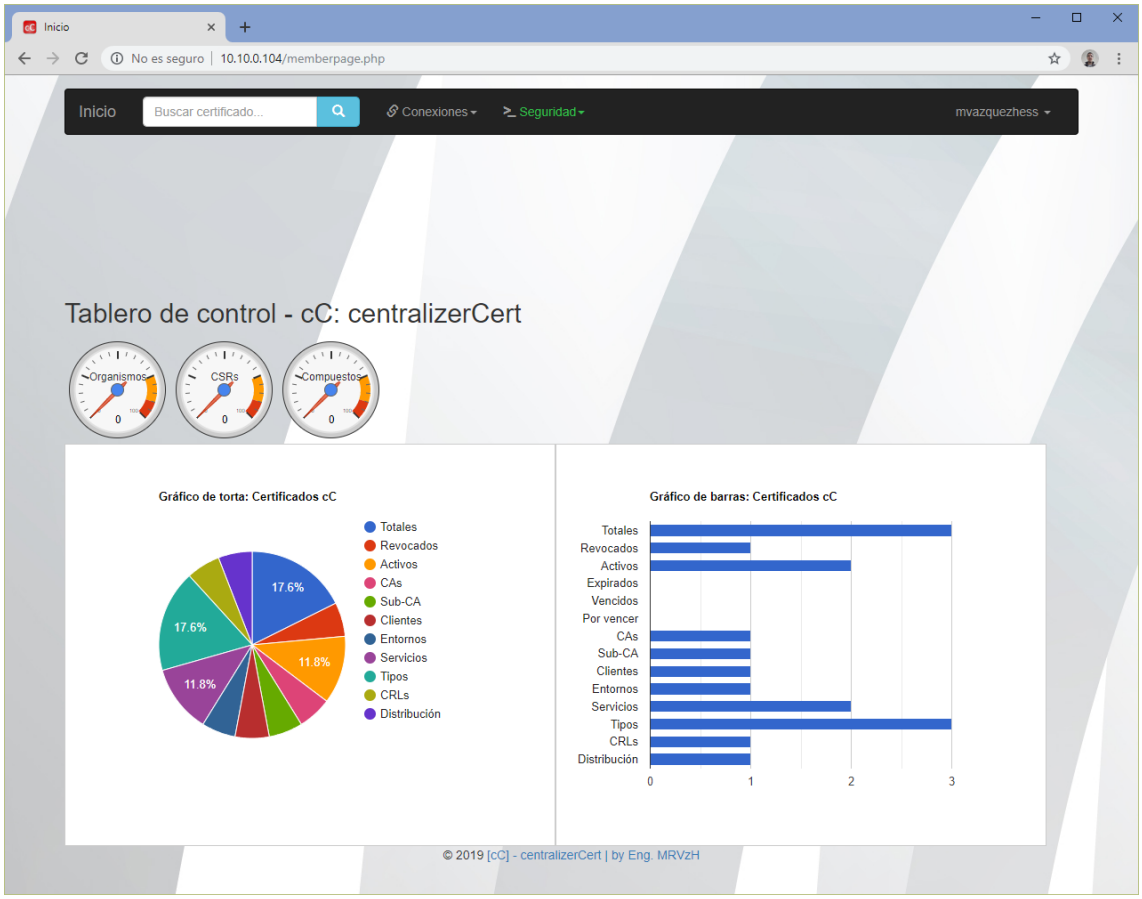

Figura 255. Paso 14 – Revocar certificado cliente humano manual

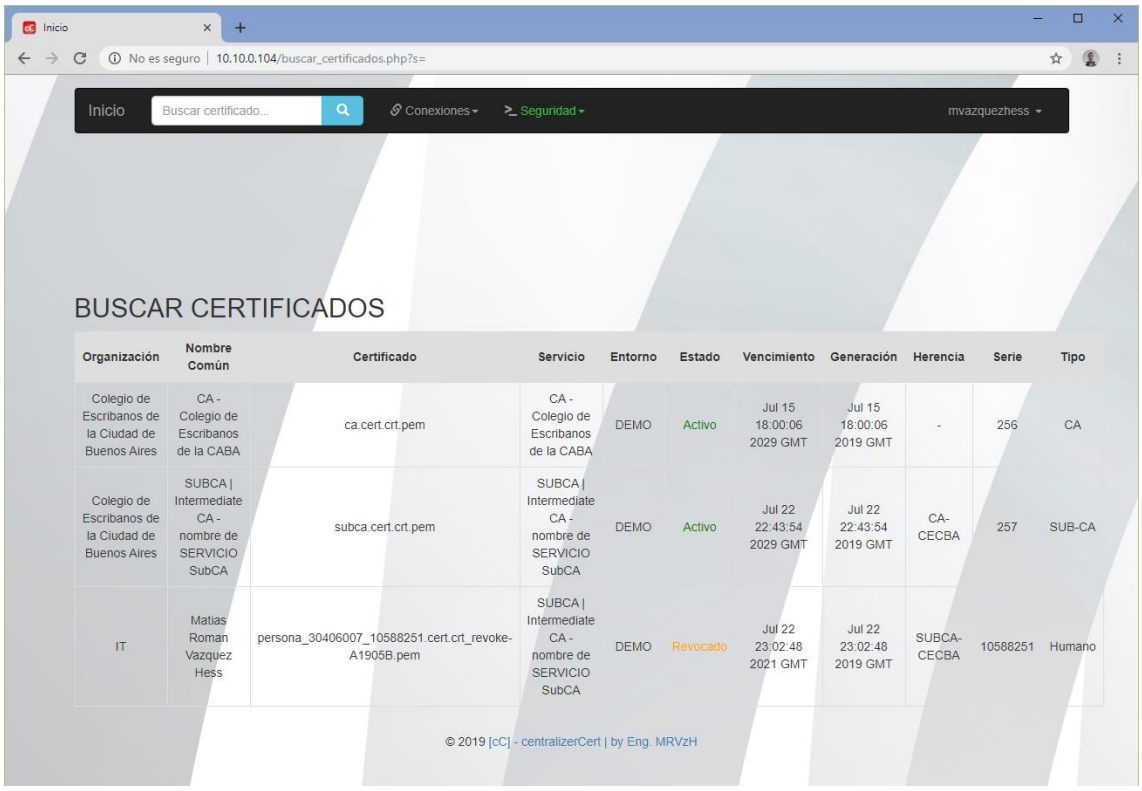

Figura 256. Paso 15 – Revocar certificado cliente humano manual

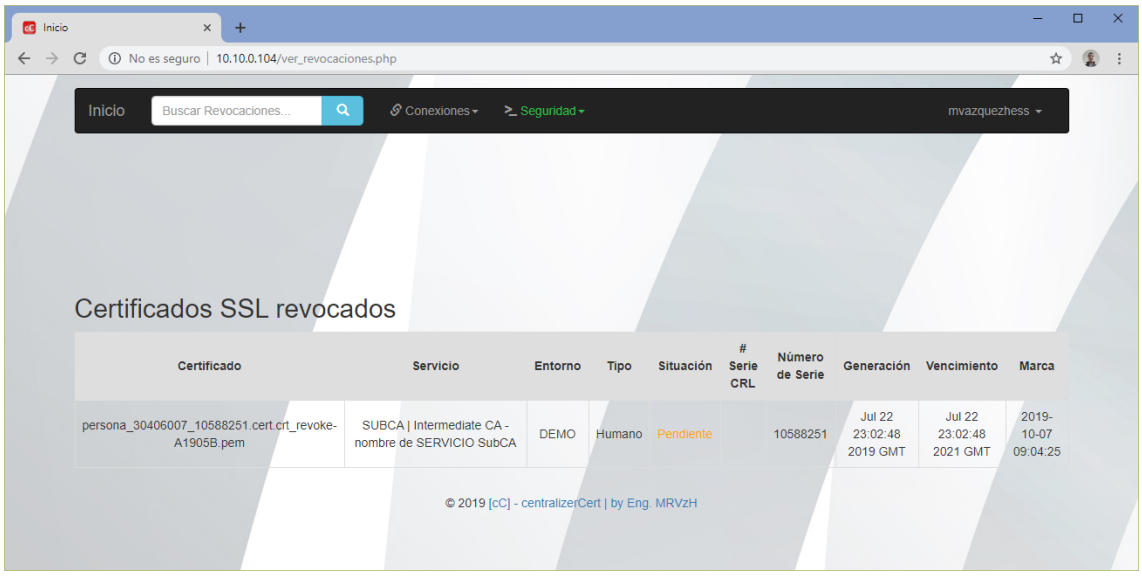

Figura 257. Paso 16 – Revocar certificado cliente humano manual

2.8.2.17.6. Re carga de CRL con revocaciones

Ahora sí, se podrá visualizar el proceso a ejecutar para re generar la Lista de Revocación de Certificados, la cual será la segunda CRL en este caso, para mantener operativo el servicio, donde se incluirá y actualizará la mecánica de uso por incluir el certificado cliente revocado anteriormente. Por

lo cual, se deprecará la CRL previa, se incluirá el certificado revocado, que será obsoleto, dada la nueva CRL disponible, junto al historial correspondiente mediante el panel de control unificado. Para que este sea efectivo, se deberá publicar la CRL y el certificado revocado pasara al estado invalido:

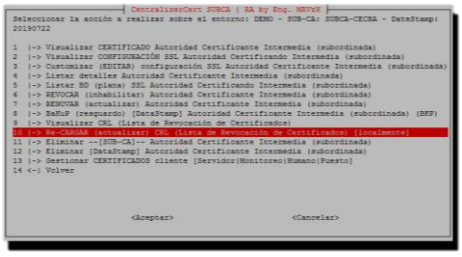

Figura 258. Paso 1 – Re carga de CRL con certificados revocados incluidos

Figura 259. Paso 2 – Re carga de CRL con certificados revocados incluidos

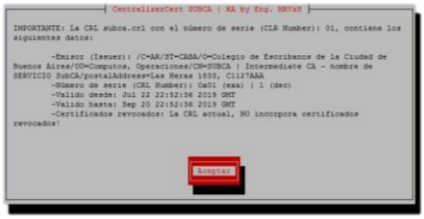

Figura 260. Paso 3 – Re carga de CRL con certificados revocados incluidos

Figura 261. Paso 4 – Re carga de CRL con certificados revocados incluidos

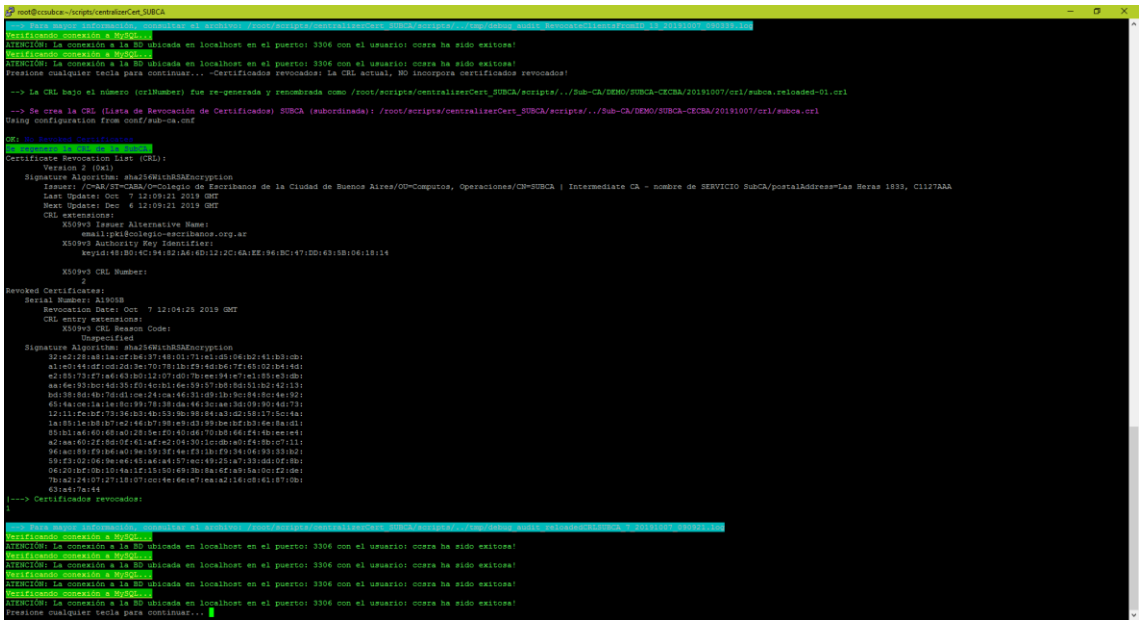

Figura 262. Paso 5 – Re carga de CRL con certificados revocados incluidos

Figura 263. Paso 6 – Re carga de CRL con certificados revocados incluidos

Figura 264. Paso 7 – Re carga de CRL con certificados revocados incluidos

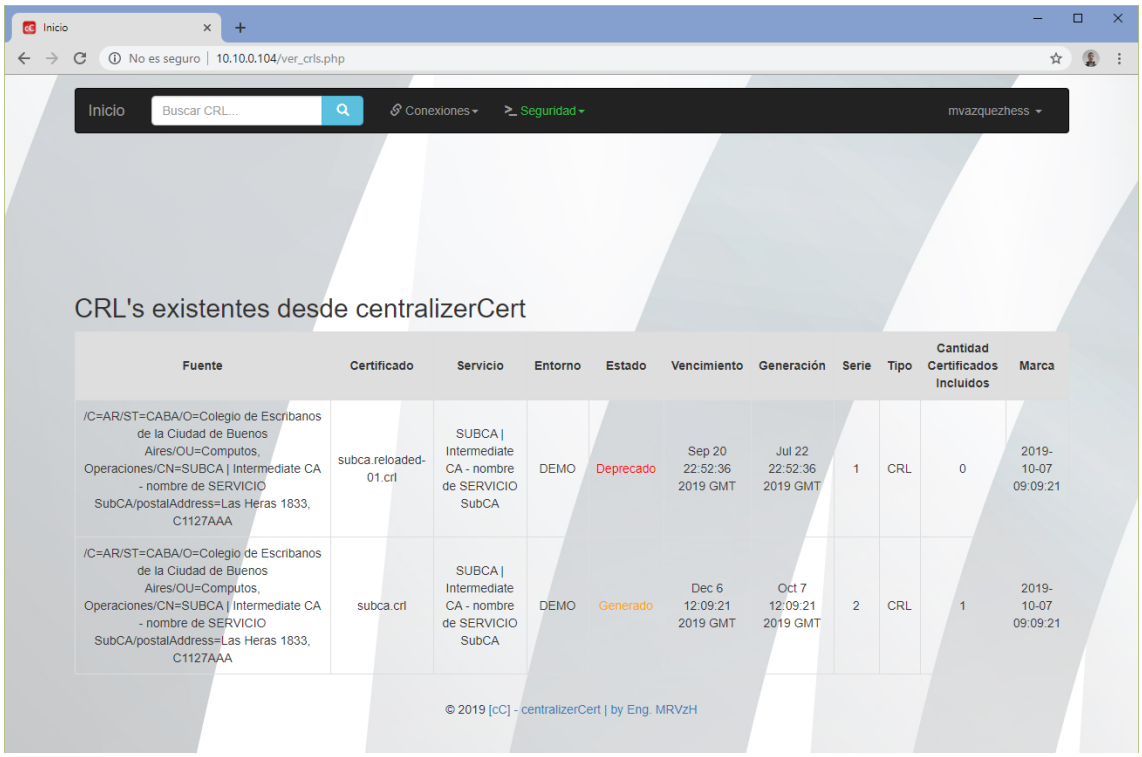

Figura 265. Paso 8 – Re carga de CRL con certificados revocados incluidos

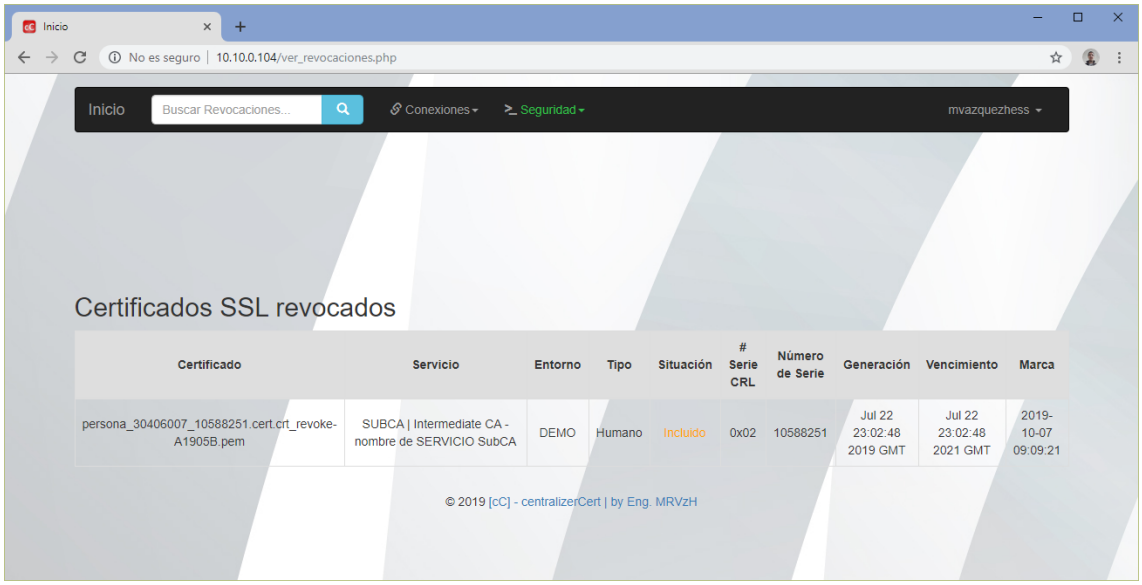

Figura 266. Paso 9 – Re carga de CRL con certificados revocados incluidos

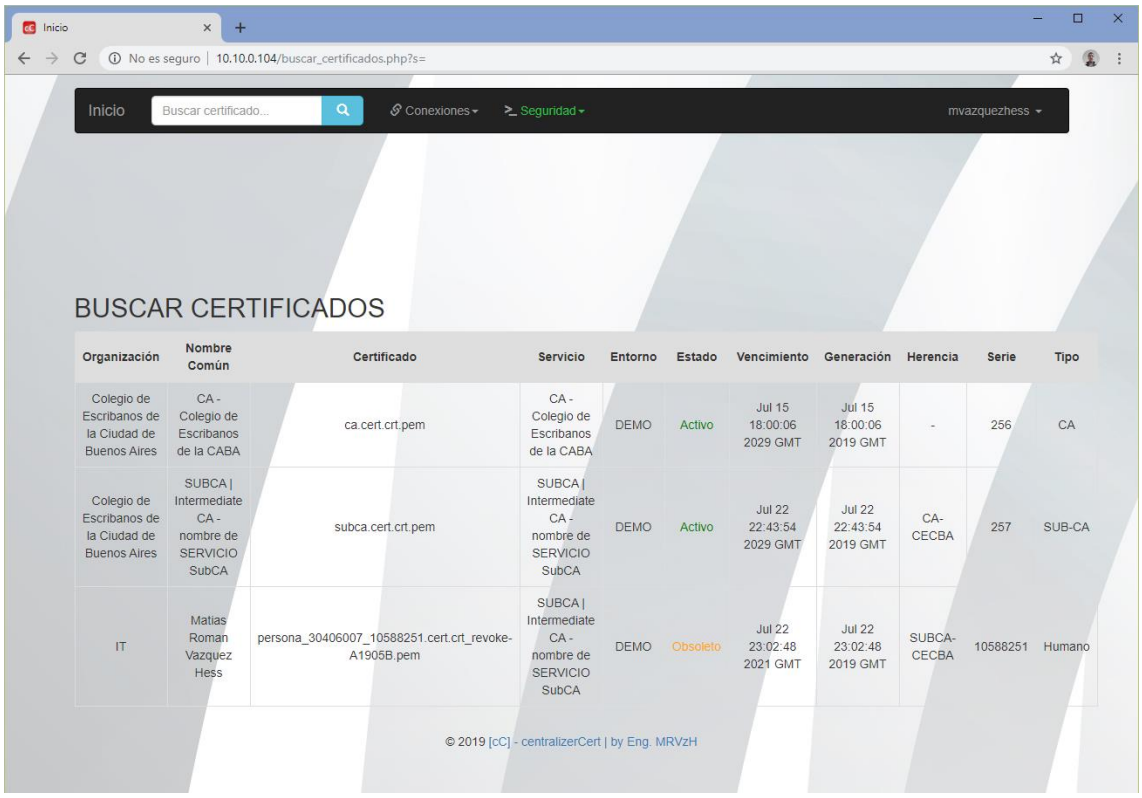

Figura 267. Paso 10 – Re carga de CRL con certificados revocados incluidos

2.8.2.17.7. Distribución de Cliente: Manual – Puesto

Se procede a crear certificado de tipo puesto, en modalidad manual, distribuyendo el mismo en formato pfx [14] [15] por correo a la cuenta denunciada como se visualizará a continuación:

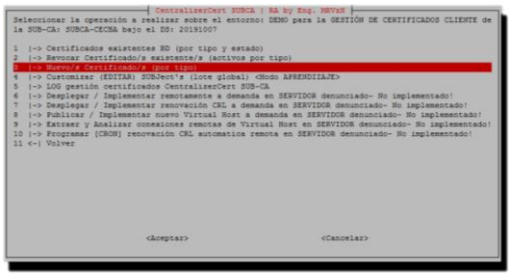

Figura 268. Paso 1 – Distribución de certificado cliente puesto manual

Figura 269. Paso 2 – Distribución de certificado cliente puesto manual

Figura 270. Paso 3 – Distribución de certificado cliente puesto manual

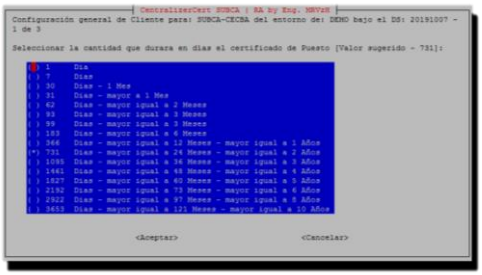

Figura 271. Paso 4 – Distribución de certificado cliente puesto manual

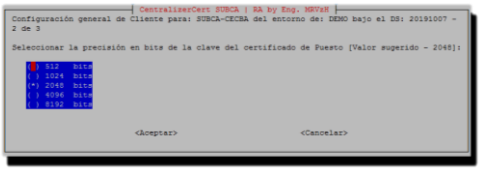

Figura 272. Paso 5 – Distribución de certificado cliente puesto manual

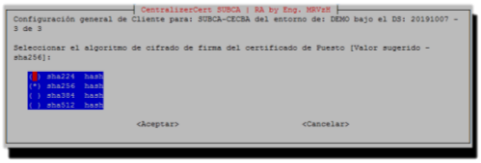

Figura 273. Paso 6 – Distribución de certificado cliente puesto manual

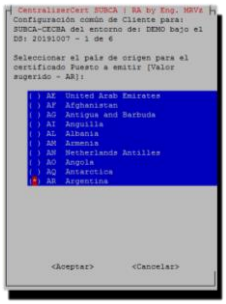

Figura 274. Paso 6 – Distribución de certificado cliente puesto manual

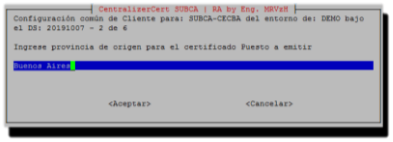

Figura 275. Paso 7 – Distribución de certificado cliente puesto manual

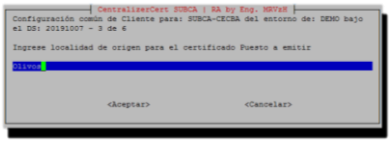

Figura 276. Paso 8 – Distribución de certificado cliente puesto manual

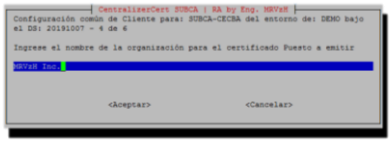

Figura 277. Paso 9 – Distribución de certificado cliente puesto manual

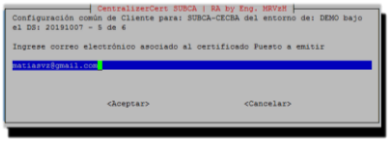

Figura 278. Paso 10 – Distribución de certificado cliente puesto manual

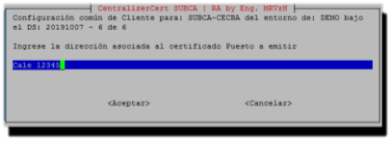

Figura 279. Paso 11 – Distribución de certificado cliente puesto manual

Figura 280. Paso 12 – Distribución de certificado cliente puesto manual

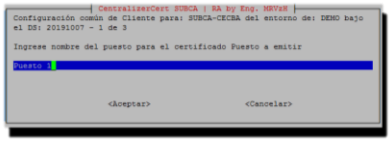

Figura 281. Paso 13 – Distribución de certificado cliente puesto manual

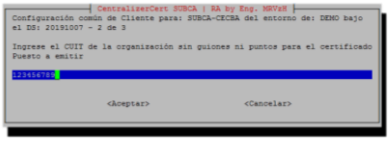

Figura 282. Paso 14 – Distribución de certificado cliente puesto manual

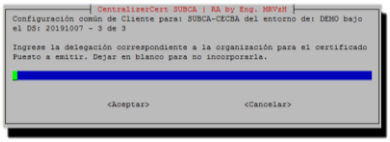

Figura 283. Paso 15 – Distribución de certificado cliente puesto manual

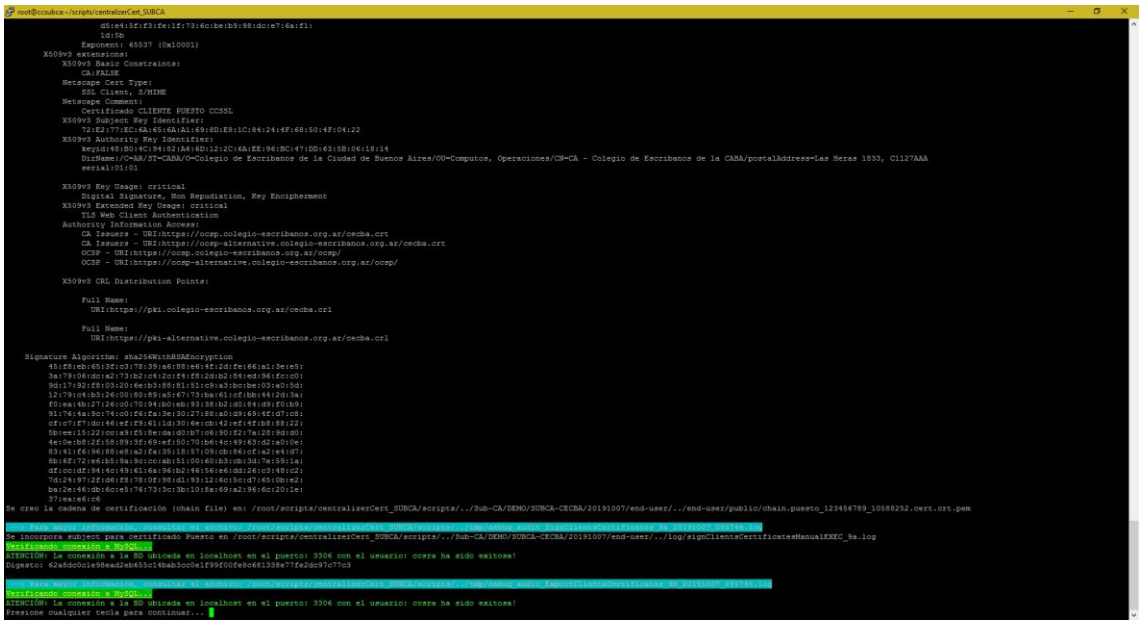

Figura 284. Paso 16 – Distribución de certificado cliente puesto manual

Figura 285. Paso 17 – Distribución de certificado cliente puesto manual

Figura 286. Paso 18 – Distribución de certificado cliente puesto manual

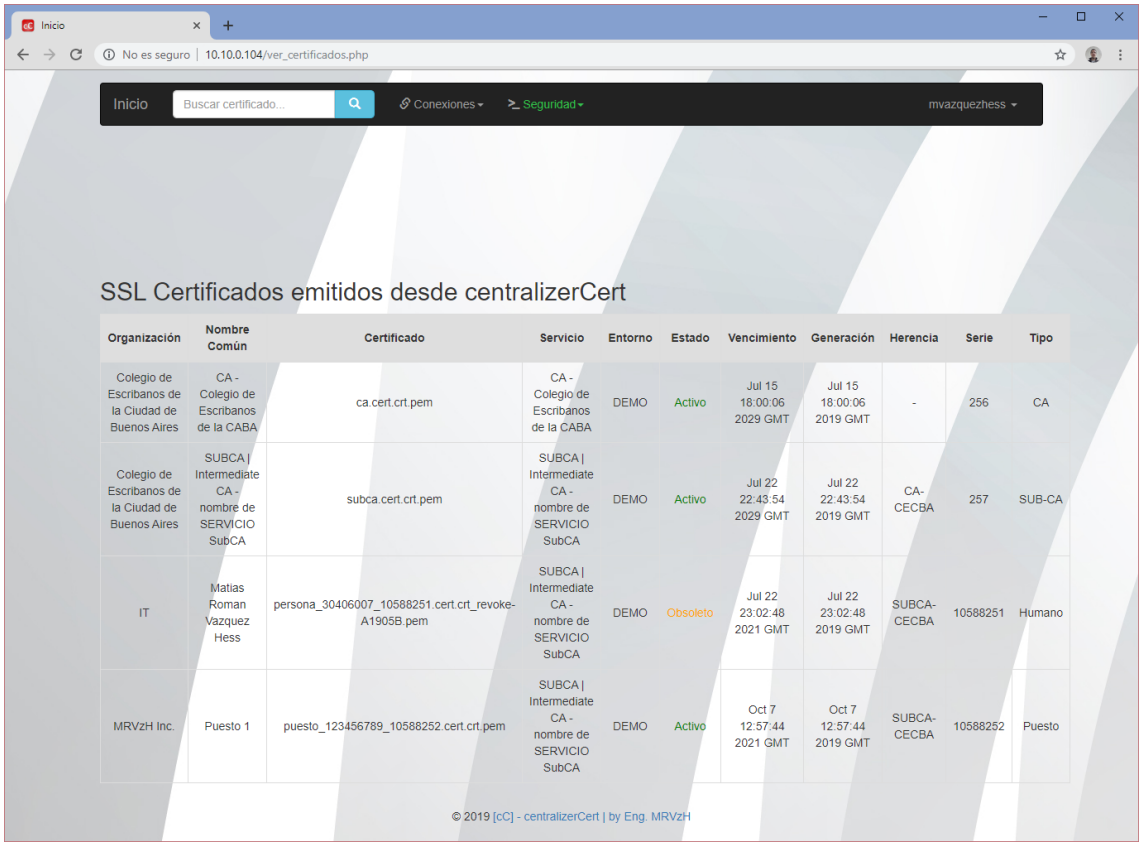

Figura 287. Paso 19 – Distribución de certificado cliente puesto manual

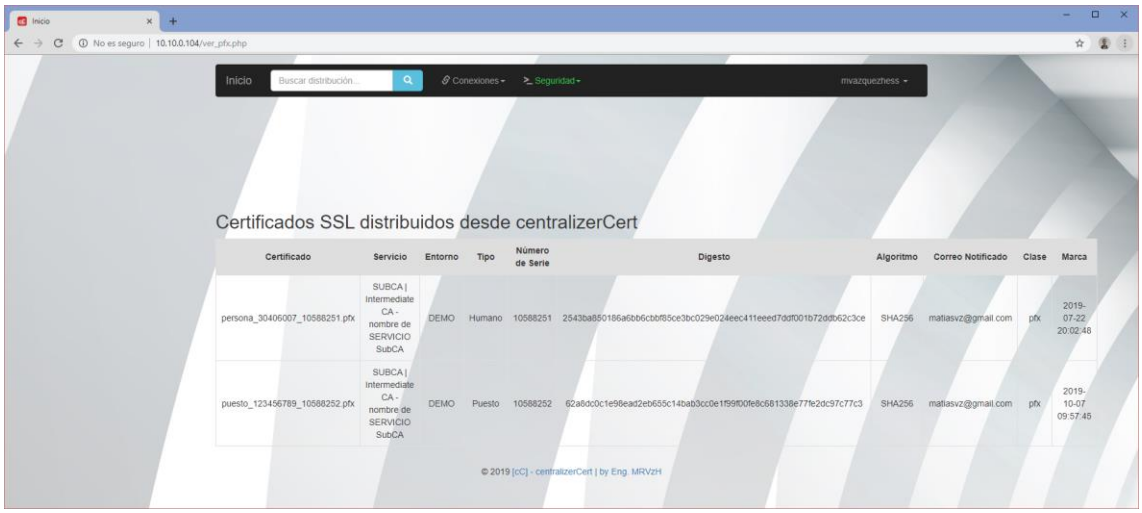

Figura 288. Paso 20 – Distribución de certificado cliente puesto manual

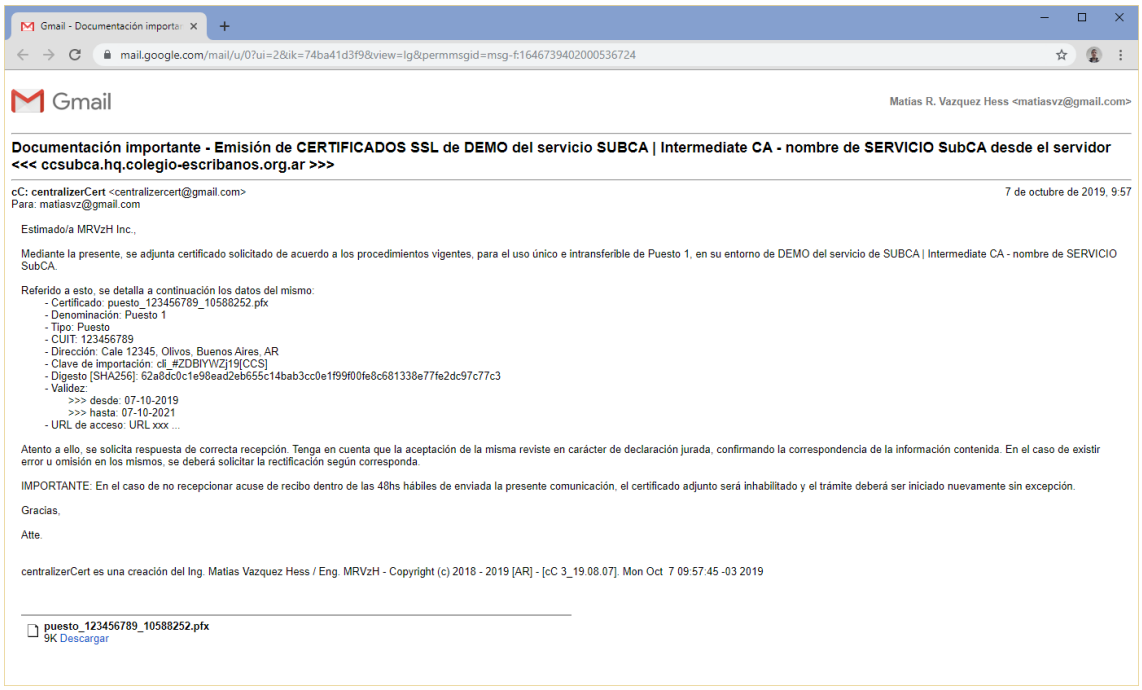

Figura 289. Paso 21 – Distribución de certificado cliente puesto manual

2.8.2.17.8. Distribución de Cliente: CSR – Humano

Se crea certificado de tipo humano, en modalidad CSR, distribuyendo el mismo por correo a la cuenta denunciada como se visualizará a continuación.

Con el fin de cubrir el circuito completo, se simulará mediante el apartado CSR: Pedido de certificado, la creación de un pedido de certificado enviando la clave pública a fin visualizar el mecanismo involucrado aumentado la seguridad del certificado a distribuir.

Una vez recepcionado el CSR, con la especificación indicada en la tabla a continuación, de acuerdo al tipo de certificado y método disponible, el archivo deberá copiarse al repositorio correspondiente a fin de ser absorbido por cC y en caso de ser válido, proceder a su uso como se verá a continuación:

Especificación de Subject	Tipo	Campos Opcionales	Campos Obligatorios
/C=Pais (2)/ST=Provincia/L=Localidad /O=Organización/OU=TIPO/CN=Nombre y Apellido /SN=DNI/emailAddress=correo /postalAddress=Direccion 1234 /dateOfBirth=Fecha de nacimiento /countryOfCitizenship=Nacionlidad /[O=Delegacion - OPCIONAL]	Humano	1	12
/C=Pais(2)/ST=Provincia/L=Localidad/O=Organización /OU=TIPO/CN=Puesto/SN=CUIT /emailAddress=correo /postalAddress=Direccion 1234 /[O=Delegacion - OPCIONAL]	Puesto	1	9

Tabla 2. Especificación de SUBJ's sugeridos por tipo de certificado

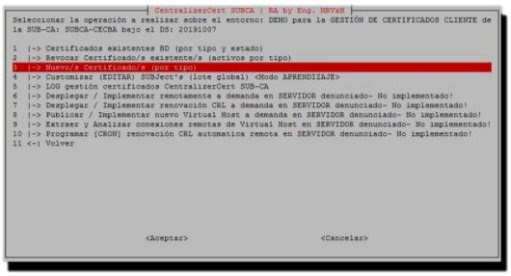

Figura 290. Paso 1 – Distribución de certificado cliente CSR humano

Figura 291. Paso 2 – Distribución de certificado cliente CSR humano

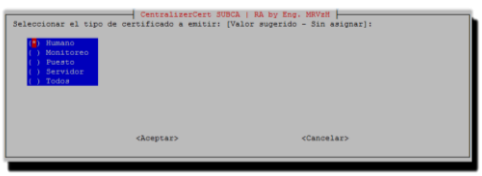

Figura 292. Paso 3 – Distribución de certificado cliente CSR humano

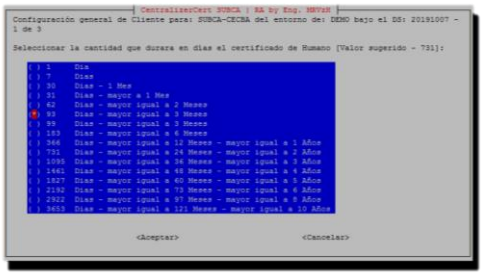

Figura 293. Paso 4 – Distribución de certificado cliente CSR humano

Figura 294. Paso 5 – Distribución de certificado cliente CSR humano

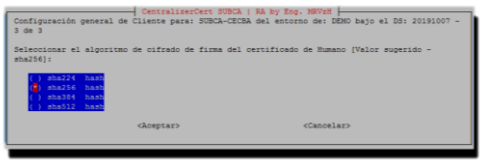

Figura 295. Paso 6 – Distribución de certificado cliente CSR humano

Sin CSR existente dentro del repositorio:

Figura 296. Paso 7 – Distribución de certificado cliente CSR humano

Con CSR existente dentro del repositorio:

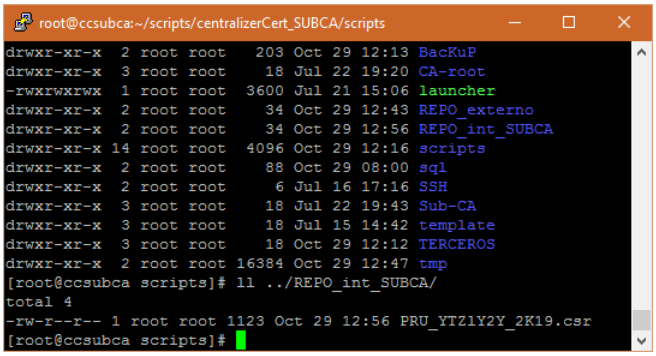

Figura 297. Paso 8 – Distribución de certificado cliente CSR humano

Figura 298. Paso 9 – Distribución de certificado cliente CSR humano

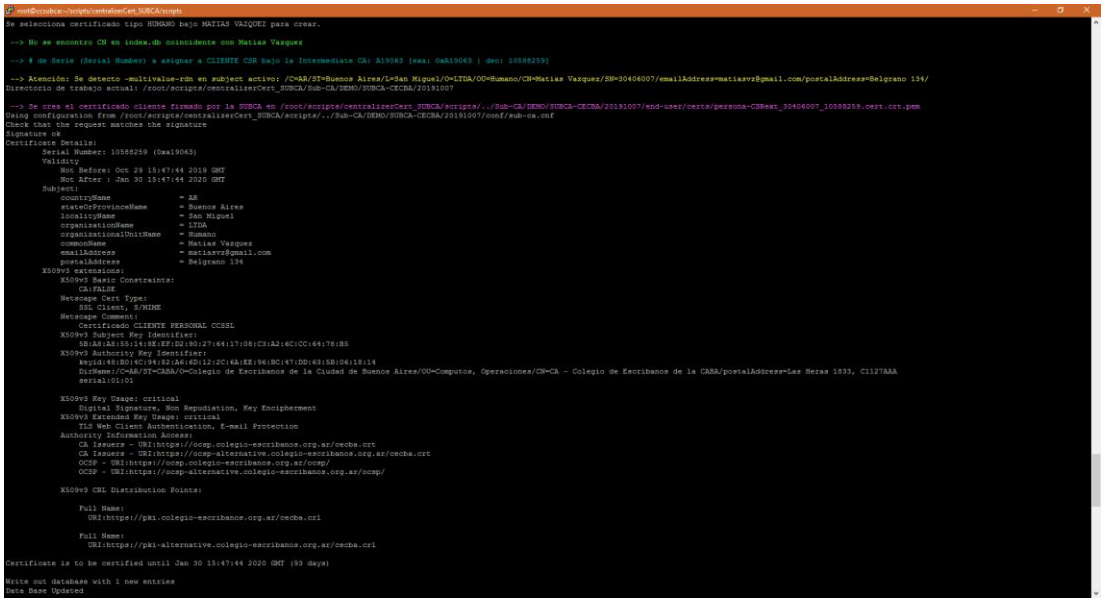

Figura 299. Paso 10 – Distribución de certificado cliente CSR humano

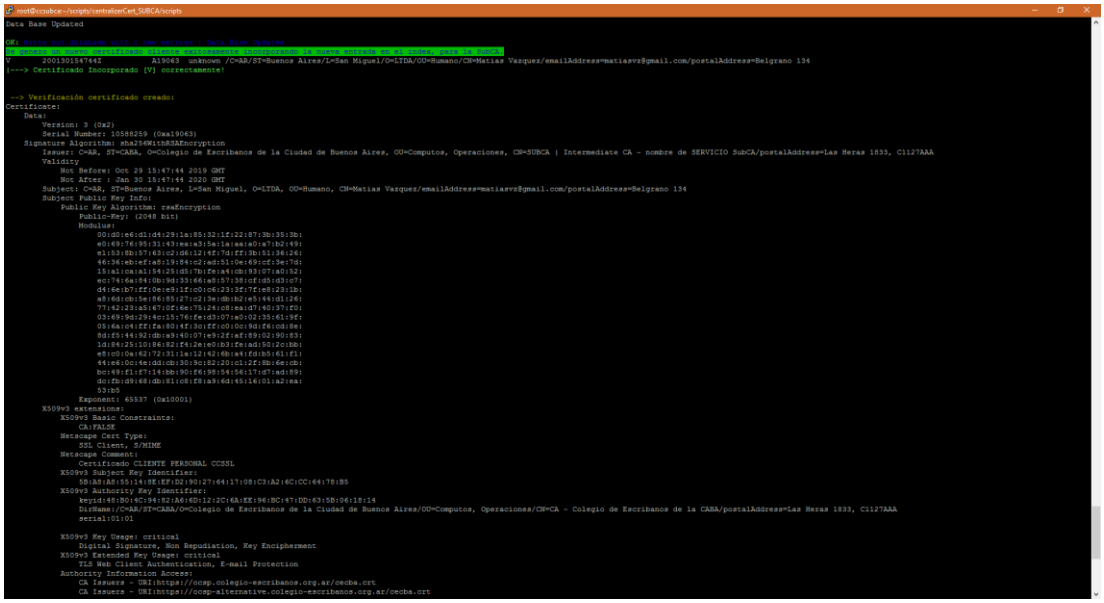

Figura 300. Paso 11 – Distribución de certificado cliente CSR humano

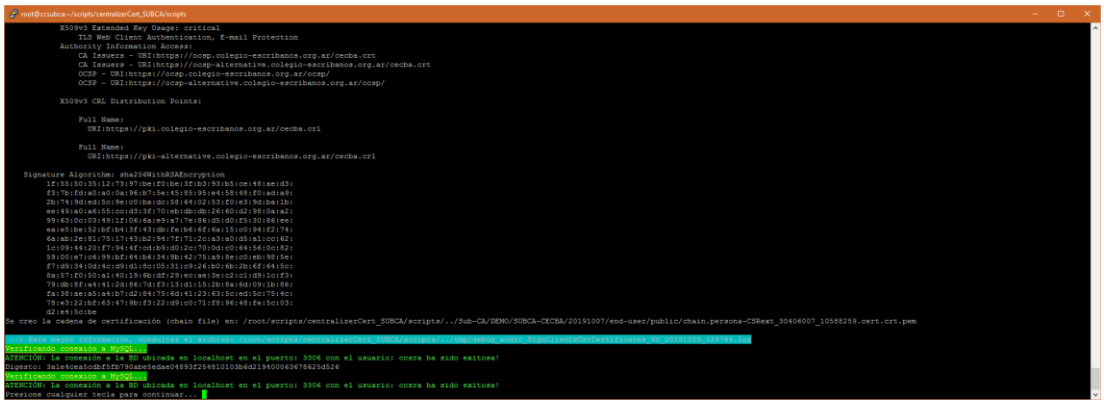

Figura 301. Paso 12 – Distribución de certificado cliente CSR humano

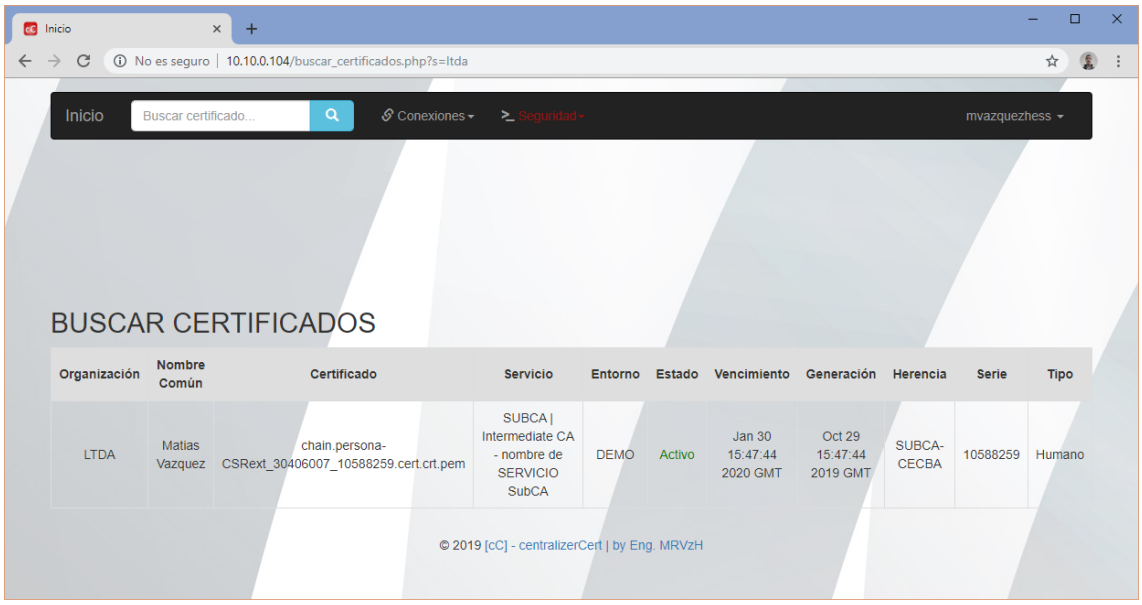

Figura 302. Paso 13 – Distribución de certificado cliente CSR humano

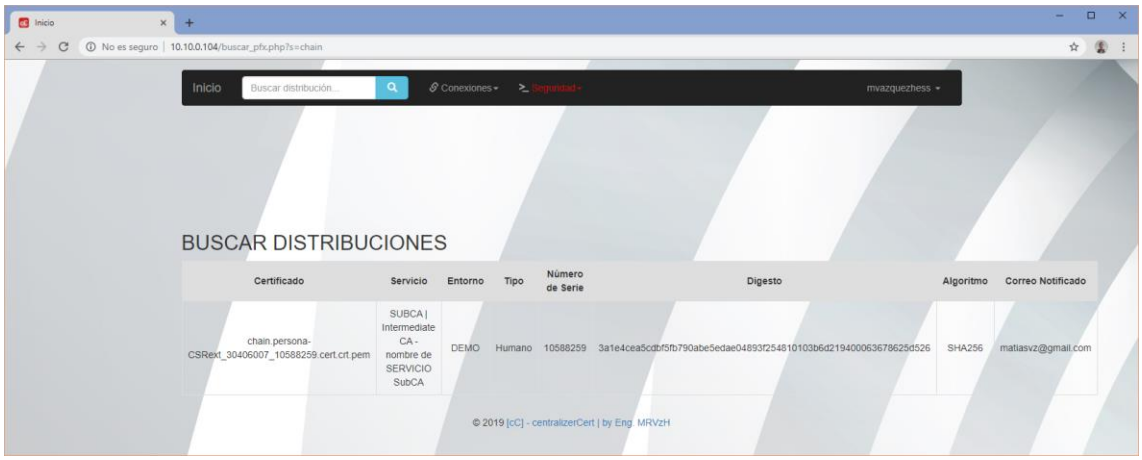

Figura 303. Paso 14 – Distribución de certificado cliente CSR humano

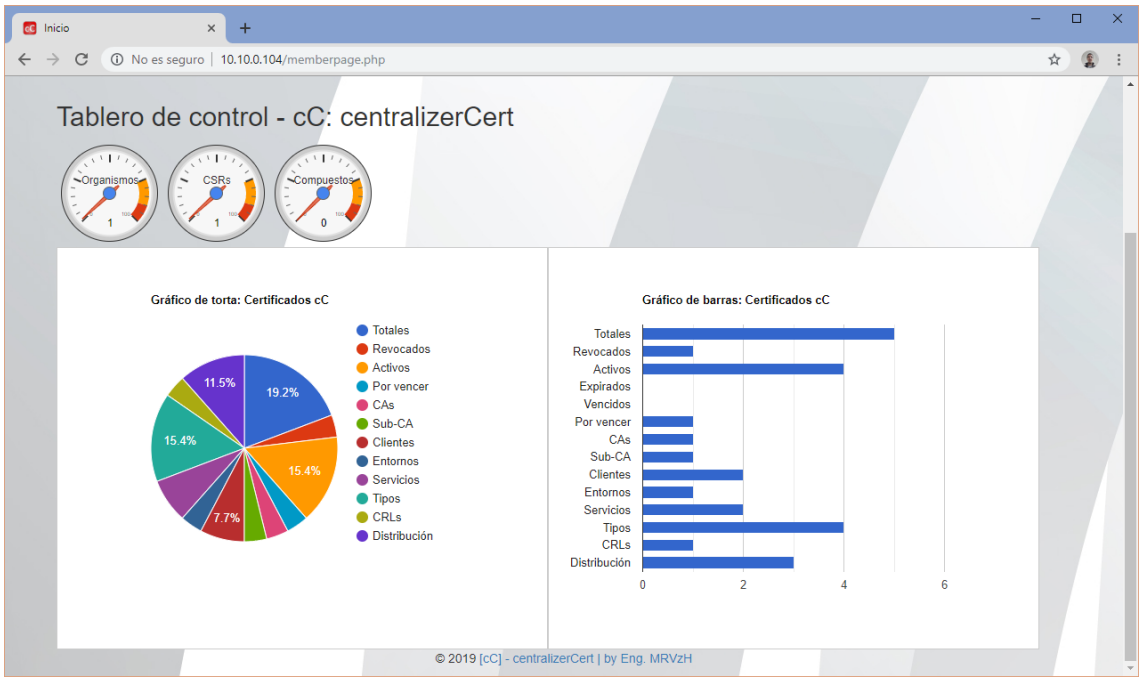

Figura 304. Paso 15 – Distribución de certificado cliente CSR humano

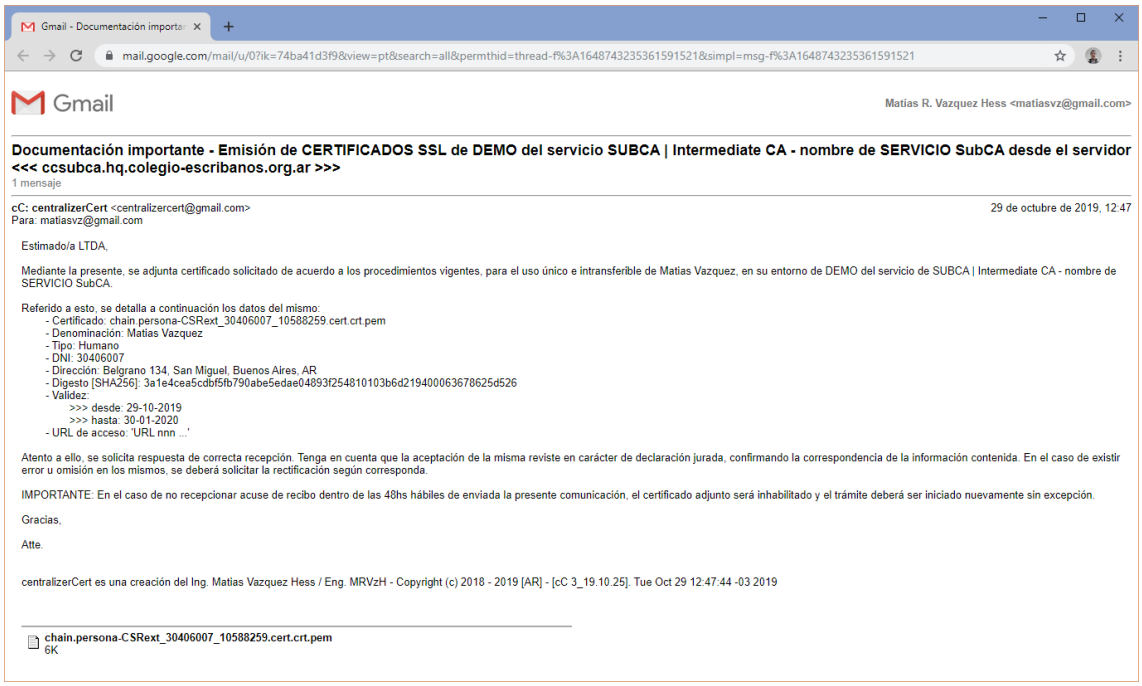

Figura 305. Paso 16 – Distribución de certificado cliente CSR humano

2.8.2.17.9. Creación de certificado Servidor

Se crea el certificado servidor, donde se visualizarán a continuación de forma intuitiva y descriptiva los pasos a realizar:

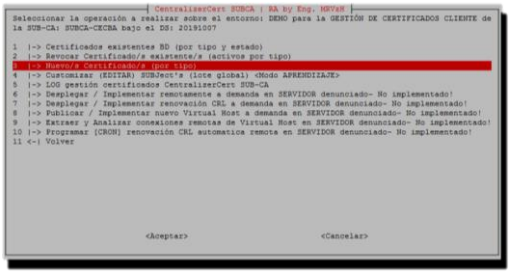

Figura 306. Paso 1 – Creación de certificado Servidor

Figura 307. Paso 2 – Creación de certificado Servidor

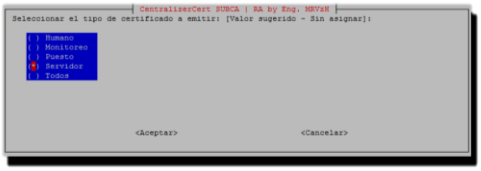

Figura 308. Paso 3 – Creación de certificado Servidor

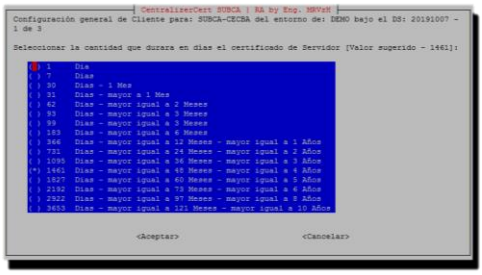

Figura 309. Paso 4 – Creación de certificado Servidor

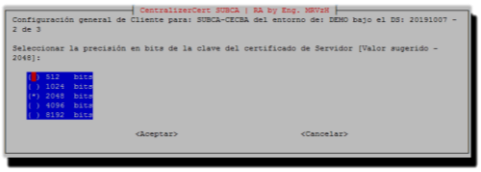

Figura 310. Paso 5 – Creación de certificado Servidor

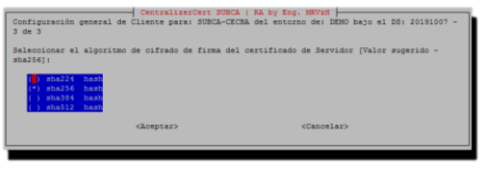

Figura 311. Paso 6 – Creación de certificado Servidor

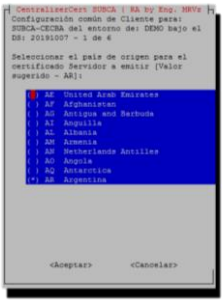

Figura 312. Paso 7 – Creación de certificado Servidor

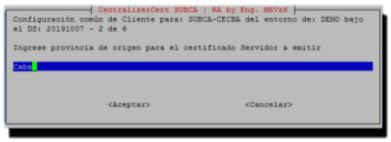

Figura 313. Paso 8 – Creación de certificado Servidor

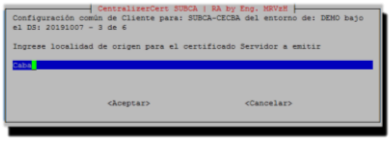

Figura 314. Paso 9 – Creación de certificado Servidor

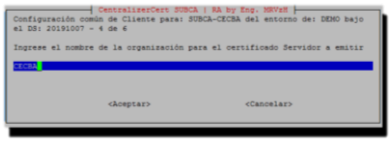

Figura 315. Paso 10 – Creación de certificado Servidor

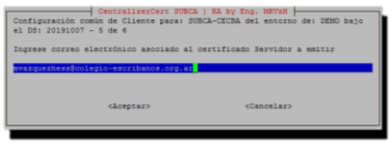

Figura 316. Paso 11 – Creación de certificado Servidor

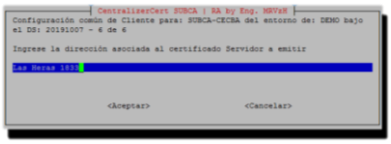

Figura 317. Paso 12 – Creación de certificado Servidor

Figura 318. Paso 13 – Creación de certificado Servidor

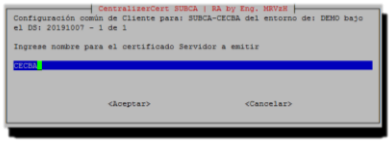

Figura 319. Paso 14 – Creación de certificado Servidor

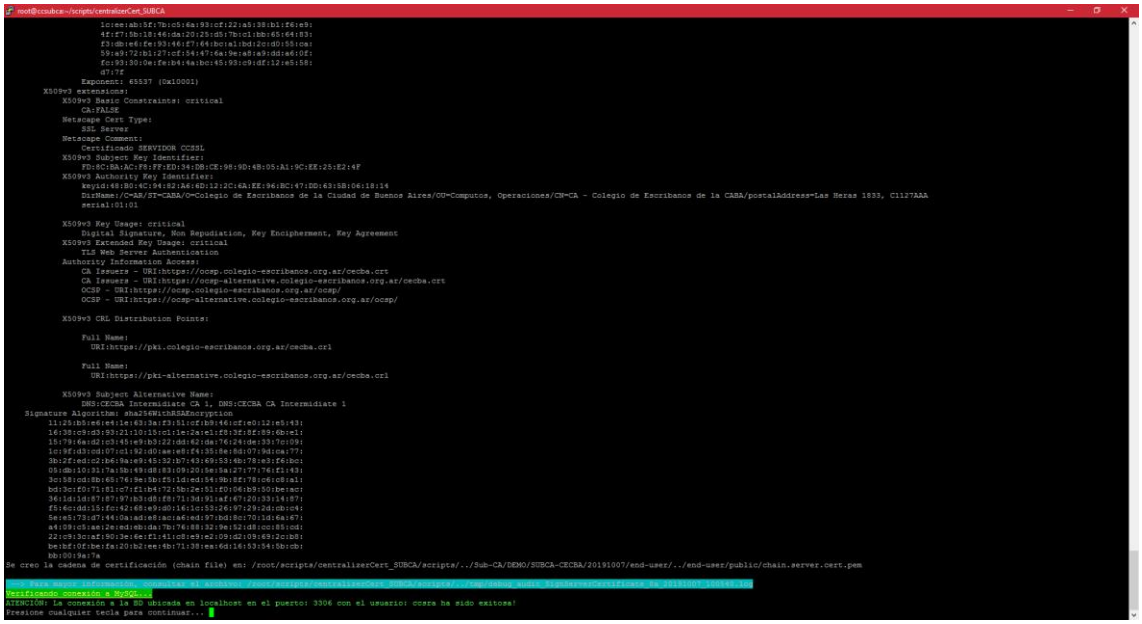

Figura 320. Paso 15 – Creación de certificado Servidor

Figura 321. Paso 16 – Creación de certificado Servidor

Figura 322. Paso 17 – Creación de certificado Servidor

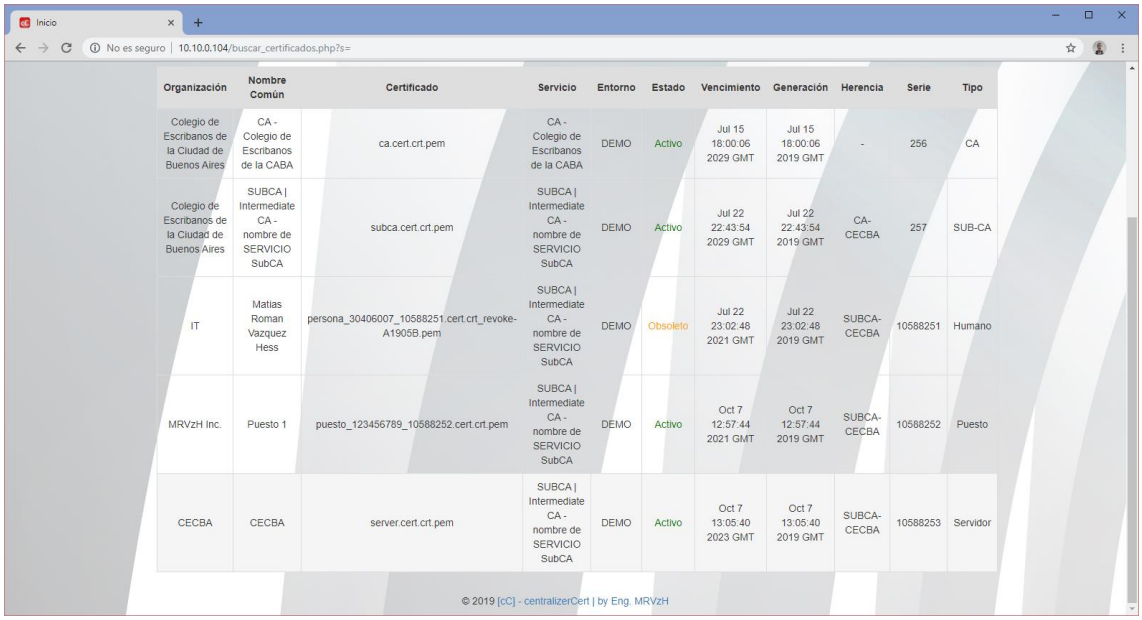

Figura 323. Paso 18 – Creación de certificado Servidor

2.8.2.18. Alertas y notificaciones

Con el objeto de visualizar las alertas graficas visibles correspondientes a vencimientos de certificados propios (PKI), internos (de terceros) o externos agendados, se procede a continuación a detallar los mismos según corresponda para que se pueda comprender y mostrar fehacientemente el

nivel de gestión que permite la consola web, conjuntamente con las notificaciones enviadas por correo electrónico:

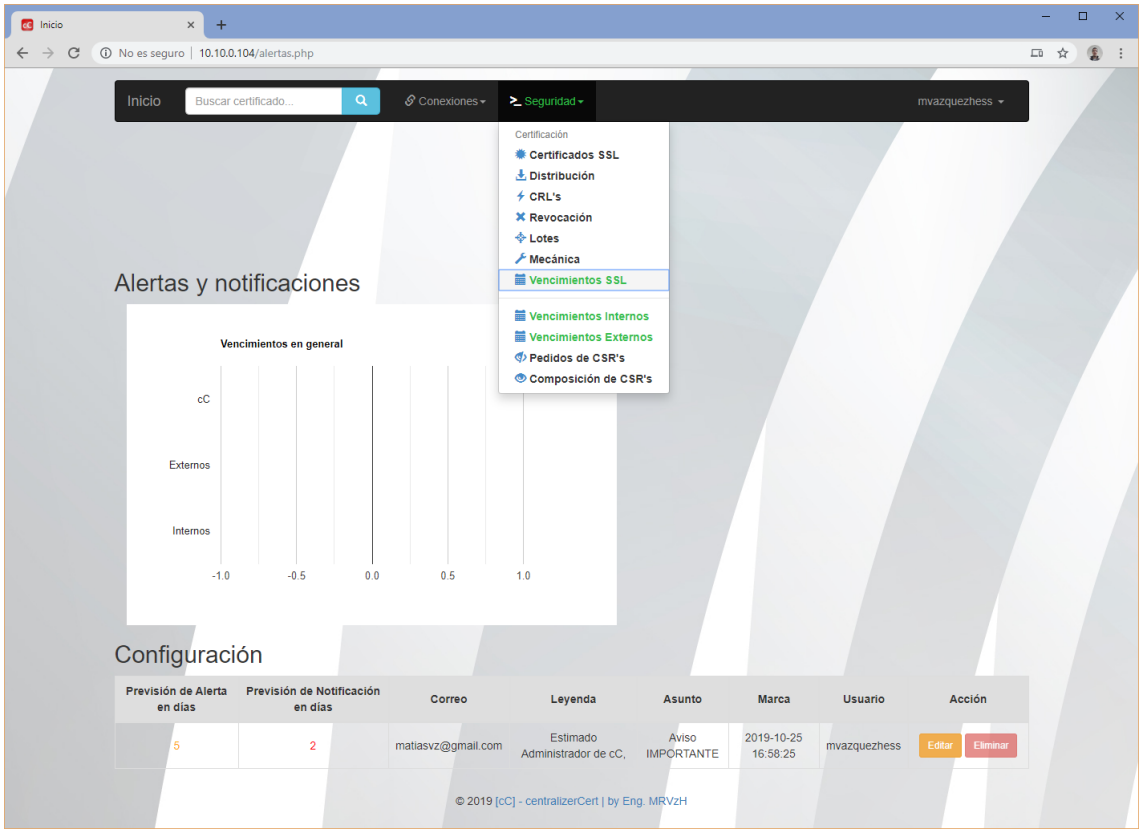

Figura 324. Alertas y Notificaciones - Configuración

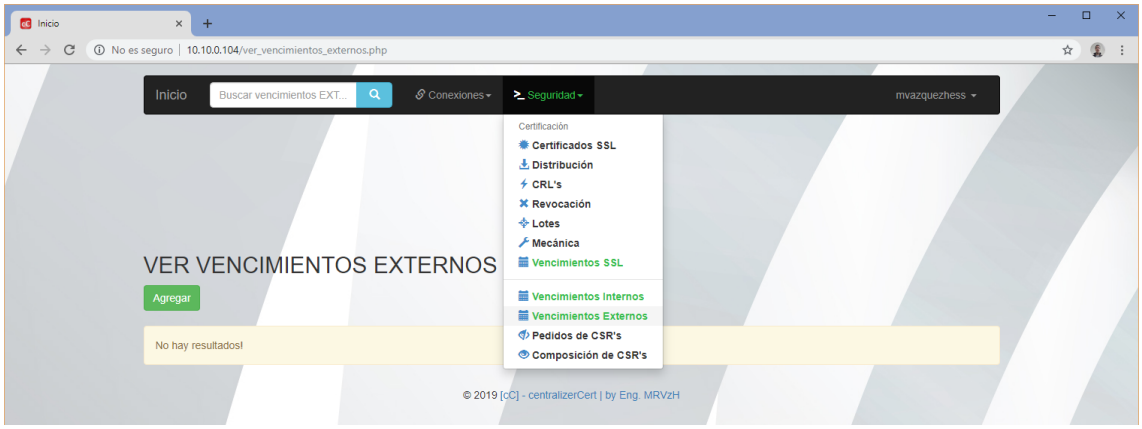

Figura 325. Alertas y Notificaciones - Vencimientos externos

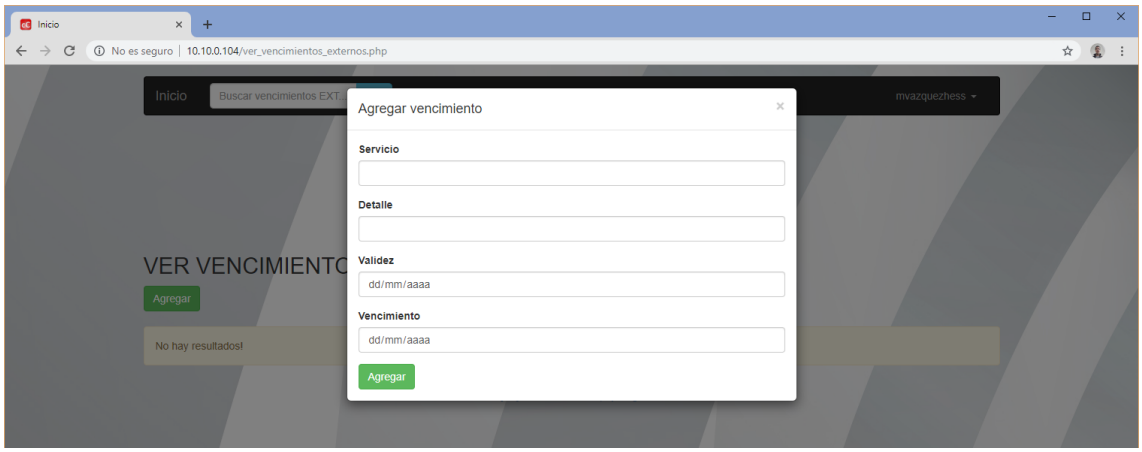

Figura 326. Paso 1 - Agregar Vencimiento externo

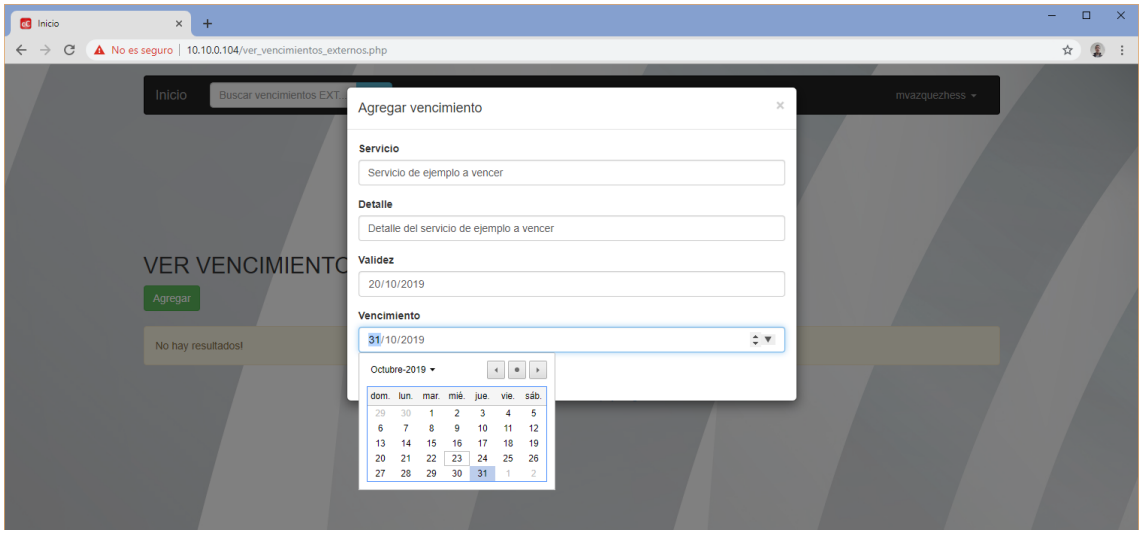

Figura 327. Paso 2 - Agregar Vencimiento externo

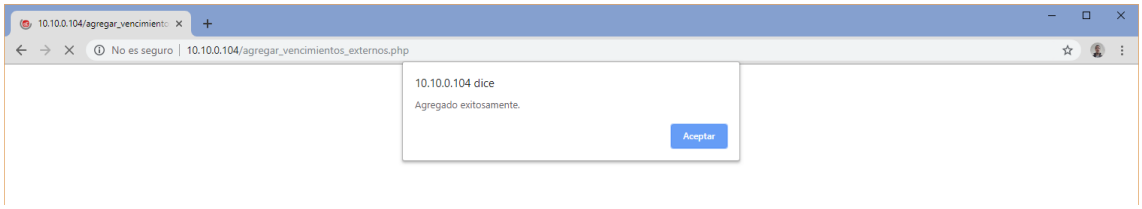

Figura 328. Paso 3 - Agregar Vencimiento externo

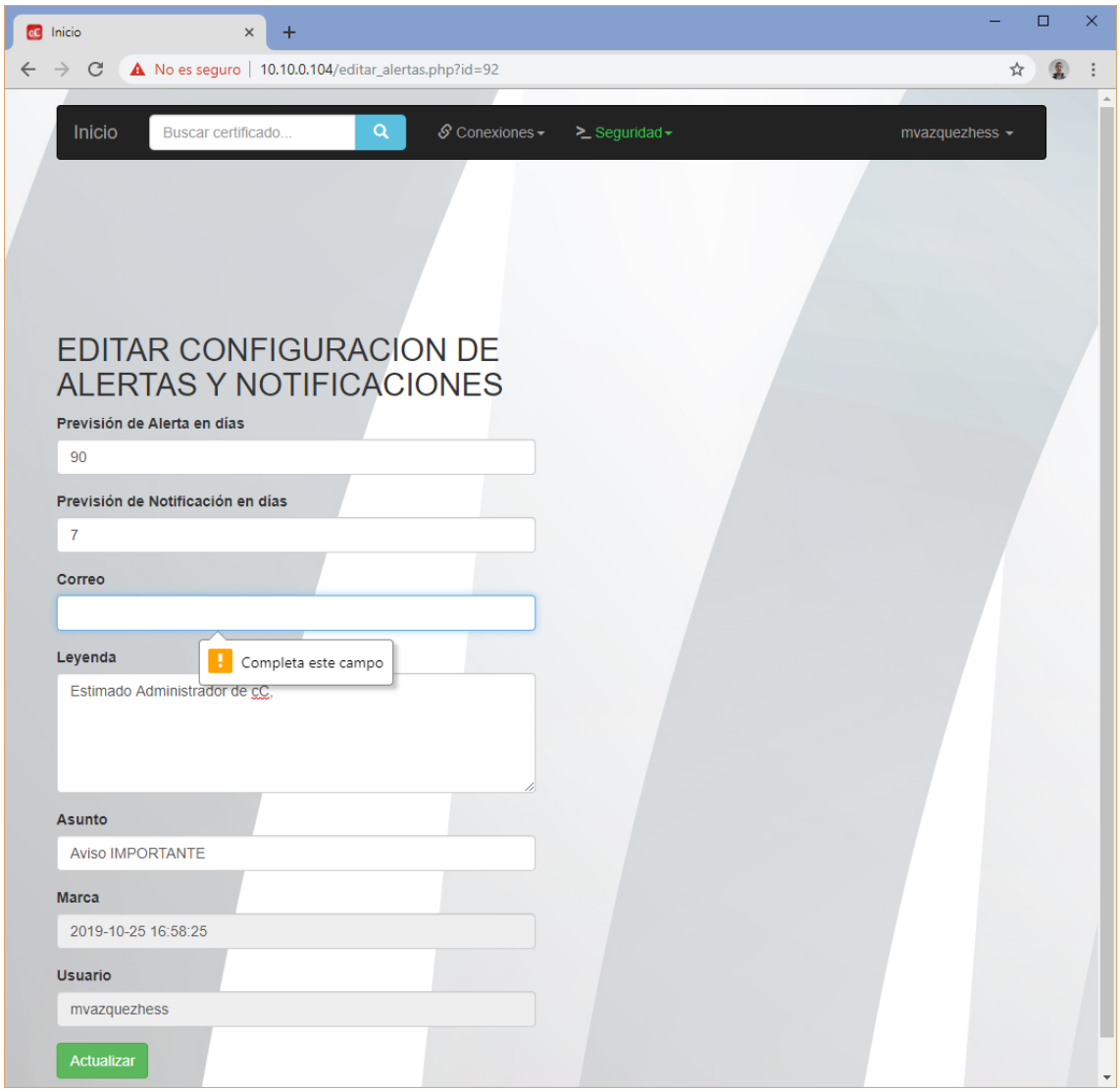

Figura 329. Alertas y Notificaciones – Edición de Configuración

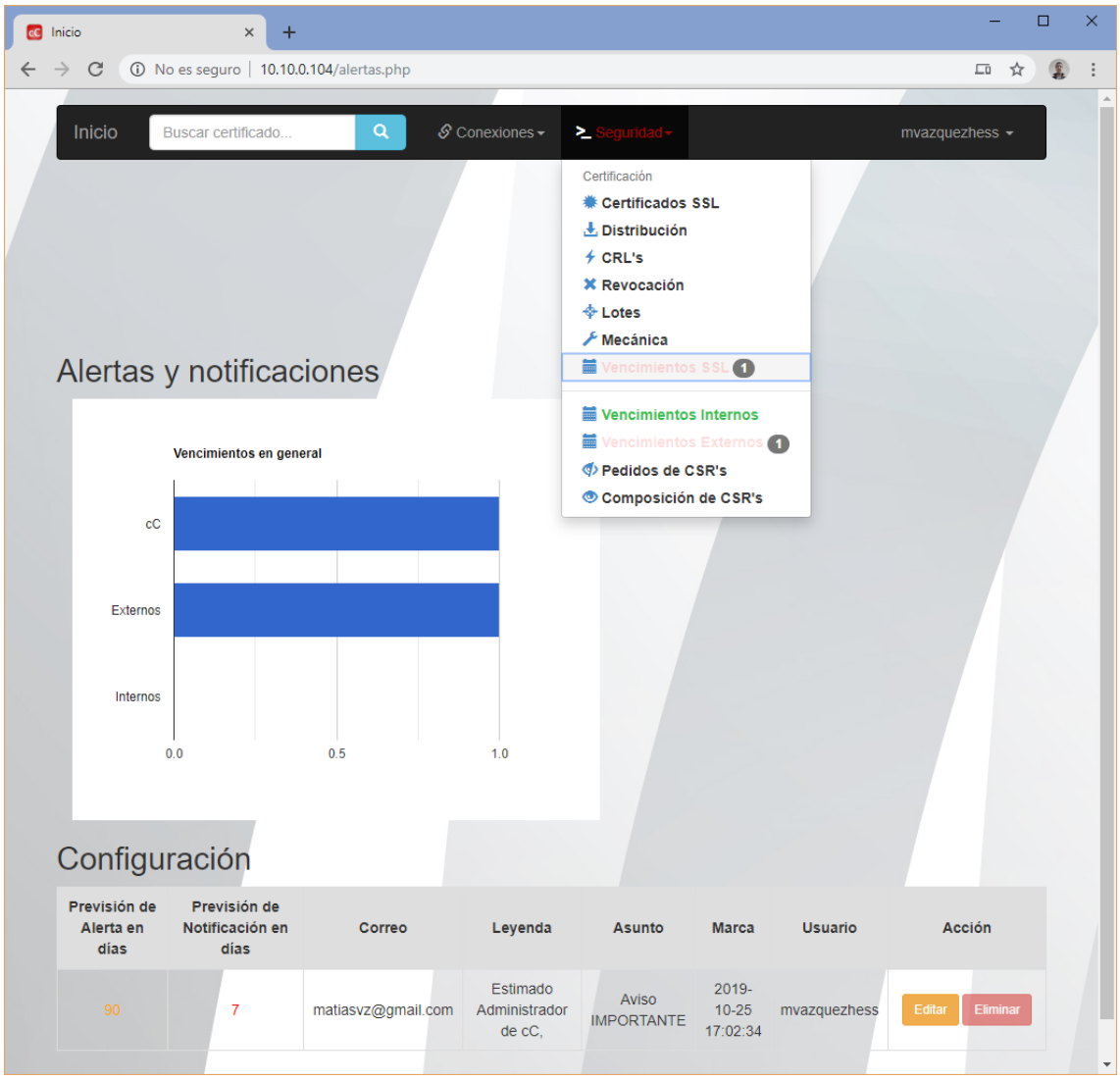

Figura 330. Alertas y Notificaciones – Alerta activa por previsión de alerta en días

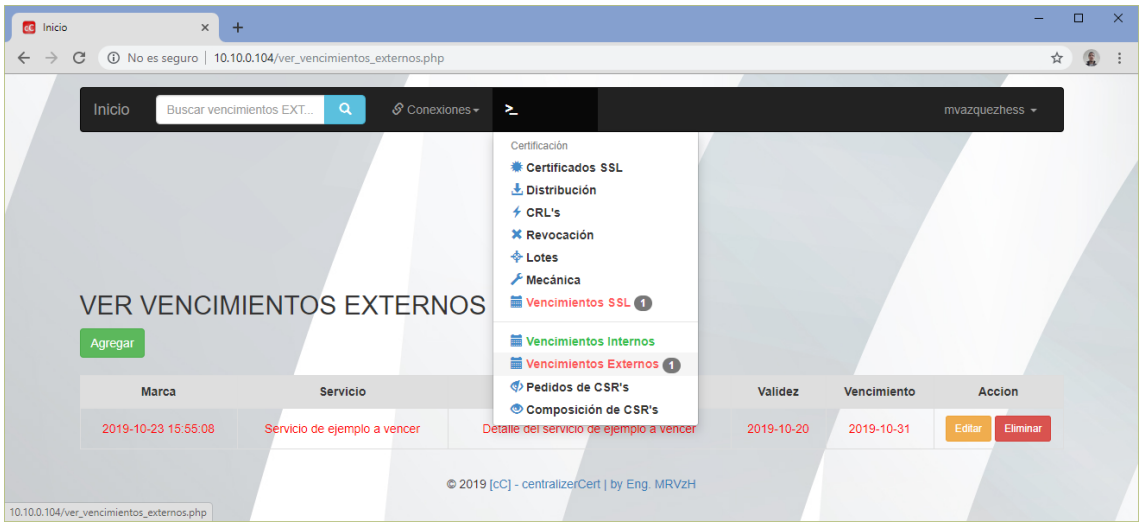

Figura 331. Alertas y Notificaciones – Alerta de Vencimiento externo

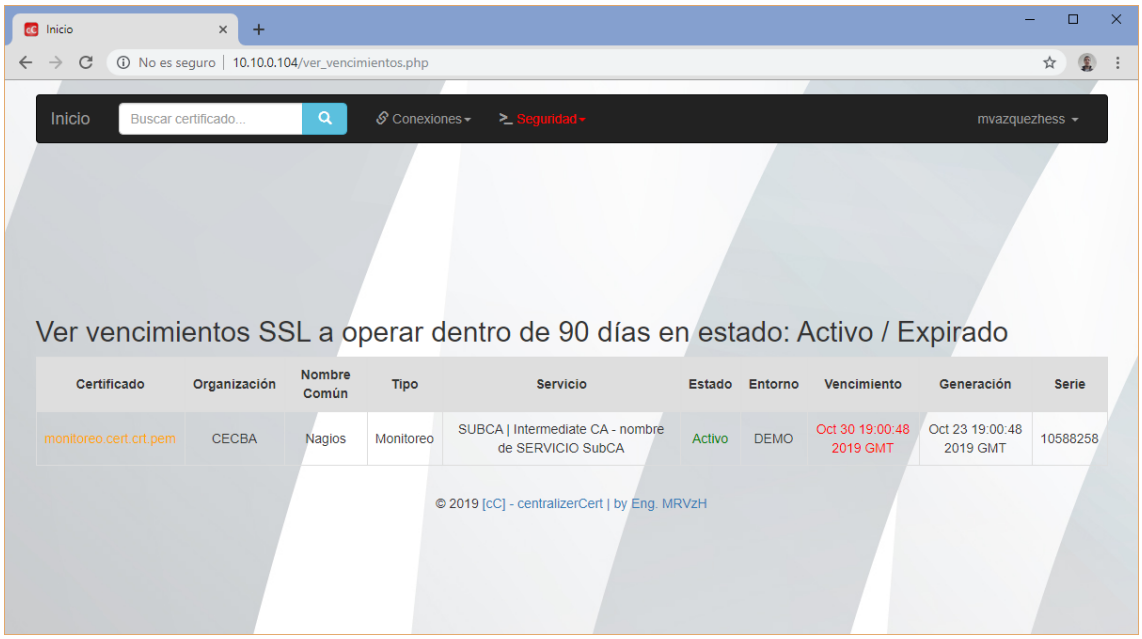

Figura 332. Alertas y Notificaciones – Alerta de Vencimientos SSL

Figura 333. Paso 1 - Alerta por tarea programada

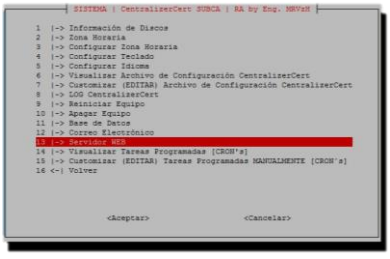

Figura 334. Paso 2 - Alerta por tarea programada

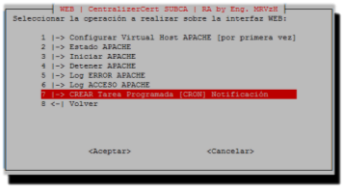

Figura 335. Paso 3 - Alerta por tarea programada

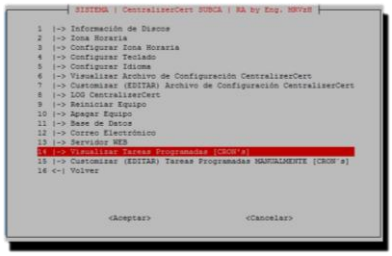

Figura 336. Paso 4 - Alerta por tarea programada

Figura 337. Paso 5 - Alerta por tarea programada

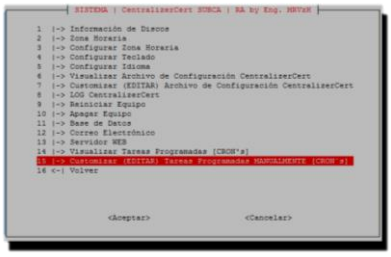

Figura 338. Paso 6 - Alerta por tarea programada

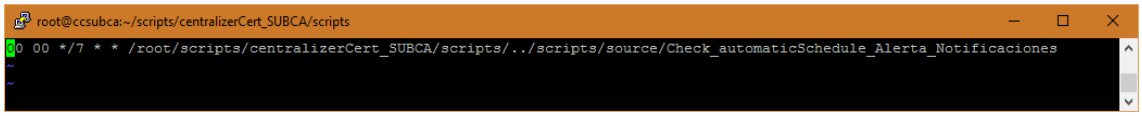

Figura 339. Paso 7 - Alerta por tarea programada

Mensaje enviado con vencimientos próximos a operar con configuración de 90 días:

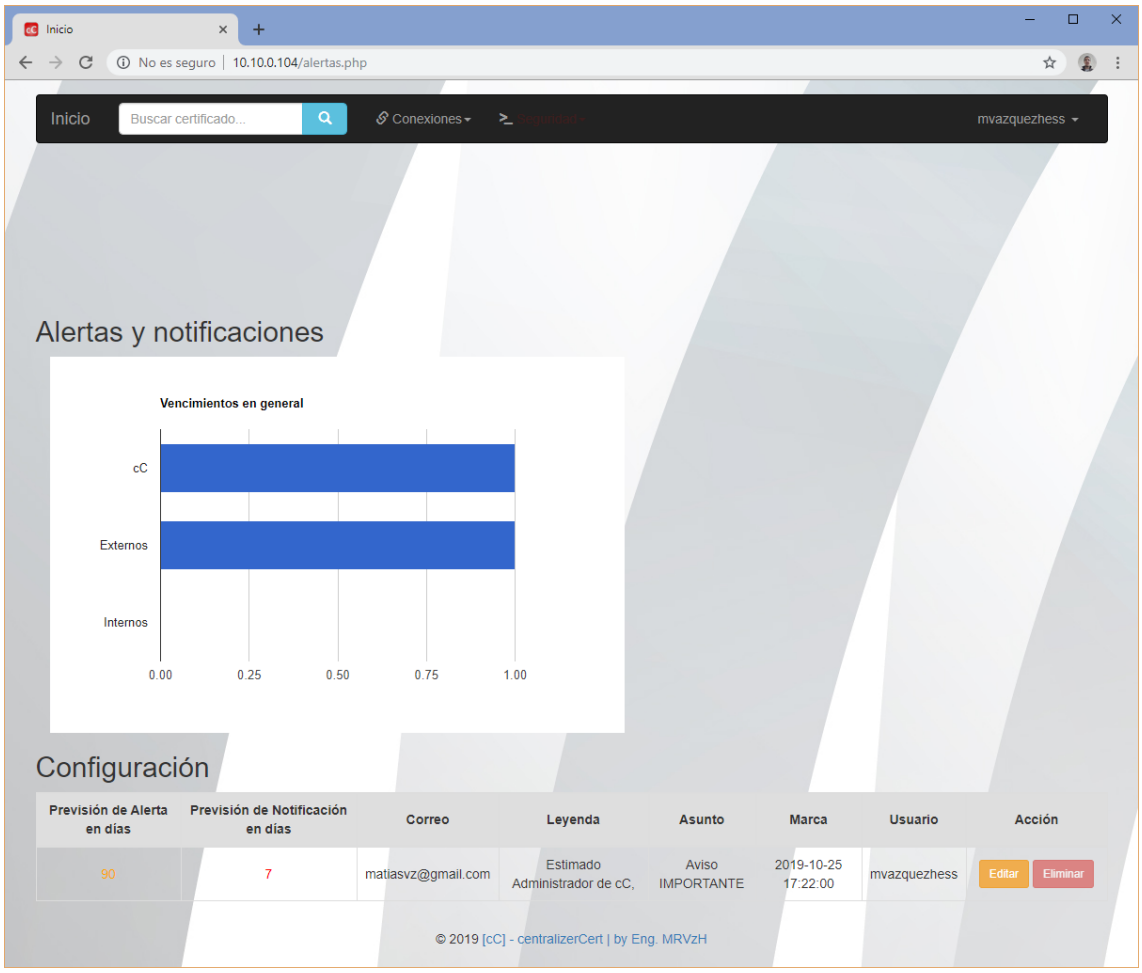

Figura 340. Paso 8A - Alerta por tarea programada

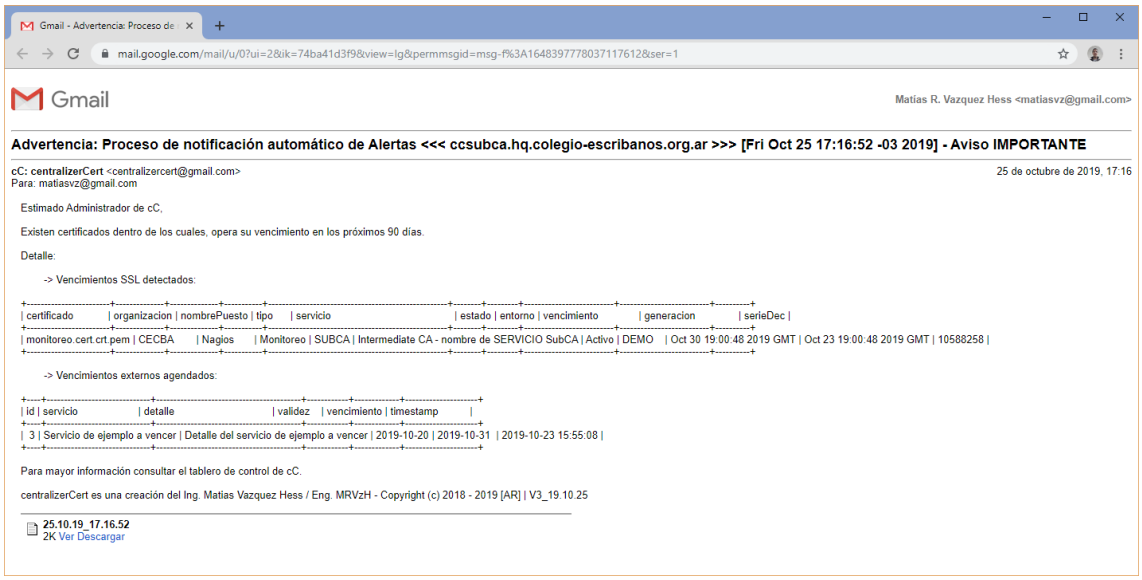

Figura 341. Paso 9A - Alerta por tarea programada

Mensaje enviado sin vencimientos próximos a operar con configuración de 1 día:

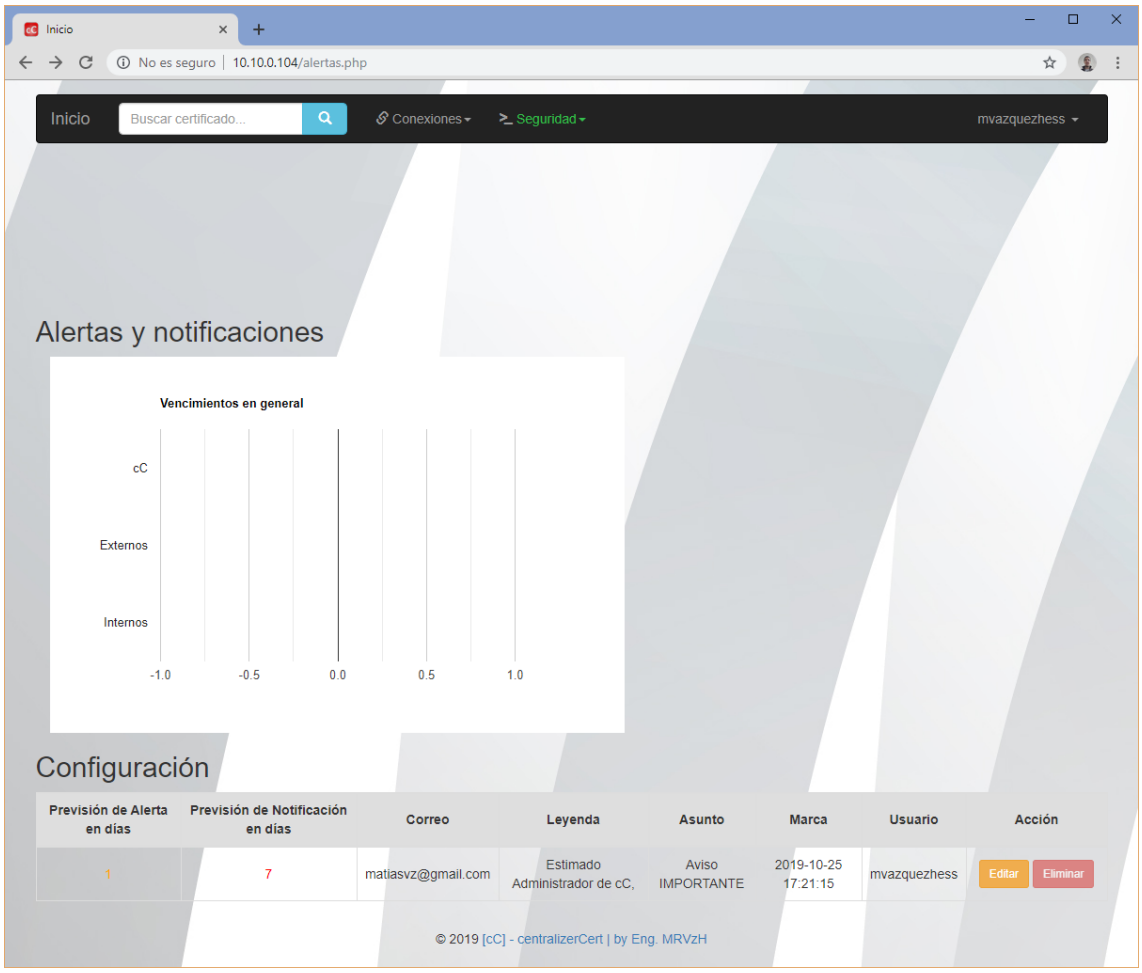

Figura 342. Paso 8B - Alerta por tarea programada

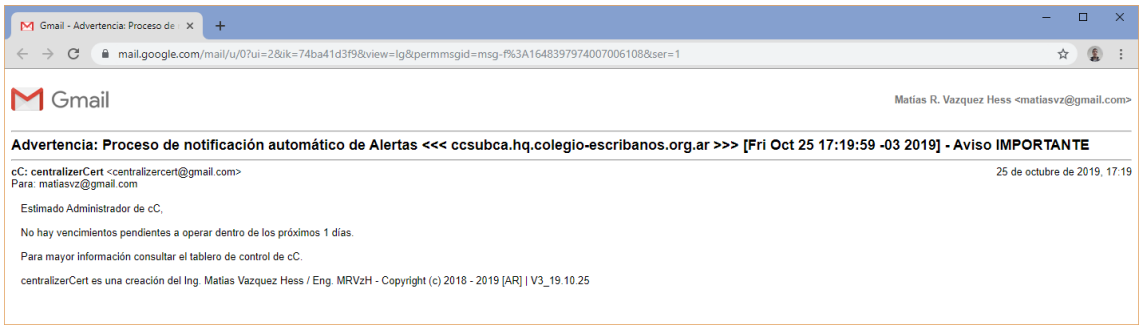

Figura 343. Paso 9B - Alerta por tarea programada

2.8.2.19. Certificados de terceros

Para la gestión de certificados externos, existe un set de herramientas básicas diseñadas para permitir realizar una serie de operaciones que se visualizaran a continuación de forma intuitiva y descriptiva paso a paso:

Figura 344. Paso 1 - Certificados de terceros

Figura 345. Paso 2 - Certificados de terceros

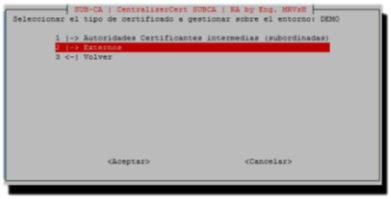

Figura 346. Paso 3 - Certificados de terceros

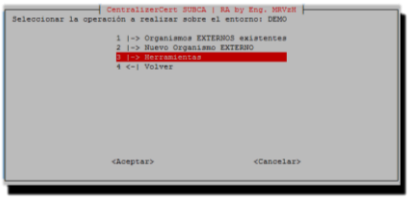

Figura 347. Paso 4 - Herramientas

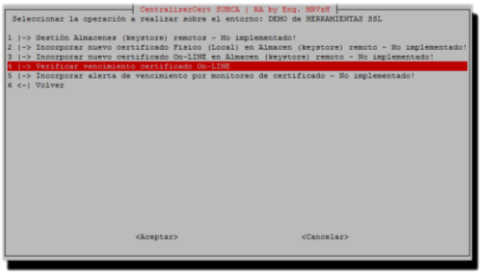

Figura 348. Paso 5 – Verificar vencimiento On-Line

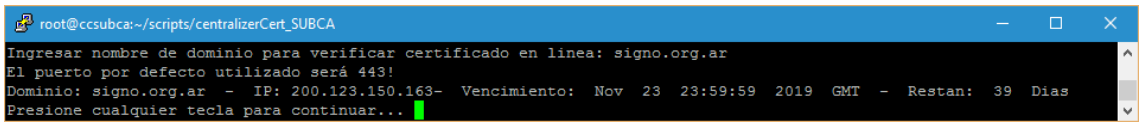

Figura 349. Paso 6 – Ejemplo verificación de vencimiento On-Line

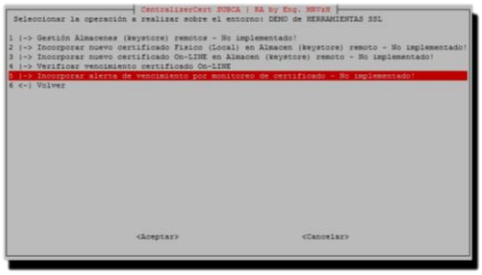

Figura 350. Paso 7A – Ejemplo de operación sin implementar

Figura 351. Paso 7B – Ejemplo de operación sin implementar

2.8.2.19.1. CSR: Pedido de certificado

Para la gestión de certificados externos, existe un set de herramientas básicas diseñadas para permitir realizar una serie de operaciones que se visualizaran a continuación. Básicamente y entre otras acciones permite generar CSR's a demanda, pre definidos o creados en el momento, ya sea para solicitar certificados externos a diversos proveedores, por ejemplo, como así también, simular ser un usuario final y solicitar certificado mediante CSR:

Figura 352. Paso 1 - Pedido de certificado

Figura 353. Paso 2 - Pedido de certificado

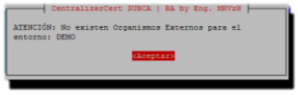

Figura 354. Paso 3 - Pedido de certificado

Figura 355. Paso 4 - Pedido de certificado

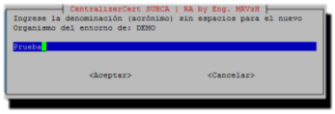

Figura 356. Paso 5 - Pedido de certificado

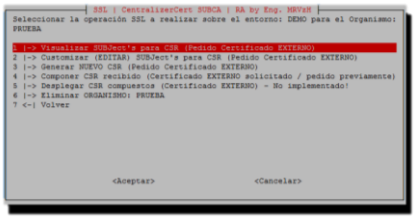

Figura 357. Paso 6 – Pedido de certificado

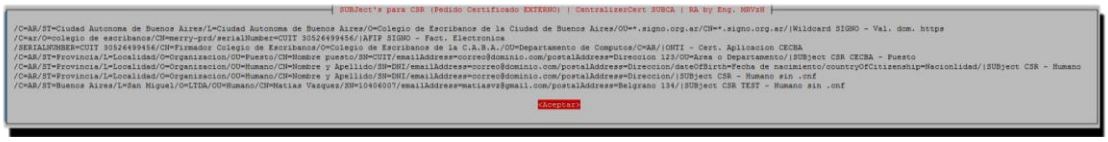

Figura 358. Paso 7 – Ejemplo de Subjets CSR pre cargados

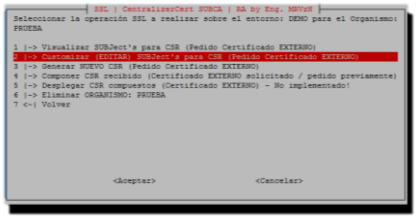

Figura 359. Paso 8 – Edición de Subjets CSR pre cargados

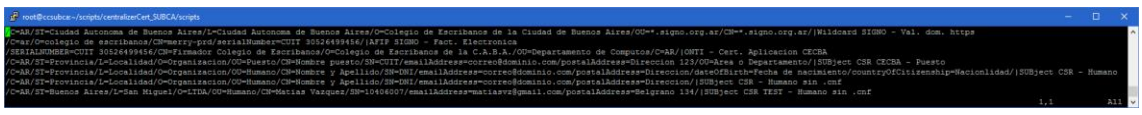

Figura 360. Paso 9 – Ejemplo de edición de Subjets CSR pre cargados

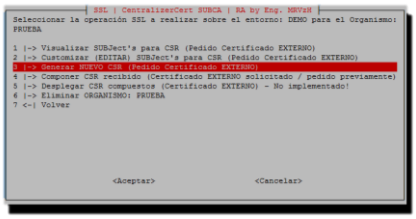

Figura 361. Paso 10 - Pedido de certificado

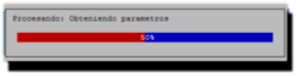

Figura 362. Paso 11 - Pedido de certificado

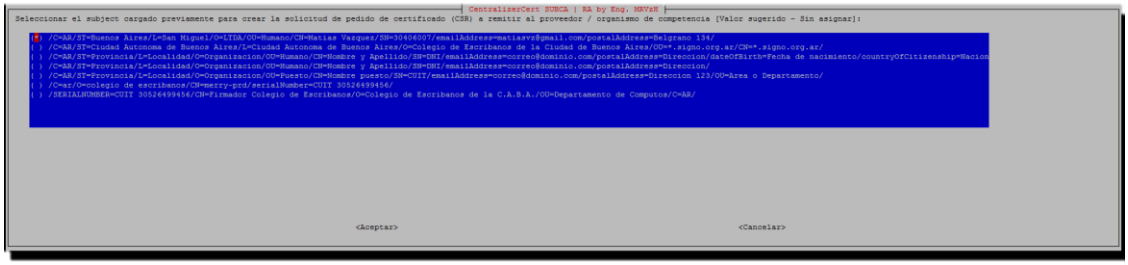

Figura 363. Paso 12 - Pedido de certificado

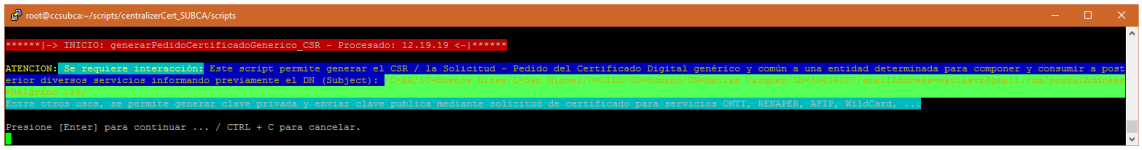

Figura 364. Paso 13 - Pedido de certificado

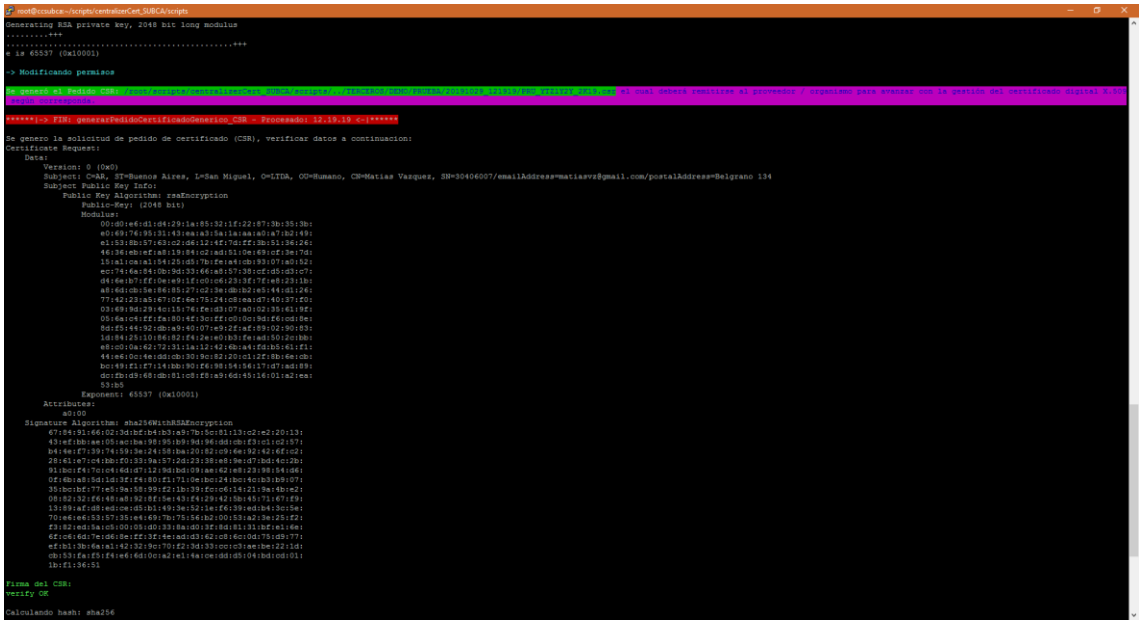

Figura 365. Paso 14 - Pedido de certificado

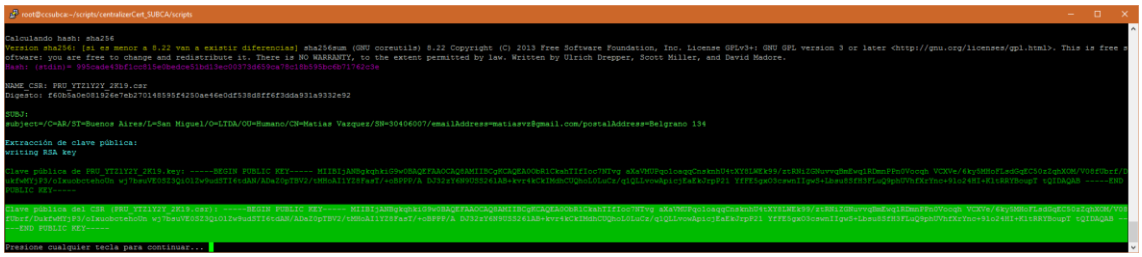

Figura 366. Paso 15 - Pedido de certificado

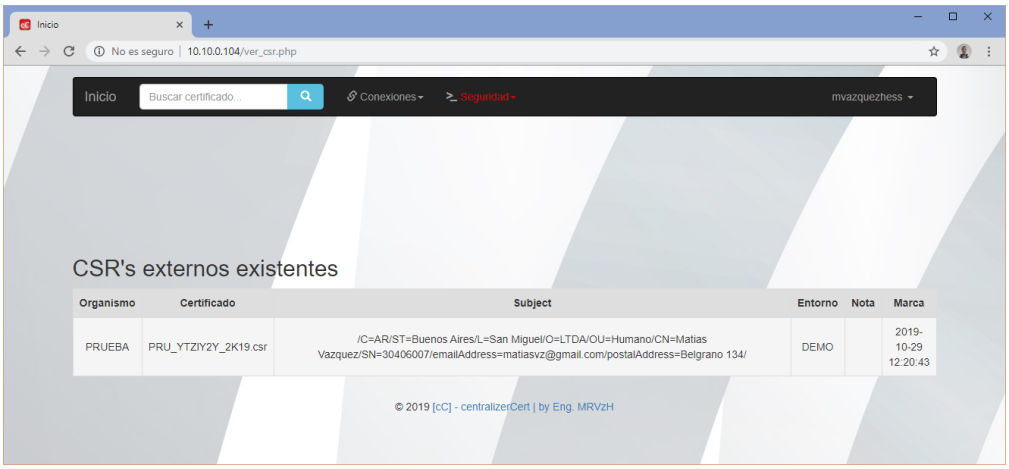

Figura 367. Paso 16 - Pedido de certificado

Figura 368. Paso 17 - Pedido de certificado

Figura 369. Paso 18 - Pedido de certificado

2.8.2.19.2. CSR: Recepción y composición de certificado final

Una vez recibido el certificado solicitado, se deberá componer el mismo, con la clave privada para luego utilizar según corresponda, como se apreciará a continuación:

Figura 370. Paso 1 – Recepción y composición de certificado final

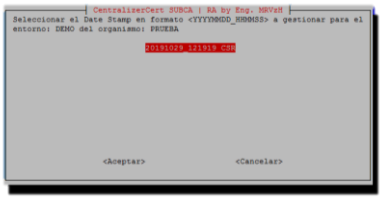

Figura 371. Paso 2 – Recepción y composición de certificado final

Con PEM existente dentro del repositorio:

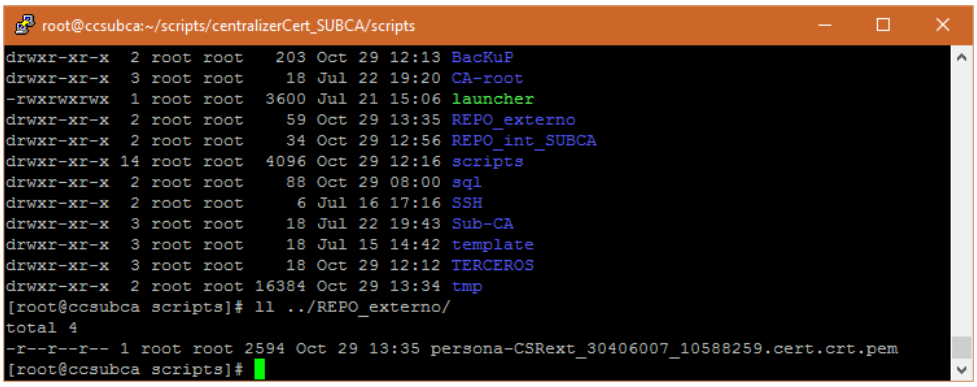

Figura 372. Paso 3 – Recepción y composición de certificado final

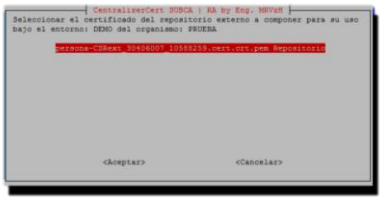

Figura 373. Paso 4A – Recepción y composición de certificado final

Sin PEM existente dentro del repositorio:

Figura 374. Paso 4B – Recepción y composición de certificado final

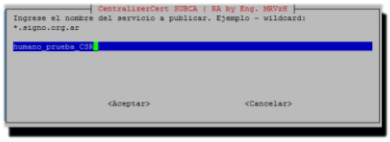

Figura 375. Paso 5 – Recepción y composición de certificado final

Figura 376. Paso 6 – Recepción y composición de certificado final

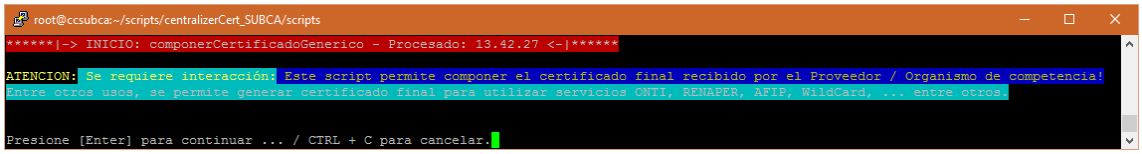

Figura 377. Paso 7 – Recepción y composición de certificado final

Figura 378. Paso 8 – Recepción y composición de certificado final

Figura 379. Paso 9 – Recepción y composición de certificado final

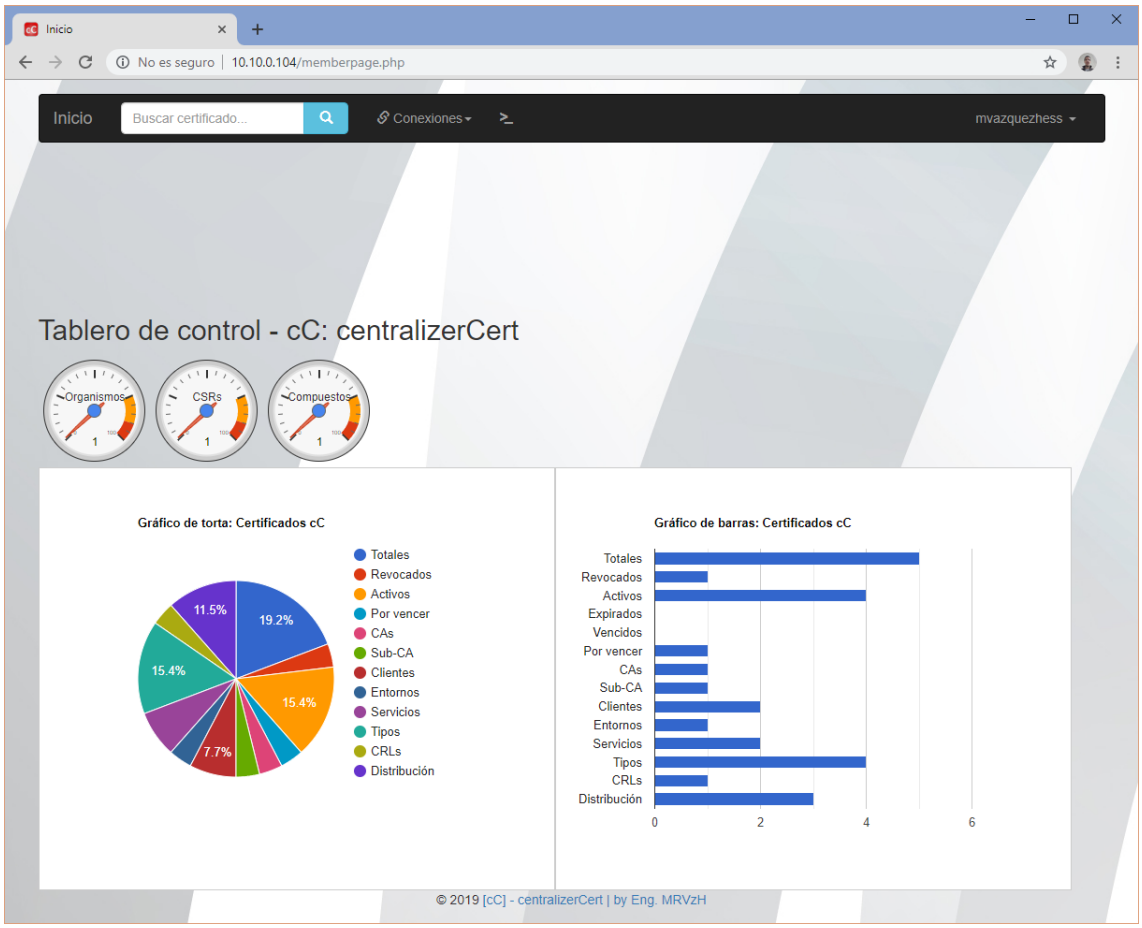

Figura 380. Paso 10 – Recepción y composición de certificado final

2.8.2.20. Validaciones

Entre otras, podemos ver la existencia de diversas validaciones embebidas dentro de la interfaz pura SSH de cC como así también en el backend web, a fin de limitar errores y hacer más sencilla y dinámica la utilización de cC, como podremos apreciar a continuación:

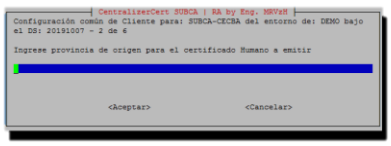

Figura 381. Validaciones varias – Text box campo vacío

Figura 382. Validaciones varias – Text box Mensaje

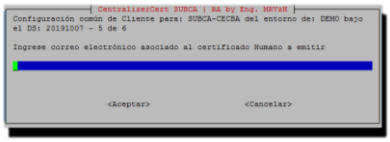

Figura 383. Validaciones varias – Text box correo electrónico

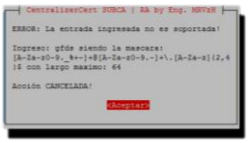

Figura 384. Validaciones varias – Text box Mensaje

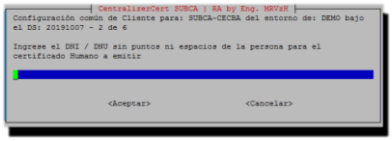

Figura 385. Validaciones varias – Text box Documento de Identidad

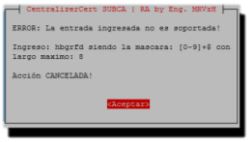

Figura 386. Validaciones varias – Text box Mensaje

Figura 387. Validaciones varias – Check list tipo certificado

Figura 388. Validaciones varias – Check list Mensaje

Para las validaciones en general, el core incorpora una función sobre la cual se pueden incluir diferentes mascaras a validar sobre el control text box desarrollado, por ejemplo, como se puede ver a continuación y entre otras:

Mascara	Validación	Uso
[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}$	Correo electrónico	Correo electrónico valido z@n.l
[[:space:]]*$ || [[:alnum:]]*$	Espacio o números	No permite espacios o números

Tabla 3. Ejemplos de máscaras de validación en controles cC

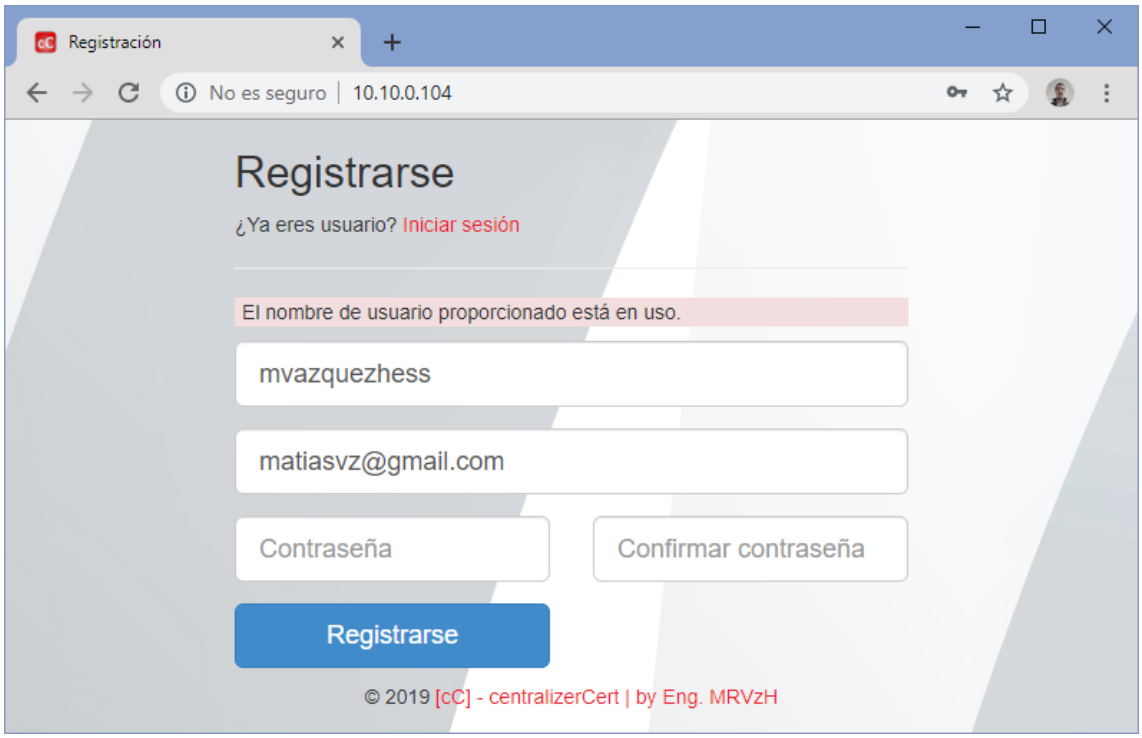

Figura 389. Validaciones varias – Nombre de usuario duplicado

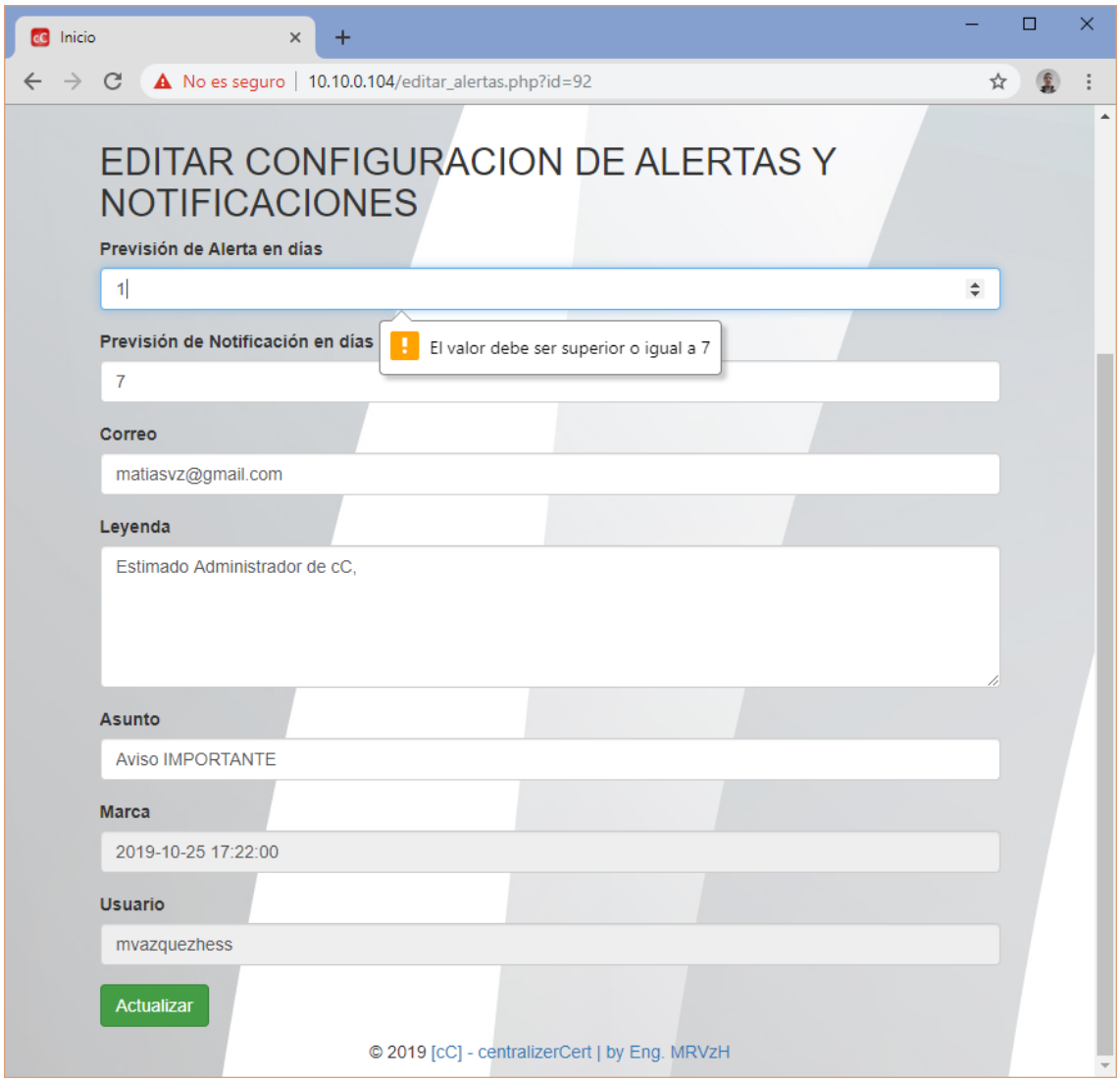

Figura 390. Validaciones varias – Días mínimo y máximos permitidos

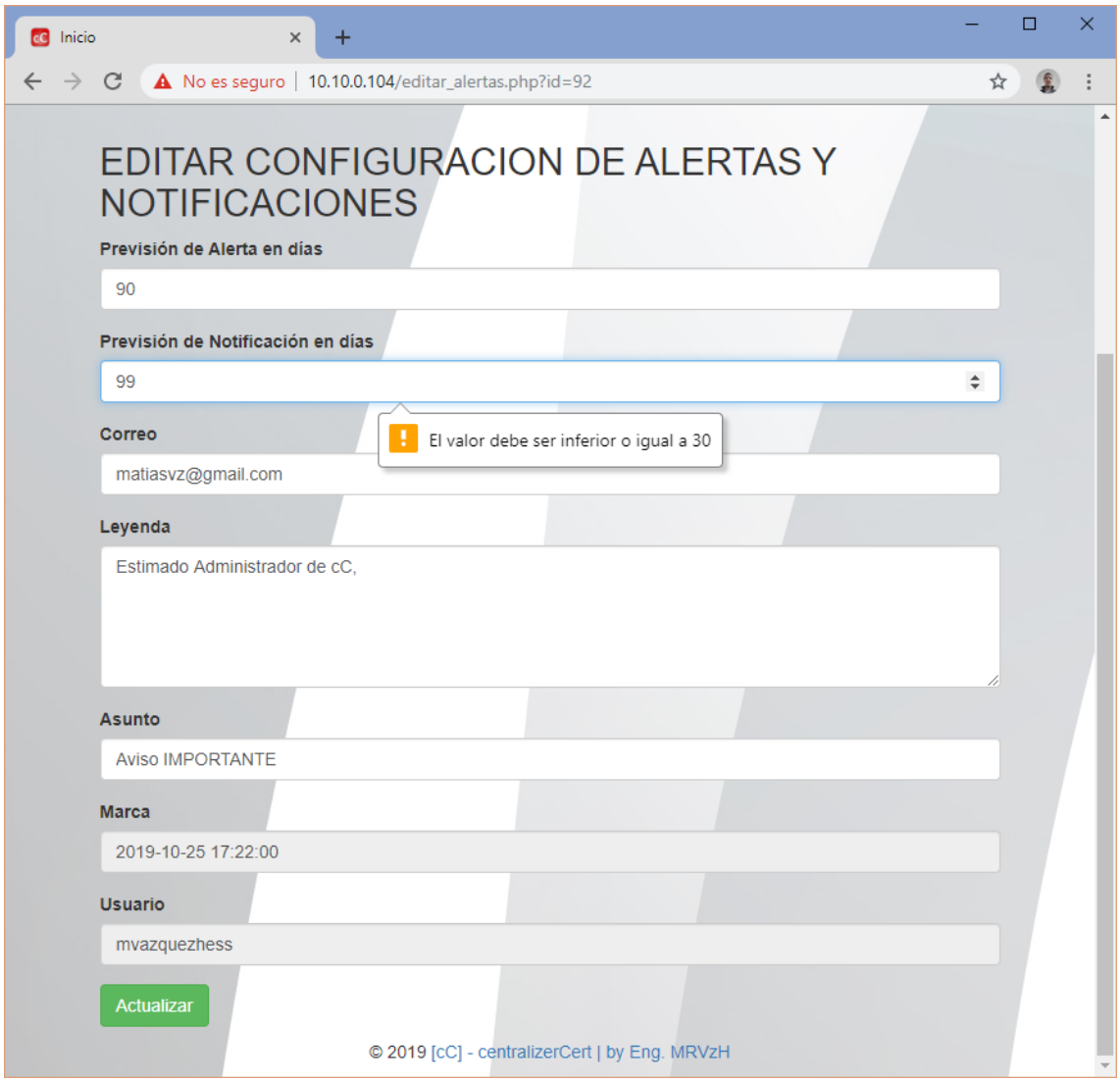

Figura 391. Validaciones varias – Días mínimo y máximos permitidos

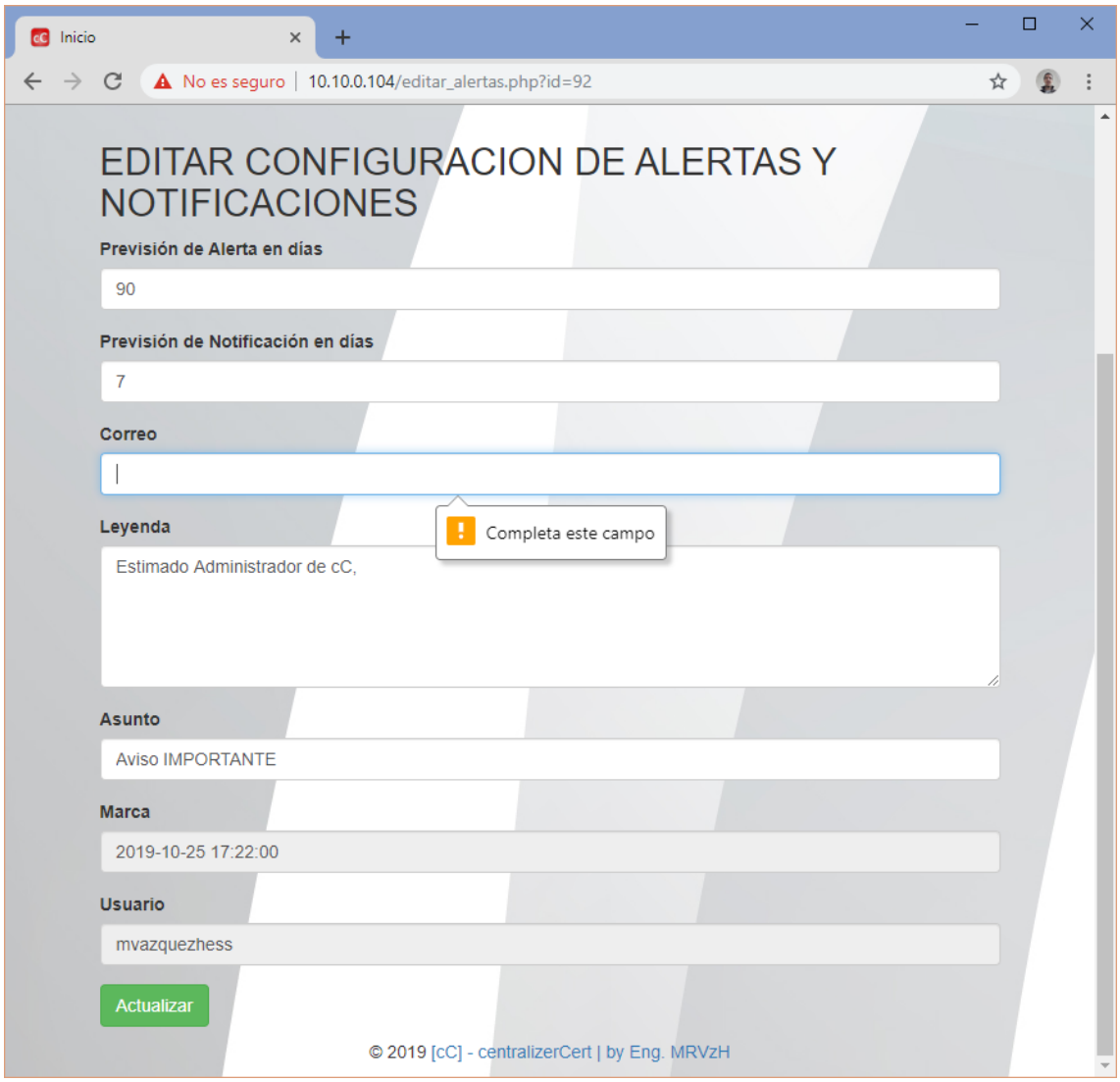

Figura 392. Validaciones varias – Campo vacío

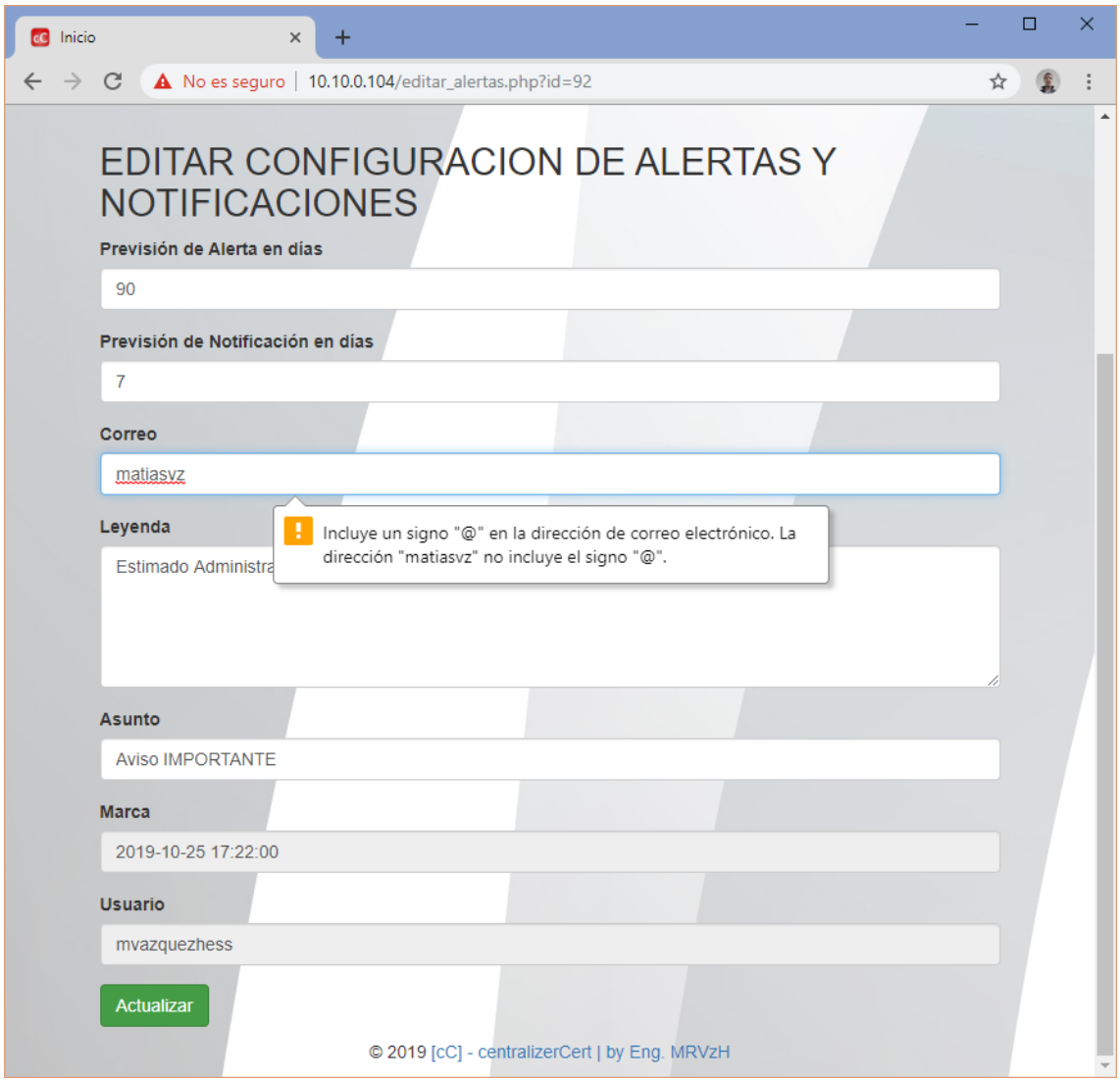

Figura 393. Validaciones varias – Correo electrónico

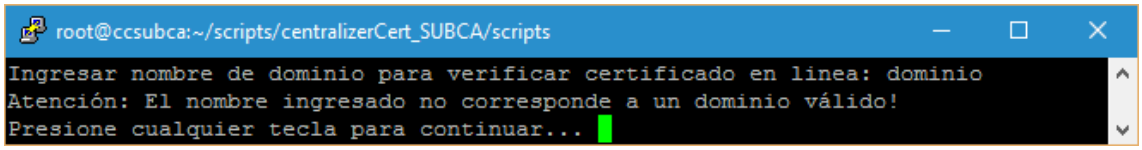

Figura 394. Validaciones varias – Dominio on line

2.8.2.21. Auditoria y manejo de errores

Con el objetivo de disponer de un mecanismo que permita analizar el comportamiento de las acciones realizadas sobre cC, es que se motivó la incorporación a través de su core base, de un mecanismo que refleje el control de cambios involucrado, mediante log detallado auditable. De acuerdo al tipo de archivo se podrá identificar, circunscribir y capturar rápidamente errores, en el caso de visualizar archivos '.ERR', o logs puntuales según corresponda,

como veremos en algunos ejemplos a continuación. Estos, de forma descriptiva tendrán una nomenclatura determinada por: DS + TS + procedimiento involucrado + tipo de archivo, donde permitirán auditar las acciones realizadas en cada momento, siempre y cuando se encuentren encendidas sus entradas correspondientes en el archivo de configuración global:

Figura 395. Paso 1 - Auditoria y manejo de errores

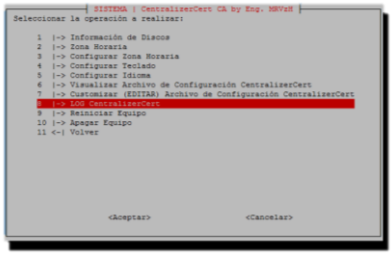

Figura 396. Paso 2 - Auditoria y manejo de errores

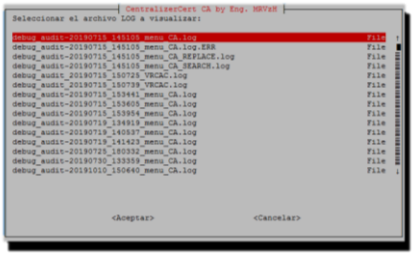

Figura 397. Paso 3 - Auditoria y manejo de errores

Figura 398. Paso 4 - Auditoria y manejo de errores

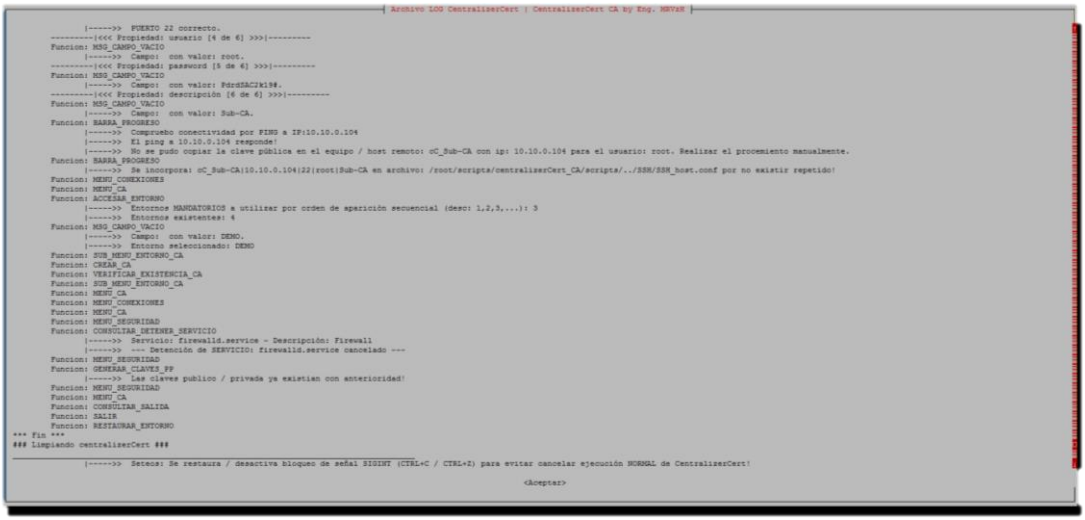

Figura 399. Paso 5 - Auditoria y manejo de errores

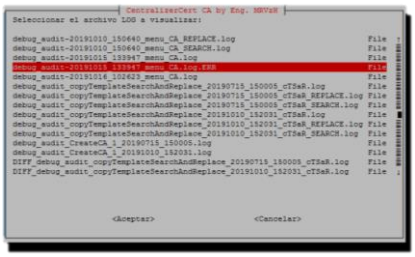

Figura 400. Paso 6 - Auditoria y manejo de errores

Figura 401. Paso 7 - Auditoria y manejo de errores

2.8.2.22. Modo aprendizaje de carga colectiva

Permite, basado en los subjects introducidos con anterioridad y de manera global, sugerir su generación según corresponda, en modo lote, donde se presentará la posibilidad de seleccionar los certificados emitidos y cargados a generar, como veremos en las figuras a continuación, filtrando por tipo de certificado de acuerdo a la selección realizada:

Figura 402. Paso 1 - Modo aprendizaje

Figura 403. Paso 2 - Modo aprendizaje

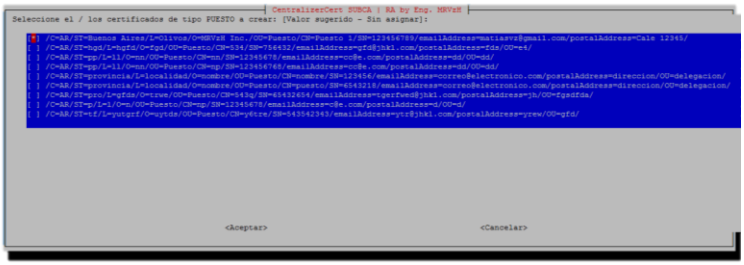

Figura 404. Paso 3 - Modo aprendizaje

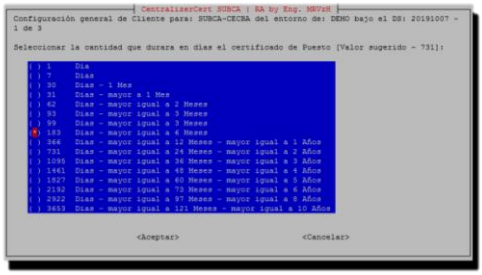

Figura 405. Paso 4 - Modo aprendizaje

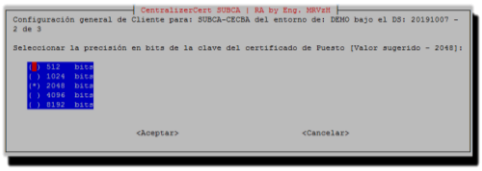

Figura 406. Paso 5 - Modo aprendizaje

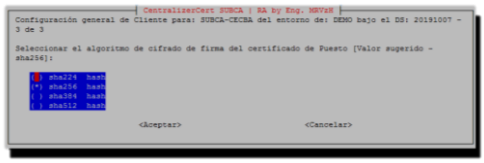

Figura 407. Paso 6 - Modo aprendizaje

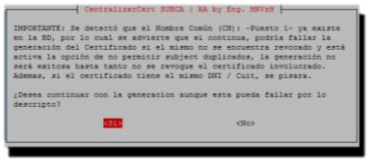

Figura 408. Paso 7 - Modo aprendizaje

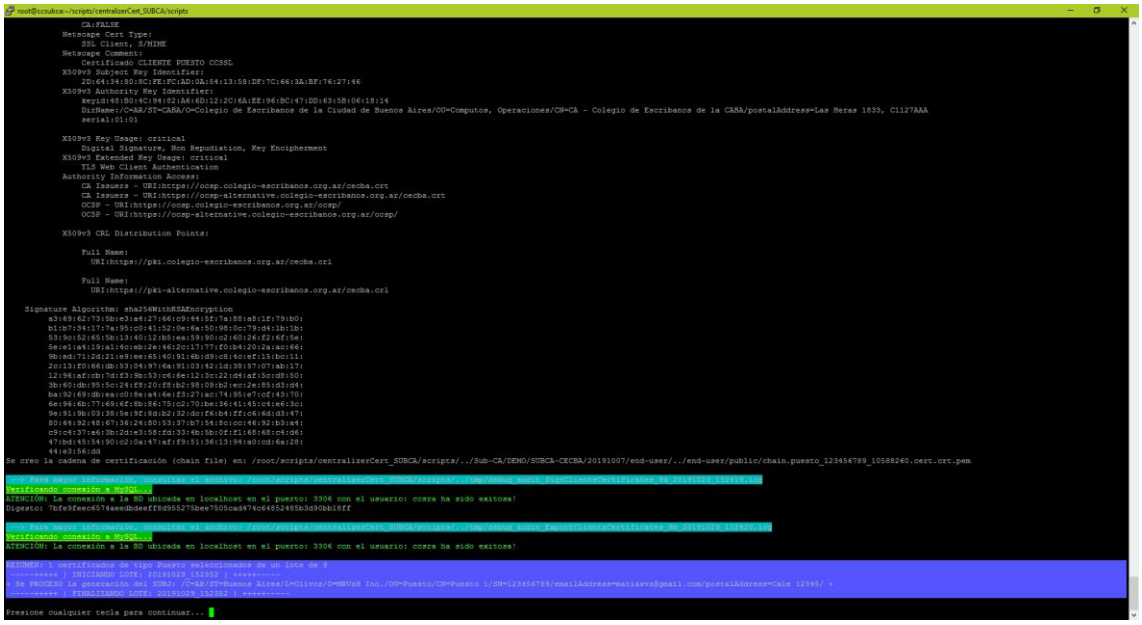

Figura 409. Paso 8 - Modo aprendizaje

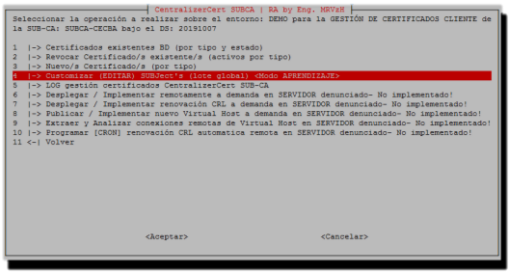

Figura 410. Paso 9 - Modo aprendizaje – Customización de Subject

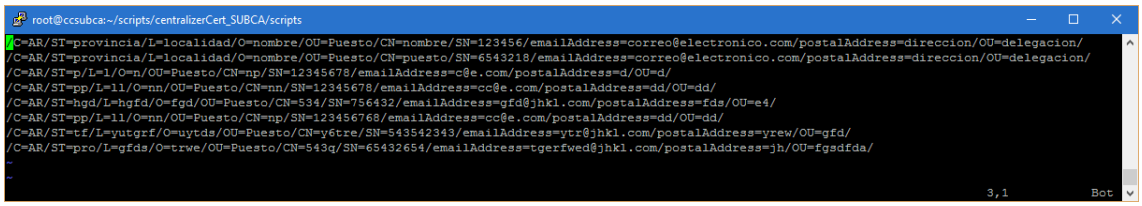

Figura 411. Paso 10 - Modo aprendizaje – Customización de Subject

2.9. Templates SSL

Corresponde a los templates pre configurados inicialmente e incluidos por defecto dentro de cC, lo cuales son detallados a continuación:

Archivo	Tecnología	Tipo
root-ca.cnf	cC CA	CA
human.cnf	cC Sub-CA | RA	Humano
monitoreo.cnf	cC Sub-CA | RA	Monitoreo
point.cnf	cC Sub-CA | RA	Puesto
server.cnf	cC Sub-CA | RA	Servidor
sub-ca.cnf	cC Sub-CA | RA	SubCA

Tabla 4. Templates existentes y pre configurados por cC

2.9.1. cC Sub-CA | RA - Puesto

- `HOME = .` # Ruta relativa
- `RANDFILE = $ENV::HOME/.rnd` # Archivo pseudo aleatorio
- `oid_section = new_oids` # Denominación de sección de identificador de objetos
- `[new_oids]` # Sección: identificador de objetos
  - `postalAddress = 2.5.4.16` # Dirección postal
  - `serialNumber = 2.5.4.5` # Número de serie
- `[ ca ]` # Sección: CA

    - default_ca = CA_default # Denominación de sección CA default
- [CA_default] # Sección: CA default
    - dir = . # Ruta relativa
    - certs = $dir/certs # Ruta certificados
    - crl_dir = $dir/crl # Ruta CRL
    - new_certs_dir = $dir/newcerts # Ruta certificados firmados
    - database = $dir/index.db # Archivo Base de Datos ssl
    - serial = $dir/serial # Archivo serial
    - RANDFILE = $dir/private/.rand # Archivo pseudo aleatorio leer / escribir
    - private_key = $dir/private/puesto.key.pem # Archivo clave privada
    - certificate = $dir/certs/puesto.cert.pem # Archivo de certificado
    - default_md = sha384 # Algoritmo de cifrado de firma por defecto
    - name_opt = ca_default # Define la forma en que el nombre del certificado se verá antes de firmar
    - cert_opt = ca_default # Define la forma en que la información del certificado se verá antes de firmar
    - default_days = 732 # Días por defecto de vida predeterminados del certificado
    - preserve = no # Permite preservar o no el DN
    - policy = policy_match # Denominación de sección de política predeterminada a utilizar para la emisión donde se especifican campos obligatorios, opcionales y necesarios
- [policy_match] # Sección: política por defecto
    - countryName = match # Campo obligatorio
    - stateOrProvinceName = match # Campo obligatorio
    - organizationName = match # Campo obligatorio
    - organizationalUnitName = optional # Campo opcional (no obligatorio)
    - commonName = supplied # Campo necesario
    - emailAddress = match # Campo obligatorio
    - postalAddress = match # Campo obligatorio
    - serialNumber = match # Campo obligatorio
- [req] # Sección: req – Solicitud de certificado (CSR)
    - default_bits = 4096 # Tamaño predeterminado de bits para la clave
    - distinguished_name = req_distinguished_name # Denominación de sección DN

- `string_mask = utf8only` # Definición del tipo de cadenas a aceptar
- `default_md = sha384` # Algoritmo de hash
- `x509_extensions = usr_cert_point_has_san` # Denominación de sección con extensiones x509v3 a solicitar en la solicitud del certificada e incluir en el certificado firmado

- `[ req_distinguished_name ]` # Sección: información DN – Define como formar el DN
  - `countryName_min = 2` # Tamaño máximo de país predeterminado
  - `countryName_max = 2` # Tamaño mínimo de país predeterminado
  - `countryName = Pais (Codigo de 2 letras ISO 3166)` # Nombre del país
  - `stateOrProvinceName = Provincia` # Provincia
  - `localityName = Localidad` # Localidad
  - `0.organizationName = Nombre de la Organizacion` # Nombre de la organización
  - `organizationalUnitName = Tipo de certificado` # Tipo de certificado
  - `commonName = Nombre del PUESTO` # Nombre del certificado
  - `emailAddress = Email` # Correo electrónico
  - `postalAddress = Direccion` # Dirección postal
  - `serialNumber = C.U.I.T. (sin puntos ni guiones)` # CUIT de la organización
  - `countryName_default = AR` # Valor predeterminado de país
  - `stateOrProvinceName_default = CABA` # Valor predeterminado de provincia
  - `localityName_default = CABA` # Valor predeterminado de localidad
  - `0.organizationName_default = Organizacion` # Valor predeterminado de Organización
  - `organizationalUnitName_default = Puesto` # Valor predeterminado de área o departamento
  - `emailAddress_default = correo` # Valor predeterminado de correo electrónico
  - `postalAddress_default = Direccion` # Valor predeterminado de dirección postal
- `[ usr_cert_point_has_san ]` # Sección: x509v3 [16] con parametrización del certificado a firmar
  - `basicConstraints = CA:FALSE` # Indica que el certificado no podrá ser utilizado como CA
  - `nsCertType = client` # Tipo de certificado

- `nsComment = "POINT client Certificate to centralizerCert"` # Comentario del certificado
- `subjectKeyIdentifier = hash` # Método de identificación de llave publica
- `authorityKeyIdentifier = keyid,issuer` # Forma de identificación de llave publica
- `keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment` # Uso de clave
- `extendedKeyUsage = clientAuth` # Propósito de utilización de clave publica

Para conocer en detalle, el resto de los templates existentes, ver: Ampliación de Templates SSL.

2.10. Configuración global

El archivo de configuración global, se creó con el propósito de disponer de una arquitectura flexible, dinámica y escalable, la cual de forma muy rápida y breve implemente los cambios necesarios a fin de disponer de un ambiente concreto y customizable. Dependiendo de la tecnología involucrada, se detalla en la tabla a continuación los archivos según corresponda:

Archivo	Tecnología
config.ini	cC CA
config.ini	cC Sub-CA | RA

Tabla 5. Configuraciones globales existentes y pre configuradas incluidas en cC

La segmentación en diversos apartados permite una organización y agrupación estratégica, como podremos observar:

2.10.1. Config.ini: cC Sub-CA | RA

Sección: VARIABLES GLOBALES

- `ABOUT_FILE="about"` # Archivo acerca de
- `SPLASH_FILE="splash"` # Archivo de pantalla inicio
- `CORE_VERSION="version"` # Archivo de número de versión
- `GLOBAL_TMP="tmp"` # Ruta temporal

- GLOBAL_CERT="" # Ruta CA
- GLOBAL_DEBUG="ON | OFF" # Auditoria: control de cambios y errores
- GLOBAL_DEBUG_FULL="ON | OFF" # Auditoria verborragica
- GLOBAL_DEBUG_PREFIX="debug_audit" # Prefijo archivo de auditoria
- GLOBAL_DEBUG_PREFIX_COPY_TEMPLATE="debug_audit_copyTemplateSearchAndReplace" # Prefijo archivo nuevo template
- GLOBAL_TIME_SHUTDOWN_REBOOT="3" # Tiempo de espera en minutos para programar apagado o reinicio de VM
- GLOBAL_TIME_OUT_CONNECT="2" # Tiempo de espera en segundos para cancelar comandos de conexión remota
- GLOBAL_BKP="BacKuP" # Ruta backup
- GLOBAL_SSH_SCP="SSH" # Protocolo SCP
- GLOBAL_BKP_PREFIX="BKP" # Prefijo backup
- GLOBAL_VACIO="Sin asignar" # Leyenda texto vacío
- GLOBAL_PSEUDORANDOM="archivoAleatorioDeUsoUnico" # Prefijo archivo pseudo aleatorio de utilización temporal
- DATESTAMP=date +%Y%m%d # Prefijo archivo DS
- TIMESTAMP=date +%H%M%S # Prefijo archivo TS
- DATETIMESTAMP=date +%Y%m%d_%H%M%S # Prefijo archivo DTS

Sección: INTERFAZ GRAFICA GLOBAL

- TITLE="CentralizerCert SUBCA | RA by Eng. MRVzH" # Titulo de interfaz
- BACKTITLE="centralizerCert es una creación del Ing. Matias Vazquez Hess / Eng. MRVzH - Copyright (c) 2018 - 2019 [AR]" # Titulo secundario de interfaz
- GUI="whiptail" # Interfaz gráfica utilizada
- GUI_FILE_CORRECTION="6" # Parámetro de corrección visual de archivo
- GUI_TERMINAL_CORRECTION="10" # Parámetro de corrección visual de terminal
- YES_BTN="Si" # Leyenda botón Si
- NO_BTN="No" # Leyenda botón No
- OK_BTN="Aceptar" # Leyenda botón Aceptar
- CANCEL_BTN="Cancelar" # Leyenda botón Cancelar
- FACTOR_ENVIRONMENT=3 # Cantidad de entornos a leer de la sección environment

Sección: MENSAJES GLOBALES

- MSG_DISCLAIMER="ATENCIÓN: Se encuentra ejecutando 'centralizerCert' para la administración de sus certificados

SSL. Los scripts involucrados pueden ser difíciles de depurar porque la interfaz oculta algunos mensajes de error. Por esta razón, a pesar de tomar el cuidado necesario en su escritura, puede quedarse atascado en una pantalla sin poder cancelar. Esto puede forzarlo a cancelar una sesión SSH o matar el proceso zombie.\n\nIMPORTANTE: ¡Las acciones a realizar a partir de este momento, no son reversibles!\n\n¿Desea continuar?" # Mensaje de Descargo de responsabilidad

- MSG_KEY_TO_CONTINUE="Presione cualquier tecla para continuar..." # Mensaje para reanudar ejecución

Sección: environment

- ENVMT_1="PRODUCCION" # Entorno 1
- ENVMT_2="TESTING" # Entorno 2
- ENVMT_3="demo" # Entorno 3
- ENVMT_4="validacion" # Entorno 4
- … # Entorno …

Sección: template

- TEMPLATE_ROOT_CA="root-ca.cnf" # Archivo ssl template base CA
- TEMPLATE_SUB_CA="sub-ca.cnf" # Archivo ssl template base Sub-CA
- TEMPLATE_SERVER="server.cnf" # Archivo ssl template base Servidor
- TEMPLATE_HUMAN="human.cnf" # Archivo ssl template base Humano
- TEMPLATE_POINT="point.cnf" # Archivo ssl template base Puesto
- TEMPLATE_MONITORING="monitoreo.cnf" # Archivo ssl template base Monitoreo

Sección: subcaroot

- SUBCA_PREFIX="" # Prefijo Sub-CA
- SUBCA_BASED_ROOT_CA_MSK="CA-root" # Mascara de CA
- SUBCA_MSK="Sub-CA" # Mascara de Sub-CA
- SUBCA_LOG="log" # Ruta log
- SUBCA_CSR="CSR" # Ruta CSR interno
- SUBCA_REPO_CSR_EXTERNO="REPO_int_SUBCA" # Ruta CSR externo
- SUBCA_LOG_CLIENTS_LOTE_ABORT="abort" # Tag log aborte lote
- SUBCA_LOG_CLIENTS_LOTE_PROCESS="ok" # Tag log lote ok
- SUBCA_LOG_CLIENTS_LOTE_SUMMARY="summary" # Tag log resumen lote

- SUBCA_MSK_CLIENTS="end-user" # Ruta archivos clientes
- SUBCA_FILENAME_KEY_SSH_REMOTE="id_rsa" # Archivo llave ssh
- SUBCA_FILENAME_KEY_SSH_REMOTE_HOST="SSH_host.conf" # Archivo host ssh
- SUBCA_FILENAME_TYPE_CLIENT="subcaTypeClient.conf" # Archivo tipos de clientes
- SUBCA_FILENAME_STATUS_CERT_TYPE="subcaStatus.conf" # Archivo estados de certificados
- SUBCA_BASED_ON_CA="CA_BASE" # Archivo con ruta a CA root en que se basó Sub-CA
- SUBCA_BASED_SERVICE="SERVICE_SUBCA" # Nombre del servicio por defecto
- SUBCA_UNIQUE_SUBJECT="OFF | ON" # Permite DN (nombres) duplicados
- SUBCA_NAME_SERVER="Servidor" # Nombre a mostrar para tipo Servidor
- SUBCA_NAME_HUMAN="Humano" # Nombre a mostrar para tipo Servidor
- SUBCA_NAME_POINT="Puesto" # Nombre a mostrar para tipo Servidor
- SUBCA_NAME_MONITORING="Monitoreo" # Nombre a mostrar para tipo Servidor
- SUBCA_NAME_TAG_SERVER="server" # Nombre sección SSL Sub-CA para certificados de tipo servidor
- SUBCA_NAME_TAG_HUMAN="person" # Nombre sección SSL Sub-CA para certificados tipo humano
- SUBCA_NAME_TAG_POINT="point" # Nombre sección SSL Sub-CA para certificados tipo puesto
- SUBCA_NAME_TAG_MONITORING="monitor" # Nombre sección SSL Sub-CA para certificados tipo monitor
- #------ Valores sugeridos ------
    - SUBCA_ACRONYM_DEFAULT="SUBCA-CECBA" # Acrónimo sugerido por defecto
    - SUBCA_COUNTRIES_FILE="subcaCountry.conf" # Archivo países
    - SUBCA_DAYS_FILE="subcaDays.conf" # Archivo días
    - SUBCA_MD_FILE="subcaMD.conf" # Archivo cifrado
    - SUBCA_BITS_FILE="subcaBits.conf" # Archivo bits
    - SUBCA_CRL_DAYS_FILE="subcaCRL.conf" # Archivo días
    - SUBCA_REVOKE_REASON_FILE="subcaReasonRevoke.conf" # Archivo motivos de revocación
    - SUBCA_DAYS_ON_DEFAULT_LIST="3653" # Días sugeridos por defecto para en general
    - SUBCA_DAYS_ON_DEFAULT_LIST_SERVER="1461" # Días sugeridos por defecto para servidor

- SUBCA_DAYS_ON_DEFAULT_LIST_MONITORING="1461" # Días sugeridos por defecto para monitoreo
- SUBCA_DAYS_ON_DEFAULT_LIST_CLIENTS="731" # Días sugeridos por defecto para clientes en general
- SUBCA_DAYS_ON_DEFAULT_CRL="60" # Días sugeridos por defecto para clientes CRL
- SUBCA_MD_ON_DEFAULT="sha256" # Algoritmo de cifrado sugerido por defecto
- SUBCA_BITS_ON_DEFAULT="2048" # Tamaño de la clave sugerida por defecto
- SUBCA_REVOKE_REASON_ON_DEFAULT="unspecified" # Razón de revocación sugerida por defecto
- SUBCA_COUNTRY_NAME_DEFAULT="AR" # País sugerido por defecto
- SUBCA_STATE_OR_PROVINCE_NAME_DEFAULT="CABA" # Provincia sugerida por defecto
- SUBCA_LOCALITY_NAME_DEFAULT="CABA" # Localidad sugerido por defecto
- SUBCA_ORGANIZATION_NAME_DEFAULT="Colegio de Escribanos de la Ciudad de Buenos Aires" # Organización sugerido por defecto
- SUBCA_COMMON_NAME_DEFAULT="SUBCA | Intermediate CA - nombre de SERVICIO SubCA" # Nombre de Sub-CA sugerido por defecto
- SUBCA_ORGANIZATIONAL_UNIT_NAME_DEFAULT="Computos, Operaciones" # Área o Departamento sugerido por defecto
- SUBCA_EMAIL_ADDRESS_DEFAULT="pki@colegio-escribanos.org.ar" # Correo sugerido por defecto
- SUBCA_POSTAL_ADDRESS_DEFAULT="Las Heras 1833, C1127AAA" # Dirección sugerida por defecto
- SUBCA_DNS_PRIMARY_DEFAULT="CECBA Intermidiate CA 1" # DNS primario sugerido por defecto
- SUBCA_DNS_SECONDARY_DEFAULT="CECBA CA Intermidiate 1" # DNS secundario sugerido por defecto
- SUBCA_URI_CRL_PRIMARY_DEFAULT="https://pki.colegio-escribanos.org.ar/cecba.crl" # CRL primaria sugerida por defecto
- SUBCA_URI_CRL_SECONDARY_DEFAULT="https://pki-alternative.colegio-escribanos.org.ar/cecba.crl" # CRL secundaria sugerida por defecto

- SUBCA_URI_OCSP_CRT_PRIMARY_DEFAULT="https://ocsp.colegio-escribanos.org.ar/cecba.crt" # CRT primario sugerido por defecto
- SUBCA_URI_OCSP_CRT_SECONDARY_DEFAULT="https://ocsp-alternative.colegio-escribanos.org.ar/cecba.crt" # CRT secundario sugerido por defecto
- SUBCA_URI_OCSP_PRIMARY_DEFAULT="https://ocsp.colegio-escribanos.org.ar/ocsp/" # OCSP primario sugerido por defecto
- SUBCA_URI_OCSP_SECONDARY_DEFAULT="https://ocsp-alternative.colegio-escribanos.org.ar/ocsp/" # OCSP secundario sugerido por defecto
- SUBCA_SERIAL_NUMBER="A1905B" # Número de serie hexadecimal de inicio
- SUBCA_CRL_NUMBER="01" # Número de CRL inicial

Sección: ra

- RA_ACRONYM_DEFAULT="ORGANISMO" # Acrónico de organismo
- RA_GENERAL_MSK="TERCEROS" # Mascara general
- RA_GENERAL_TOOL_MSK="tools" # Mascara de herramientas
- RA_SUBJ_DN_FILE="subjDNRA.conf" # Archivo de Subjects por tipo soportados
- RA_TYPE_FILE="typeRA.conf" # Archivo de tipos de RA soportados
- RA_LOG="LOG" # Ruta log
- RA_SUBJ_FILE="subRA.lot" # Archivo de lotes de RA
- #--- Certificados externos de aplicación ---
  - RA_APPLICATION_PREFIX="" # Prefijo
  - RA_APPLICATION_MSK="applicacion" # Mascara
  - RA_APPLICATION_NAME="Aplicacion" # Nombre
- #--- Certificados externos de facturación electrónica ---
  - RA_ELECTRONIC_BILLING_PREFIX="" # Prefijo
  - RA_ELECTRONIC_BILLING_MSK="facElectronica" # Mascara
  - RA_ELECTRONIC_BILLING_NAME="Facturacion" # Nombre
- #--- Certificados externos de servidor ---
  - RA_SERVER_PREFIX="" # Prefijo
  - RA_SERVER_MSK="servidor" # Mascara
  - RA_SERVER_NAME="Servidor" # Nombre
- #--- Certificados externos de validación de dominios (wildcard)---
  - RA_DOMAIN_VALIDATION_PREFIX="" # Prefijo
  - RA_DOMAIN_VALIDATION_MSK="validaDominio" # Mascara

    - RA_DOMAIN_VALIDATION_NAME="Validacion" # Nombre
- #---REPOSITORIO EXTERNO DE CERTIFICADOS RECIBIDOS DE ORGANISMOS / PROVEEDORES...
    - RA_REPO_RA="REPO_externo" # Ruta repositorio externo

Sección: db

- DB_USER="ccsra" # Usuario
- DB_PASS="XXXXX" # Contraseña
- DB_HOST="10.10.0.104" # Dirección IP
- DB_PORT="3306" # Puerto
- DB_BD="centralizerCert" # Nombre de la BD
- DB_BKP="sql" # Ruta backup
- DB_OFF="offdb" # Nombre archivo consulta DB pendiente

Sección: web

- WEB_SERVER_NAME="centralizerCert" # Nombre virtual host
- WEB_SERVER_PORT="80" # Puerto
- WEB_SERVER_MAIL="no-reply.cecba.ar@gmail.com" # Dirección de correo

Sección: email

- EMAIL_REALNAME="cC: centralizerCert" # Nombre
- EMAIL_FROM="no-reply.centralizerCert@gmail.com" # Remitente
- EMAIL_USER="centralizercert@gmail.com" # Dirección de correo
- EMAIL_PASS="XXXXX" # Contraseña
- EMAIL_SMTP="smtp://centralizercert@gmail.com@smtp.gmail.com:587/" # SMTP
- EMAIL_FOLDER="imaps://imap.gmail.com:993" # Dirección IMAP
- EMAIL_SEND_TEST="matiasvz@gmail.com" # Dirección test de correo
- EMAIL_SEND_ADMIN="matiasvz@gmail.com" # Correo del administrador

Para conocer el archivo pre configurado correspondiente a la cC CA, ver: Config.ini: cC CA.

2.11. Archivos dinámicos

Con el objetivo de obtener una solución flexible, dinámica y escalable en él tiempo, contamos con la posibilidad de incorporar dentro de las opciones

interactivas, datos dinámicos según las necesidades, los cuales permiten que los mismos sean escalables y resistentes al tiempo, como se podrá observar a continuación. Esto permite mantener el código fuente original, incorporando nueva parametrización, convirtiendo a cC en resistente a la obsolescencia programada con un mecanismo defensivo.

La tecnología común del core de cC, incluye de forma común para las CA y Sub-CA:

- Tamaño de generación de clave en Bits: 512, 1024, 2048, …
- Duración en días de los certificados: 1, 7, 30, 31, 62, 93, …
- Algoritmo de cifrado de firma: sha224, sha256, sha384, …

Específicamente para la Sub-CA se incorporan, además:

- País de origen: …, AR Argentina, …
- Frecuencia de renovación de CRL en días: 30, 45, 60, …
- Estados permitidos de certificados: V - Valido, R - Revocado, E - Caduco
- Razones de revocación de certificados: sin especificar, Clave comprometida, CA comprometida, …
- Tipos de clientes: Humano, Puesto, Servidor, Monitoreo, Todos

Entre otros.

Los mismos son identificados por estar codificados bajo la extensión '.conf' e incluidos dentro del archivo de configuración global en la ruta '/scripts'.

Archivo	Tecnología	Función
caBits.conf	cC CA	Tamaño de clave RSA
caDays.conf	cC CA	Duración en días del certificado
caMD.conf	cC CA	Algoritmo de cifrado de firma
subcaBits.conf	cC Sub-CA | RA	Tamaños de claves soportadas
subcaCountry.conf	cC Sub-CA | RA	Países soportados
subcaCRL.conf	cC Sub-CA | RA	Frecuencia en días de renovación
subcaDays.conf	cC Sub-CA | RA	Duración en días del certificado
subcaMD.conf	cC Sub-CA | RA	Algoritmo de cifrado de firma
subcaReasonRevoke.conf	cC Sub-CA | RA	Razones de revocación soportadas

subcaStatus.conf	cC Sub-CA | RA	Estados de certificados soportados
subcaTypeClient.conf	cC Sub-CA | RA	Tipos de clientes soportados
subjDNRA.conf	cC Sub-CA | RA	Subjets soportados por la RA
typeRA.conf	cC Sub-CA | RA	Tipos de certificados RA soportados

Tabla 6. Datos dinámicos parametrizables resistentes a la obsolescencia programada

2.12. Control de versiones

Con el fin de lograr un control de versiones de código fuente de cC, se escribió el siguiente script para su administración controlada de versiones:

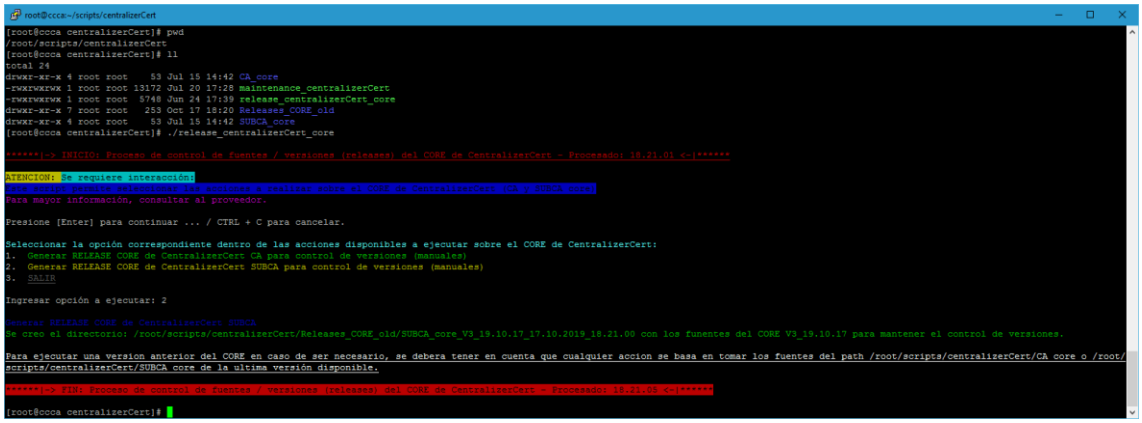

Figura 412. Control de versiones

2.13. Aportes principales

A modo de síntesis, se detallan las principales características desarrolladas a lo largo del presente trabajo con el fin de destacar los aspectos más sobresalientes de cC a tener en cuenta:

- Trazabilidad auditable por control de cambios
- Visibilidad por tablero de control y búsqueda unificada
- Gestión centralizada de múltiples fuentes
- Alerta pro activa e identificación temprana de vencimientos
- Distribución efectiva
- Facilidad de uso e integración
- Limitación de errores humanos
- Reducción de complejidad para el usuario
- Integración de múltiples certificados y fuentes
- Portabilidad

- Diseño flexible y escalable
- Confianza
- Control de perdidas
- Emisión, revocación, expiración y destrucción segura
- Explotación y exploración de datos
- Soporte con monitoreo activo de canales (zondas) y servicios (publicados) de certificados propios por uptime y expiración

2.14. Futuro

Con el objetivo de generar un desarrollo sustentable y sostenible en el tiempo, se evaluará en etapas futuras la posibilidad de incorporar las siguientes líneas con el simple hecho de ampliar en el tiempo las ventajas que brindaría potencialmente cC:

- ✓ Appliances Virtuales: a discreción
- ✓ FrontEnd: público de gestión para usuarios finales con solicitud de certificado, baja y rectificación de datos
- ✓ Incorporación de TSA [17] [18]
- ✓ Incorporación de validación remota de identidad con Renaper (SID)[19]
- ✓ Incorporación de bloqueo de acceso: en tiempo real por geolocalización y saltos
- ✓ Incorporación de seguimiento: accesos por usuario y certificado
- ✓ Detección de conexiones en tiempo real y en modo diferido
- ✓ Incorporación de certificación cruzada
- ✓ Incorporación de mecanismos no soportados
- ✓ Incorporación de doble factor de autenticación
- ✓ Identificación: distribución de cedula al cliente final, con el fin de identificar el puesto y su vencimiento tanto por este como para casos que requieran soporte (análogamente seria como los datos del conductor exhibidos al pasajero en un taxi AR [20]), para dar mayor transparencia y fiabilidad respecto al operador autorizado por organismos.

Entre otros.

3. Conclusiones

En la actualidad, la problemática inherente a la gestión de múltiples certificados, reviste de un nivel de complejidad tal, que se torna un cuello de botella crítico. Más aun, cuando no existe la posibilidad de disponer de personal especializado. Dado que para lograr los objetivos del negocio o poder desarrollar las actividades cotidianas, existen una amplia gama de factores a considerar además de las amenazas y vulnerabilidades asociadas. Donde entendemos que la seguridad de la información es más que un problema de seguridad de datos, orientado a proteger la propiedad intelectual tanto de organizaciones como de personas.

Recordemos que los certificados son un mecanismo potente y seguro; pero en la mayoría de los casos, por más seguro que estos sean, un uso negligente o el desconocimiento, podría producir más riesgos que beneficios.

Ahora bien, y luego de evaluar el prototipo implementado, de acuerdo al análisis pormenorizado desarrollado, conjuntamente con de las definiciones adoptadas, y con el fin de aprovechar la experiencia y los modelos existentes en tal materia, se puede concluir que es más que viable el modelo cC planteado, afirmando que es posible centralizar los certificados digitales de una organización sin el presupuesto necesario para la adquisición de más de una herramienta y sin personal especializado, sea cual fuere su envergadura. Por tal motivo, se corrobora la hipótesis planteada de forma afirmativa, y se entiende, que el modelo implementado corresponde a un aporte importante en tal materia, haciendo uso de herramientas triviales, y no tanto conjuntamente, además de aplicar el ingenio y sentido común sobre el mismo.

4. Anexo

El presente anexo tiene como finalidad, explicar y ampliar según corresponda, los términos técnicos y específicos que se usan en la presente Tesis de Maestría, como así también fomentar su uso razonable y correcto, aplicando la terminología específica para lograr una comprensión clara y eficaz.

4.1. Ampliación de Configuración Global

La configuración global es de vital importancia. Por ello, se incorpora el detalle del archivo de configuración incluido en cC CA a fin de poder ampliar y conocer la misma.

4.1.1. Config.ini: cC CA

Sección: VARIABLES GLOBALES

- `ABOUT_FILE="about"`
- `SPLASH_FILE="splash"`
- `CORE_VERSION="version"`
- `GLOBAL_TMP="tmp"`
- `GLOBAL_CERT=""`
- `GLOBAL_DEBUG="ON|OFF"`
- `GLOBAL_DEBUG_FULL="ON|OFF"`
- `GLOBAL_DEBUG_PREFIX="debug_audit"`
- `GLOBAL_DEBUG_PREFIX_COPY_TEMPLATE="debug_audit_copyTemplateSearchAndReplace"`
- `GLOBAL_TIME_SHUTDOWN_REBOOT="3"`
- `GLOBAL_BKP="BacKuP"`
- `GLOBAL_SSH_SCP="SSH"`
- `GLOBAL_BKP_PREFIX="BKP"`
- `GLOBAL_VACIO="Sin asignar"`
- `DATESTAMP=date +%Y%m%d`
- `TIMESTAMP=date +%H%M%S`
- `DATETIMESTAMP=date +%Y%m%d_%H%M%S`

Sección: INTERFAZ GRAFICA GLOBAL

- TITLE="CentralizerCert CA by Eng. MRVzH"
- BACKTITLE="centralizerCert es una creación del Ing. Matias Vazquez Hess / Eng. MRVzH - Copyright (c) 2018 - 2019 [AR]"
- GUI="whiptail"
- GUI_FILE_CORRECTION="6"
- GUI_TERMINAL_CORRECTION="10"
- YES_BTN="Si"
- NO_BTN="No"
- OK_BTN="Aceptar"
- CANCEL_BTN="Cancelar"
- FACTOR_ENVIRONMENT=3

Sección: MENSAJES GLOBALES

- MSG_DISCLAIMER="ATENCIÓN: Se encuentra ejecutando 'centralizerCert' para la administración de sus certificados SSL. Los scripts involucrados pueden ser difíciles de depurar porque la interfaz oculta algunos mensajes de error. Por esta razón, a pesar de tomar el cuidado necesario en su escritura, puede quedarse atascado en una pantalla sin poder cancelar. Esto puede forzarlo a cancelar una sesión SSH o matar el proceso zombie.\n\nIMPORTANTE: ¡Las acciones a realizar a partir de este momento, no son reversibles!\n\n¿Desea continuar?"
- MSG_KEY_TO_CONTINUE="Presione cualquier tecla para continuar... "

Sección: environment

- ENVMT_1="PRODUCCION"
- ENVMT_2="TESTING"
- ENVMT_3="demo"
- ENVMT_4="validacion"

Sección: template

- TEMPLATE_ROOT_CA="root-ca.cnf"

Sección: caroot

- CA_ACRONYM_DEFAULT="CA-CECBA"
- CA_PREFIX=""
- CA_MSK="CA-root"

- CA_DAYS_FILE="caDays.conf"
- CA_MD_FILE="caMD.conf"
- CA_BITS_FILE="caBits.conf"
- CA_DAYS_ON_DEFAULT_LIST="3653"
- CA_DAYS_ON_DEFAULT_CRL="30"
- CA_MD_ON_DEFAULT="sha256"
- CA_BITS_ON_DEFAULT="2048"
- CA_COUNTRY_NAME_DEFAULT="AR"
- CA_STATE_OR_PROVINCE_NAME_DEFAULT="CABA"
- CA_LOCALITY_NAME_DEFAULT="CABA"
- CA_ORGANIZATION_NAME_DEFAULT="Colegio de Escribanos de la Ciudad de Buenos Aires"
- CA_COMMON_NAME_DEFAULT="CA - Colegio de Escribanos de la CABA"
- CA_ORGANIZATIONAL_UNIT_NAME_DEFAULT="Cómputos, Operaciones"
- CA_EMAIL_ADDRESS_DEFAULT="pki@colegio-escribanos.org.ar"
- CA_POSTAL_ADDRESS_DEFAULT="Las Heras 1833, C1127AAA"
- CA_URI_CRL_DEFAULT="https://pki.colegio-escribanos.org.ar/queCRL"
- CA_URI_OCSP_CRT_DEFAULT="https://ocsp.colegio-escribanos.org.ar/ocsp.crt"
- CA_URI_OCSP_DEFAULT="https://ocsp.colegio-escribanos.org.ar"
- CA_SERIAL_NUMBER="0100"
- CA_FILENAME_KEY_SSH_REMOTE="id_rsa"
- CA_FILENAME_KEY_SSH_REMOTE_HOST="SSH_host.conf"

Sección: subcaroot

- SUB_CA_CORE_PATH="/root/scripts/centralizerCert/SUBCA_core"
- SUB_CA_INSTALL_PATH="/root/scripts/centralizerCert_SUBCA"
- SUB_CA_GLOBAL_CERT=""
- SUB_CA_PREFIX=""
- SUB_CA_MSK="SubCA-root"
- SUB_CA_TIME_OUT_CONNECT="2"

4.2. Ampliación de Templates SSL

Los templates SSL [21] son imprescindibles, dado que por su diseño permiten una rápida y dinámica implementación en muy corto tiempo. Por

ello, se incluyen a continuación, los restantes a fin de poder ampliar y conocer los mismos.

4.2.1. cC Sub-CA | RA – Humano

A continuación, se detalla el template SSL [22] de tipo Humano para cualquier tipo de emisión:

- `HOME = .`
- `RANDFILE = $ENV::HOME/.rnd`
- `oid_section = new_oids`
- `[new_oids]`
  - `postalAddress = 2.5.4.16`
  - `serialNumber = 2.5.4.5`
  - `dateOfBirth = 1.3.6.1.5.5.7.9.1`
  - `countryOfCitizenship = 1.3.6.1.5.5.7.9.4`
- `[ ca ]`
  - `default_ca = CA_default`
- `[ CA_default ]`
  - `dir = .`
  - `certs = $dir/certs`
  - `crl_dir = $dir/crl`
  - `new_certs_dir = $dir/newcerts`
  - `database = $dir/index.db`
  - `serial = $dir/serial`
  - `RANDFILE = $dir/private/.rand`
  - `private_key = $dir/private/persona.key.pem`
  - `certificate = $dir/certs/persona.cert.pem`
  - `default_md = sha384`
  - `name_opt = ca_default`
  - `cert_opt = ca_default`
  - `default_days = 732`
  - `preserve = no`
  - `policy = policy_match`
- `[ policy_match ]`
  - `countryName = match`
  - `stateOrProvinceName = match`
  - `organizationName = match`
  - `organizationalUnitName = optional`
  - `commonName = supplied`
  - `emailAddress = match`

- postalAddress = match
- serialNumber = match
- dateOfBirth = optional
- countryOfCitizenship = optional

- [req]
  - default_bits = 4096
  - distinguished_name = req_distinguished_name
  - string_mask = utf8only
  - default_md = sha384
  - x509_extensions = usr_cert_human_point_has_san
- [req_distinguished_name]
  - countryName = Pais (Codigo de 2 letras ISO 3166)
  - stateOrProvinceName = Provincia
  - localityName = Localidad
  - 0.organizationName = Nombre de la Organización
  - organizationalUnitName = Tipo de certificado
  - commonName = Nombre completo (como figura en el DNI o DNU)
  - emailAddress = Email
  - postalAddress = Direccion
  - serialNumber = Número de DNI o DNU (sin puntos)
  - dateOfBirth = Fecha de nacimiento
  - countryOfCitizenship = Nacionalidad
  - countryName_default = AR
  - stateOrProvinceName_default = CABA
  - localityName_default = CABA
  - 0.organizationName_default = Organización
  - organizationalUnitName_default = Humano
  - emailAddress_default = correo
  - postalAddress_default = Dirección
  - countryOfCitizenship_default = Argentino
- [usr_cert_human_point_has_san]
  - basicConstraints = CA:FALSE
  - nsCertType = client
  - nsComment = "HUMAN client Certificate to centralizerCert"
  - subjectKeyIdentifier = hash
  - authorityKeyIdentifier = keyid,issuer
  - keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
  - extendedKeyUsage = clientAuth

4.2.2. cC Sub-CA | RA – Servidor

A continuación, se detalla el template SSL [23] de tipo Servidor:

- HOME = .
- RANDFILE = $ENV::HOME/.rnd
- oid_section = new_oids
- [new_oids]
  - postalAddress = 2.5.4.16
- [ca]
  - default_ca = CA_default
- [CA_default]
  - dir = .
  - certs = $dir/certs
  - crl_dir = $dir/crl
  - new_certs_dir = $dir/newcerts
  - unique_subject = no
  - database = $dir/index.db
  - serial = $dir/serial
  - RANDFILE = $dir/private/.rand
  - private_key = $dir/private/server.key.pem
  - certificate = $dir/certs/server.cert.crt.pem
  - default_md = sha384
  - name_opt = ca_default
  - cert_opt = ca_default
  - default_days = 1095
  - preserve = no
  - policy = policy_loose
- [policy_strict]
  - countryName = match
  - stateOrProvinceName = match
  - organizationName = match
  - organizationalUnitName = optional
  - commonName = supplied
  - emailAddress = optional
  - postalAddress = optional
- [policy_loose]
  - countryName = optional
  - stateOrProvinceName = optional
  - localityName = optional
  - organizationName = optional

- organizationalUnitName = optional
- commonName = supplied
- emailAddress = optional
- postalAddress = optional

- [req]
  - default_bits = 4096
  - distinguished_name = req_distinguished_name
  - string_mask = utf8only
  - default_md = sha384
  - x509_extensions = server_cert_has_san
- [req_distinguished_name]
  - countryName_min = 2
  - countryName_max = 2
  - countryName = Pais (Codigo de 2 letras ISO 3166)
  - stateOrProvinceName = Provincia
  - localityName = Localidad
  - 0.organizationName = Nombre de la Organizacion
  - organizationalUnitName = Tipo de certificado
  - commonName = Nombre del Servidor (url)
  - emailAddress = Email
  - postalAddress = Direccion
  - countryName_min = 2
  - countryName_max = 2
  - countryName_default = AR
  - stateOrProvinceName_default = CABA
  - localityName_default = CABA
  - 0.organizationName_default = Colegio de Escribanos de la Ciudad de Buenos Aires
  - commonName_default = *.colegio-escribanos.org.ar
  - organizationalUnitName_default = Servidor
  - emailAddress_default = pki@colegio-escribanos.org.ar
  - postalAddress_default = Las Heras 1833, C1127AAA
- [server_cert_has_san]
  - basicConstraints = CA:FALSE
  - nsCertType = server
  - nsComment = "Server Certificate to centralizerCert"
  - subjectKeyIdentifier = hash
  - authorityKeyIdentifier = keyid,issuer:always
  - keyUsage = critical, digitalSignature, keyEncipherment
  - extendedKeyUsage = serverAuth

4.2.3. cC Sub-CA | RA – Monitoreo

A continuación, se detalla el templates SSL de tipo Monitoreo:

- HOME = .
- RANDFILE = $ENV::HOME/.rnd
- oid_section = new_oids
- [new_oids]
    - postalAddress = 2.5.4.16
- [ca]
    - default_ca = CA_default
- [CA_default]
    - dir = .
    - certs = $dir/certs
    - crl_dir = $dir/crl
    - new_certs_dir = $dir/newcerts
    - unique_subject = no
    - database = $dir/index.db
    - serial = $dir/serial
    - RANDFILE = $dir/private/.rand
    - private_key = $dir/private/monitoreo.key.pem
    - certificate = $dir/certs/monitoreo.cert.crt.pem
    - default_md = sha384
    - name_opt = ca_default
    - cert_opt = ca_default
    - default_days = 1095
    - preserve = no
    - policy = policy_loose
- [policy_strict]
    - countryName = match
    - stateOrProvinceName = match
    - organizationName = match
    - organizationalUnitName = optional
    - commonName = supplied
    - postalAddress = optional
- [policy_loose]
    - countryName = optional
    - stateOrProvinceName = optional
    - localityName = optional
    - organizationName = optional
    - organizationalUnitName = optional

    - commonName = supplied
    - postalAddress = optional
- [req]
    - default_bits = 4096
    - distinguished_name = req_distinguished_name
    - string_mask = utf8only
    - default_md = sha384
    - x509_extensions = monitoreo_cert_has_san
- [req_distinguished_name]
    - countryName = Pais (Codigo de 2 letras ISO 3166)
    - stateOrProvinceName = Provincia
    - localityName = Localidad
    - 0.organizationName = Nombre de la Organizacion
    - organizationalUnitName = Tipo de certificado
    - commonName = Nombre del servicio de monitoreo
    - postalAddress = Direccion
    - countryName_min = 2
    - countryName_max = 2
    - countryName_default = AR
    - stateOrProvinceName_default = CABA
    - localityName_default = CABA
    - 0.organizationName_max = 70
    - 0.organizationName_default = Colegio de Escribanos de la Ciudad de Buenos Aires
    - commonName_max = 80
    - commonName_default = Servicio de Monitoreo de SSL Web
    - organizationalUnitName_default = Monitoreo
    - postalAddress_default = Las Heras 1833, C1127AAA
- [monitoreo_cert_has_san]
    - basicConstraints = CA:FALSE
    - nsCertType = client
    - nsComment = "Monitoring Certificate to centralizerCert"
    - subjectKeyIdentifier = hash
    - authorityKeyIdentifier = keyid,issuer:always
    - keyUsage = critical, digitalSignature, keyEncipherment
    - extendedKeyUsage = clientAuth

4.2.4. cC Sub-CA | RA

A continuación, se detalla el template SSL [24] de tipo Sub-CA:

- HOME = .
- RANDFILE = $ENV::HOME/.rnd
- oid_section = new_oids
- [new_oids]
    - postalAddress = 2.5.4.16
- [ca]
    - default_ca = CA_default
- [CA_default]
    - dir = .
    - certs = $dir/certs
    - crl_dir = $dir/crl
    - new_certs_dir = $dir/newcerts
    - unique_subject = no
    - database = $dir/index.db
    - serial = $dir/serial
    - RANDFILE = $dir/private/.rand
    - private_key = $dir/private/subca.key.pem
    - certificate = $dir/certs/subca.cert.crt.pem
    - crlnumber = $dir/crlnumber
    - crl = $dir/crl/subca.crl
    - crl_extensions = crl_ext
    - default_crl_days = 60
    - default_md = sha384
    - name_opt = ca_default
    - cert_opt = ca_default
    - default_days = 3653
    - preserve = no
    - policy = policy_loose
- [policy_strict]
    - countryName = match
    - stateOrProvinceName = match
    - organizationName = match
    - organizationalUnitName = optional
    - commonName = supplied
    - emailAddress = optional
    - postalAddress = optional
- [policy_loose]
    - countryName = optional
    - stateOrProvinceName = optional
    - localityName = optional

- organizationName = optional
- organizationalUnitName = optional
- commonName = supplied
- emailAddress = optional
- postalAddress = optional

- [req]
  - default_bits = 4096
  - distinguished_name = req_distinguished_name
  - string_mask = utf8only
  - default_md = sha384
  - x509_extensions = v3_sub_ca_has_san
- [req_distinguished_name]
  - countryName = Pais (Codigo de 2 letras ISO 3166)
  - stateOrProvinceName = Provincia
  - localityName = Localidad
  - 0.organizationName = Nombre de la Organizacion
  - organizationalUnitName = Departamento
  - commonName = Nombre
  - emailAddress = Email
  - postalAddress = Direccion
  - countryName_min = 2
  - countryName_max = 2
  - countryName_default = AR
  - stateOrProvinceName_default = CABA
  - localityName_default = CABA
  - 0.organizationName_max = 70
  - 0.organizationName_default = Colegio de Escribanos de la Ciudad de Buenos Aires
  - commonName_max = 80
  - commonName_default = SubCA | nombre de SERVICIO SUB-CA
  - organizationalUnitName_default = Computos, Operaciones
  - emailAddress_max = 64
  - emailAddress_default = pki@colegio-escribanos.org.ar
  - postalAddress_default = Las Heras 1833, C1127AAA
- [v3_sub_ca_has_san]
  - basicConstraints = critical,CA:FALSE
  - subjectKeyIdentifier = hash
  - authorityKeyIdentifier = keyid:always,issuer
  - keyUsage = critical, digitalSignature, keyEncipherment, cRLSign, keyCertSign
  - extendedKeyUsage = serverAuth

- crlDistributionPoints = @crl_section
- subjectAltName = @alt_names
- authorityInfoAccess = @ocsp_section
- subjectAltName = email:move

- [crl_ext]
  - issuerAltName = issuer:copy
  - authorityKeyIdentifier = keyid:always
- [alt_names]
  - DNS.0 = CECBA Intermidiate CA 1
  - DNS.1 = CECBA CA Intermidiate 1
- [crl_section]
  - URI.0 = http://pki-crl.colegio-escribanos.org.ar/cecba.crl
  - URI.1 = http://pki-alternative-crl.colegio-escribanos.org.ar/cecba.crl
- [ocsp_section]
  - caIssuers;URI.0 = http://pki-ocsp.colegio-escribanos.org.ar/cecba.crt
  - caIssuers;URI.1 = http://pki-alternative-ocsp.colegio-escribanos.org.ar/cecba.crt
  - OCSP;URI.0 = http://pki-ocsp.colegio-escribanos.org.ar/ocsp/
  - OCSP;URI.1 = http://pki-alternative-ocsp.colegio-escribanos.org.ar/ocsp/
- [ocsp]
  - basicConstraints = CA:FALSE
  - subjectKeyIdentifier = hash
  - authorityKeyIdentifier = keyid,issuer
  - keyUsage = critical, digitalSignature
  - extendedKeyUsage = critical, OCSPSigning
- [person]
  - basicConstraints = CA:FALSE
  - nsCertType = client, email
  - nsComment = "Certificado CLIENTE PERSONAL CCSSL"
  - subjectKeyIdentifier = hash
  - authorityKeyIdentifier = keyid:always, issuer:always
  - keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
  - extendedKeyUsage = critical, clientAuth, emailProtection
  - authorityInfoAccess = @ocsp_section

    - crlDistributionPoints = @crl_section
- [point]
    - basicConstraints = CA:FALSE
    - nsCertType = client, email
    - nsComment = "Certificado CLIENTE PUESTO CCSSL"
    - subjectKeyIdentifier = hash
    - authorityKeyIdentifier = keyid:always, issuer:always
    - keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
    - extendedKeyUsage = critical, clientAuth
    - authorityInfoAccess = @ocsp_section
    - crlDistributionPoints = @crl_section
- [monitor]
    - basicConstraints = CA:FALSE
    - nsCertType = client
    - nsComment = "Certificado MONITOREO CCSSL"
    - subjectKeyIdentifier = hash
    - authorityKeyIdentifier = keyid:always, issuer:always
    - keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
    - extendedKeyUsage = critical, clientAuth
    - authorityInfoAccess = @ocsp_section
    - crlDistributionPoints = @crl_section
- [server]
    - basicConstraints = critical, CA:FALSE
    - nsCertType = server
    - nsComment = "Certificado SERVIDOR CCSSL"
    - subjectKeyIdentifier = hash
    - authorityKeyIdentifier = keyid,issuer:always
    - keyUsage = critical, digitalSignature, keyEncipherment, keyAgreement, nonRepudiation
    - extendedKeyUsage = critical, serverAuth
    - authorityInfoAccess = @ocsp_section
    - crlDistributionPoints = @crl_section
    - subjectAltName = @alt_names

4.2.5. cC CA

A continuación, se detalla el template SSL [25] de tipo CA:

- HOME = .
- RANDFILE = $ENV::HOME/.rnd
- oid_section = new_oids
- [new_oids]
    - postalAddress = 2.5.4.16
- [ca]
    - default_ca = CA_default
- [CA_default]
    - dir = .
    - certs = $dir/certs
    - crl_dir   = $dir/crl
    - new_certs_dir = $dir/newcerts
    - unique_subject = yes
    - database = $dir/index.db
    - serial = $dir/serial
    - RANDFILE = $dir/private/.rand
    - private_key = $dir/private/ca.key.pem
    - certificate = $dir/certs/ca.cert.crt.pem
    - crlnumber = $dir/crlnumber
    - crl = $dir/crl/ca.crl
    - crl_extensions = crl_ext
    - default_crl_days = 30
    - default_md = sha384
    - name_opt = ca_default
    - cert_opt = ca_default
    - default_days = 6570
    - preserve = no
    - policy = policy_strict
- [policy_strict]
    - countryName = match
    - stateOrProvinceName = match
    - organizationName = match
    - organizationalUnitName = optional
    - commonName = supplied
    - emailAddress = optional
    - postalAddress = optional
- [req]
    - default_bits = 4096
    - distinguished_name = req_distinguished_name
    - string_mask = utf8only

    - default_md = sha384
    - x509_extensions = v3_ca
- [req_distinguished_name]
    - countryName = Pais (Codigo de 2 letras ISO 3166)
    - stateOrProvinceName = Provincia
    - localityName = Localidad
    - 0.organizationName = Nombre de la Organizacion
    - organizationalUnitName = Departamento
    - commonName = Nombre
    - emailAddress = Email
    - postalAddress = Direccion
    - countryName_min = 2
    - countryName_max = 2
    - countryName_default = AR
    - stateOrProvinceName_default = CABA
    - localityName_default = CABA
    - 0.organizationName_default = Colegio de Escribanos de la Ciudad de Buenos Aires
    - commonName_default = CA - CECBA
    - organizationalUnitName_default = Computos, Operaciones
    - emailAddress_default = pki@colegio-escribanos.org.ar
    - postalAddress_default = Las Heras 1833, C1127AAA
- [v3_ca_has_san]
    - subjectKeyIdentifier = hash
    - authorityKeyIdentifier = keyid:always,issuer
    - basicConstraints = critical, CA:true
    - keyUsage = critical, digitalSignature, cRLSign, keyCertSign
    - subjectAltName = email:move
- [v3_sub_ca_has_san]
    - basicConstraints = critical,CA:TRUE,pathlen:0
    - subjectKeyIdentifier = hash
    - authorityKeyIdentifier = keyid:always,issuer
    - keyUsage = critical, digitalSignature, keyEncipherment, cRLSign, keyCertSign
    - subjectAltName = email:move

4.3. Tipos de uso de claves públicas

La entrada Extended Key Usage [16], permite realizar los siguientes usos con un certificado:

Uso	Detalle
serverAuth	Autenticación de servidor web
clientAuth	Autenticación de cliente web
codeSigning	Firma de código
emailProtection	Protección de correo electrónico
timeStamping	Estampado de tiempo
OCSPSigning	OCSP
ipsecIKE	ipsec Internet Key Exchange
msCodeInd	Firma de código individual Microsoft
msCodeCom	Firma de código comercial Microsoft
msCTLSign	Firma de lista de confianza Microsoft
msEFS	Sistema de archivos cifrado Microsoft

Tabla 7. Tipos de uso de claves publicas SSL

5. Índices específicos

5.1. Índice de Figuras

Figura 1. Estructura X.509 versión 3 de Certificados Digitales [] 6
Figura 2. Detalle X.509 de Certificados Digitales [] 7
Figura 3. Logotipo de cC 9
Figura 4. Diagrama en bloques de arquitectura cC 9
Figura 5. Diagrama de flujo general de CA 10
Figura 6. Diagrama de flujo general de clave de conexión de CA 11
Figura 7. Diagrama de flujo general de vinculo CA – Sub-CA | RA 11
Figura 8. Diagrama de flujo general de despliegue de core desde CA 12
Figura 9. Diagrama de flujo general de despliegue de CA desde CA 12
Figura 10. Diagrama de flujo general de RA 13
Figura 11. Ejemplo de búsqueda y reemplazo en template SSL 17
Figura 12. Paso 1 – Instalación de cC CA 19
Figura 13. Paso 2 – Instalación de cC CA 19
Figura 14. Paso 3 – Instalación de cC CA 20
Figura 15. Paso 1 – Pre requisitos de cC CA 20
Figura 16. Paso 2 – Pre requisitos de cC CA 20
Figura 17. Paso 3 – Pre requisitos de cC CA 20
Figura 18. Paso 1 – Inicio de cC CA 21
Figura 19. Paso 2 – Inicio de cC CA 21
Figura 20. Paso 3 – Inicio de cC CA 21
Figura 21. Paso 1 – Configuración global pre existente cC CA 21
Figura 22. Paso 1 – Configuración global pre existente cC CA 22
Figura 23. Paso 3 – Configuración global pre existente cC CA 22
Figura 24. Paso 4 – Configuración global pre existente cC CA 22
Figura 25. Paso 5 – Configuración global pre existente cC CA 23
Figura 26. Paso 1 – Log cC CA 23
Figura 27. Paso 2 – Log cC CA 24
Figura 28. Paso 1 – Creación de CA 24
Figura 29. Paso 2 – Creación de CA 24
Figura 30. Paso 3 – Creación de CA 24
Figura 31. Paso 4 – Creación de CA 25
Figura 32. Paso 5 – Creación de CA 25
Figura 33. Paso 6 – Creación de CA 25
Figura 34. Paso 7 – Creación de CA 25
Figura 35. Paso 8 – Creación de CA 25
Figura 36. Paso 9 – Creación de CA 25
Figura 37. Paso 10 – Creación de CA 26
Figura 38. Paso 11 – Creación de CA 26
Figura 39. Paso 12 – Creación de CA 26
Figura 40. Paso 13 – Creación de CA 26
Figura 41. Paso 14 – Creación de CA 26
Figura 42. Paso 15 – Creación de CA 26
Figura 43. Paso 16 – Creación de CA 27
Figura 44. Paso 17 – Creación de CA 27
Figura 45. Paso 18 – Creación de CA 27
Figura 46. Paso 19 – Creación de CA 27
Figura 47. Paso 20 – Creación de CA 27
Figura 48. Paso 21 – Creación de CA 28
Figura 49. Paso 22 – Creación de CA 28
Figura 50. Paso 23 – Creación de CA 28
Figura 51. Paso 24 – Creación de CA 28

Figura 52. Paso 25 – Creación de CA 29
Figura 53. Paso 26 – Creación de CA 29
Figura 54. Paso 1 – Ver configuración SSL de CA 29
Figura 55. Paso 2 – SSL de CA 30
Figura 56. Paso 3 – SSL de CA 30
Figura 57. Paso 4 – SSL de CA 30
Figura 58. Paso 5 – SSL de CA 30
Figura 59. Paso 1 – Creación de clave de cC CA 31
Figura 60. Paso 2 – Creación de clave cC CA 31
Figura 61. Paso 3 – Creación de clave cC CA 31
Figura 62. Paso 4 – Creación de clave cC CA 31
Figura 63. Paso 1 – Denuncia de vinculo remoto desde cC CA 32
Figura 64. Paso 2 – Denuncia de vinculo remoto desde cC CA 32
Figura 65. Paso 3 – Denuncia de vinculo remoto desde cC CA 32
Figura 66. Paso 4 – Denuncia de vinculo remoto desde cC CA 32
Figura 67. Paso 5 – Denuncia de vinculo remoto desde cC CA 32
Figura 68. Paso 6 – Denuncia de vinculo remoto desde cC CA 32
Figura 69. Paso 7 – Denuncia de vinculo remoto desde cC CA 33
Figura 70. Paso 8 – Denuncia de vinculo remoto desde cC CA 33
Figura 71. Paso 9 – Denuncia de vinculo remoto desde cC CA 33
Figura 72. Paso 10 – Denuncia de vinculo remoto desde cC CA 33
Figura 73. Paso 11A – Denuncia de vinculo remoto desde cC CA 33
Figura 74. Paso 11B – Denuncia de vinculo remoto desde cC CA 33
Figura 75. Paso 12 – Denuncia de vinculo remoto desde cC CA 34
Figura 76. Paso 13 – Denuncia de vinculo remoto desde cC CA 34
Figura 77. Paso 14 – Denuncia de vinculo remoto desde cC CA 34
Figura 78. Paso 15 – Denuncia de vinculo remoto desde cC CA 34
Figura 79. Paso 1 – Despliegue de core cC Sub-CA | RA desde cC CA 34
Figura 80. Paso 2 – Despliegue de core cC Sub-CA | RA desde cC CA 35
Figura 81. Paso 3 – Despliegue de core cC Sub-CA | RA desde cC CA 35
Figura 82. Paso 4 – Despliegue de core cC Sub-CA | RA desde cC CA 35
Figura 83. Paso 1 – Despliegue de CA base hacia cC Sub-CA | RA 35
Figura 84. Paso 2 – Despliegue de CA base hacia cC Sub-CA | RA 35
Figura 85. Paso 3 – Despliegue de CA base hacia cC Sub-CA | RA 36
Figura 86. Paso 4 – Despliegue de CA base hacia cC Sub-CA | RA 36
Figura 87. Paso 5 – Despliegue de CA base hacia cC Sub-CA | RA 36
Figura 88. Paso 6 – Despliegue de CA base hacia cC Sub-CA | RA 36
Figura 89. Paso 7 – Despliegue de CA base hacia cC Sub-CA | RA 36
Figura 90. Paso 8 – Despliegue de CA base hacia cC Sub-CA | RA 36
Figura 91. Paso 9 – Despliegue de CA base hacia cC Sub-CA | RA 37
Figura 92. Paso 1 – Salir de cC CA 37
Figura 93. Paso 2 – Salir de cC CA 37
Figura 94. Paso 3 – Salir de cC CA 37
Figura 95. Paso 1 – Pre requisitos de cC Sub-CA 38
Figura 96. Paso 2 – Pre requisitos de cC Sub-CA 38
Figura 97. Paso 3 – Pre requisitos de cC Sub-CA 38
Figura 98. Paso 4 – Pre requisitos de cC Sub-CA 38
Figura 99. Paso 1 – Inicio de cC Sub-CA | RA 39
Figura 100. Paso 2 – Inicio de cC Sub-CA | RA 39
Figura 101. Paso 3 – Inicio de cC Sub-CA | RA 39
Figura 102. Paso 1 – Configuración global pre existente cC Sub-CA | RA 39
Figura 103. Paso 2 – Configuración global pre existente cC Sub-CA | RA 40
Figura 104. Paso 3 – Configuración global pre existente cC Sub-CA | RA 40
Figura 105. Paso 4 – Configuración global pre existente cC Sub-CA | RA 40
Figura 106. Paso 5 – Configuración global pre existente cC Sub-CA | RA 41
Figura 107. Paso 6 – Configuración global pre existente cC Sub-CA | RA 41

Figura 108. Paso 7 – Configuración global pre existente cC Sub-CA | RA 41
Figura 109. Paso 1 – Configurar base de datos de la RA 42
Figura 110. Paso 2 – Configurar base de datos de la RA 42
Figura 111. Paso 3 – Configurar base de datos de la RA 42
Figura 112. Paso 4 – Configurar base de datos de la RA 42
Figura 113. Paso 1 – Configurar correo electrónico de la RA 43
Figura 114. Paso 2 – Configurar correo electrónico de la RA 43
Figura 115. Paso 3 – Configurar correo electrónico de la RA 43
Figura 116. Paso 4 – Configurar correo electrónico de la RA 43
Figura 117. Paso 1 – Configurar servidor web de la RA 44
Figura 118. Paso 2 – Configurar servidor web de la RA 44
Figura 119. Paso 3 – Configurar servidor web de la RA 44
Figura 120. Paso 4 – Configurar servidor web de la RA 44
Figura 121. Paso 1 – Configuraciones generales cC Sub-CA | RA..... 45
Figura 122. Paso 2 – Configuraciones generales cC Sub-CA | RA..... 45
Figura 123. Paso 3 – Configuraciones generales cC Sub-CA | RA..... 45
Figura 124. Paso 4 – Configuraciones generales cC Sub-CA | RA..... 45
Figura 125. Paso 5 – Configuraciones generales cC Sub-CA | RA..... 45
Figura 126. Paso 6 – Configuraciones generales cC Sub-CA | RA..... 46
Figura 127. Paso 1 – Servidor web cC Sub-CA | RA – Registro de usuario 46
Figura 128. Paso 2 – Servidor web cC Sub-CA | RA – Registro de usuario 47
Figura 129. Paso 3 – Servidor web cC Sub-CA | RA – Registro de usuario 47
Figura 130. Paso 4 – Servidor web cC Sub-CA | RA – Recepcion de correo de registro 48
Figura 131. Paso 5 – Servidor web cC Sub-CA | RA – Activación de cuenta con enlace..... 48
Figura 132. Paso 6 – Servidor web cC Sub-CA | RA – Acceso usuario sin privilegios 49
Figura 133. Paso 7 – Servidor web cC Sub-CA | RA – Acceso usuario administrador..... 49
Figura 134. Paso 8 – Servidor web cC Sub-CA | RA – Acerca de cC..... 50
Figura 135. Paso 9 – Servidor web cC Sub-CA | RA - Usuarios 50
Figura 136. Paso 10 – Servidor web cC Sub-CA | RA - Usuario Administrador 51
Figura 137. Paso 1 – Consulta de CA's disponibles desde RA..... 51
Figura 138. Paso 2 – Consulta de CA's disponibles desde RA..... 52
Figura 139. Paso 3 – Consulta de CA's disponibles desde RA..... 52
Figura 140. Paso 4 – Consulta de CA's disponibles desde RA..... 52
Figura 141. Paso 5A – Consulta de CA's disponibles desde RA 52
Figura 142. Paso 5B – Consulta de CA's disponibles desde RA 52
Figura 143. Paso 6 – Consulta de CA's disponibles desde RA..... 53
Figura 144. Paso 1 – Creación de Sub-CA..... 53
Figura 145. Paso 2 – Creación de Sub-CA..... 53
Figura 146. Paso 3 – Creación de Sub-CA..... 53
Figura 147. Paso 4 – Creación de Sub-CA..... 54
Figura 148. Paso 5 – Creación de Sub-CA..... 54
Figura 149. Paso 6 – Creación de Sub-CA..... 54
Figura 150. Paso 7 – Creación de Sub-CA..... 54
Figura 151. Paso 8 – Creación de Sub-CA..... 54
Figura 152. Paso 9 – Creación de Sub-CA..... 54
Figura 153. Paso 10 – Creación de Sub-CA..... 55
Figura 154. Paso 11 – Creación de Sub-CA..... 55
Figura 155. Paso 12 – Creación de Sub-CA..... 55
Figura 156. Paso 13 – Creación de Sub-CA..... 55
Figura 157. Paso 14 – Creación de Sub-CA..... 55
Figura 158. Paso 15 – Creación de Sub-CA..... 55
Figura 159. Paso 16 – Creación de Sub-CA..... 56
Figura 160. Paso 17 – Creación de Sub-CA..... 56
Figura 161. Paso 18 – Creación de Sub-CA..... 56
Figura 162. Paso 19 – Creación de Sub-CA..... 56
Figura 163. Paso 20 – Creación de Sub-CA..... 56

Figura 164. Paso 21 – Creación de Sub-CA 56
Figura 165. Paso 22 – Creación de Sub-CA 56
Figura 166. Paso 23 – Creación de Sub-CA 57
Figura 167. Paso 24 – Creación de Sub-CA 57
Figura 168. Paso 25 – Creación de Sub-CA 57
Figura 169. Paso 26 – Creación de Sub-CA 57
Figura 170. Paso 27 – Creación de Sub-CA 57
Figura 171. Paso 28 – Creación de Sub-CA 58
Figura 172. Paso 29 – Creación de Sub-CA 58
Figura 173. Paso 30 – Creación de Sub-CA 58
Figura 174. Paso 31 – Creación de Sub-CA 59
Figura 175. Mecánica de cC Sub-CA | RA 59
Figura 176. Paso 1 – Ver configuración SSL de Sub-CA 60
Figura 177. Paso 2 – Ver configuración SSL de Sub-CA 60
Figura 178. Paso 3 – Ver configuración SSL de Sub-CA 60
Figura 179. Paso 4 – Ver configuración SSL de Sub-CA 60
Figura 180. Paso 5 – SSL de Sub-CA 61
Figura 181. Paso 6 – SSL de Sub-CA 61
Figura 182. Paso 7 – SSL de Sub-CA 61
Figura 183. Paso 8 – SSL de Sub-CA 61
Figura 184. Paso 9 – SSL de Sub-CA 61
Figura 185. Paso 10 – SSL de Sub-CA 61
Figura 186. Paso 11 – Ver configuración SSL de Sub-CA 62
Figura 187. Paso 1 – BD plana SSL de Sub-CA 62
Figura 188. Paso 2 – BD plana SSL de Sub-CA 62
Figura 189. Paso 1 – Resguardo de BD de Sub-CA 62
Figura 190. Paso 2 – Resguardo de BD a demanda de Sub-CA 63
Figura 191. Paso 3 – Resguardo de BD a demanda de Sub-CA 63
Figura 192. Paso 4 – Resguardo de BD a demanda de Sub-CA 63
Figura 193. Paso 5 – Resguardo de BD programado de Sub-CA 63
Figura 194. Paso 6 – Resguardo de BD programado de Sub-CA 63
Figura 195. Paso 6 – Resguardo de BD programado de Sub-CA 63
Figura 196. Paso 1 – Consulta de CRL de Sub-CA 64
Figura 197. Paso 2 – Consulta de CRL de Sub-CA 64
Figura 198. Paso 1 – Re carga de CRL de Sub-CA 64
Figura 199. Paso 2 – Re carga de CRL de Sub-CA 64
Figura 200. Paso 3 – Re carga de CRL de Sub-CA 65
Figura 201. Paso 4 – Re carga de CRL de Sub-CA 65
Figura 202. Paso 5 – Re carga de CRL de Sub-CA 65
Figura 203. Paso 6 – Re carga de CRL de Sub-CA 65
Figura 204. Paso 7 – Re carga de CRL de Sub-CA 65
Figura 205. Paso 8 – Re carga de CRL de Sub-CA 65
Figura 206. Paso 9 – Re carga de CRL de Sub-CA 66
Figura 207. Paso 10 – Re carga de CRL de Sub-CA 66
Figura 208. Paso 11 – Re carga de CRL de Sub-CA 66
Figura 209. Paso 12 – Re carga de CRL de Sub-CA 67
Figura 210. Paso 12 – Re carga de CRL de Sub-CA 67
Figura 211. Gestión de Certificados cliente 68
Figura 212. Paso 1 – Consulta de certificados cliente 68
Figura 213. Paso 2 – Consulta de certificados cliente 68
Figura 214. Paso 3 – Consulta de certificados cliente 68
Figura 215. Paso 1 – Revocar certificados cliente 69
Figura 216. Paso 2 – Revocar certificados cliente 69
Figura 217. Paso 3 – Revocar certificados cliente 69
Figura 218. Paso 4 – Revocar certificados cliente 69
Figura 219. Nuevo certificado cliente por tipo 70

Figura 220. Paso 1 – Crear certificado cliente humano manual 70
Figura 221. Paso 2 – Crear certificado cliente humano manual 71
Figura 222. Paso 3 – Crear certificado cliente humano manual 71
Figura 223. Paso 4 – Crear certificado cliente humano manual 71
Figura 224. Paso 5 – Crear certificado cliente humano manual 71
Figura 225. Paso 6 – Crear certificado cliente humano manual 71
Figura 226. Paso 7 – Crear certificado cliente humano manual 72
Figura 227. Paso 8 – Crear certificado cliente humano manual 72
Figura 228. Paso 9 – Crear certificado cliente humano manual 72
Figura 229. Paso 10 – Crear certificado cliente humano manual 72
Figura 230. Paso 11 – Crear certificado cliente humano manual 72
Figura 231. Paso 12 – Crear certificado cliente humano manual 72
Figura 232. Paso 13 – Crear certificado cliente humano manual 72
Figura 233. Paso 14 – Crear certificado cliente humano manual 73
Figura 234. Paso 15 – Crear certificado cliente humano manual 73
Figura 235. Paso 16 – Crear certificado cliente humano manual 73
Figura 236. Paso 17 – Crear certificado cliente humano manual 73
Figura 237. Paso 18 – Crear certificado cliente humano manual 73
Figura 238. Paso 19 – Crear certificado cliente humano manual 73
Figura 239. Paso 20 – Crear certificado cliente humano manual 73
Figura 240. Paso 21 – Crear certificado cliente humano manual 74
Figura 241. Paso 22 – Crear certificado cliente humano manual 74
Figura 242. Paso 1 – Revocar certificado cliente humano manual 75
Figura 243. Paso 2 – Revocar certificado cliente humano manual 75
Figura 244. Paso 3 – Revocar certificado cliente humano manual 75
Figura 245. Paso 4 – Revocar certificado cliente humano manual 75
Figura 246. Paso 5 – Revocar certificado cliente humano manual 75
Figura 247. Paso 6 – Revocar certificado cliente humano manual 75
Figura 248. Paso 7 – Revocar certificado cliente humano manual 76
Figura 249. Paso 8 – Revocar certificado cliente humano manual 76
Figura 250. Paso 9 – Revocar certificado cliente humano manual 76
Figura 251. Paso 10 – Revocar certificado cliente humano manual 76
Figura 252. Paso 11 – Revocar certificado cliente humano manual 76
Figura 253. Paso 12 – Revocar certificado cliente humano manual 77
Figura 254. Paso 13 – Revocar certificado cliente humano manual 77
Figura 255. Paso 14 – Revocar certificado cliente humano manual 77
Figura 256. Paso 15 – Revocar certificado cliente humano manual 78
Figura 257. Paso 16 – Revocar certificado cliente humano manual 78
Figura 258. Paso 1 – Re carga de CRL con certificados revocados incluidos 79
Figura 259. Paso 2 – Re carga de CRL con certificados revocados incluidos 79
Figura 260. Paso 3 – Re carga de CRL con certificados revocados incluidos 79
Figura 261. Paso 4 – Re carga de CRL con certificados revocados incluidos 79
Figura 262. Paso 5 – Re carga de CRL con certificados revocados incluidos 80
Figura 263. Paso 6 – Re carga de CRL con certificados revocados incluidos 80
Figura 264. Paso 7 – Re carga de CRL con certificados revocados incluidos 80
Figura 265. Paso 8 – Re carga de CRL con certificados revocados incluidos 81
Figura 266. Paso 9 – Re carga de CRL con certificados revocados incluidos 81
Figura 267. Paso 10 – Re carga de CRL con certificados revocados incluidos 82
Figura 268. Paso 1 – Distribución de certificado cliente puesto manual 82
Figura 269. Paso 2 – Distribución de certificado cliente puesto manual 82
Figura 270. Paso 3 – Distribución de certificado cliente puesto manual 83
Figura 271. Paso 4 – Distribución de certificado cliente puesto manual 83
Figura 272. Paso 5 – Distribución de certificado cliente puesto manual 83
Figura 273. Paso 6 – Distribución de certificado cliente puesto manual 83
Figura 274. Paso 6 – Distribución de certificado cliente puesto manual 83
Figura 275. Paso 7 – Distribución de certificado cliente puesto manual 84

Figura 276. Paso 8 – Distribución de certificado cliente puesto manual 84
Figura 277. Paso 9 – Distribución de certificado cliente puesto manual 84
Figura 278. Paso 10 – Distribución de certificado cliente puesto manual 84
Figura 279. Paso 11 – Distribución de certificado cliente puesto manual 84
Figura 280. Paso 12 – Distribución de certificado cliente puesto manual 84
Figura 281. Paso 13 – Distribución de certificado cliente puesto manual 84
Figura 282. Paso 14 – Distribución de certificado cliente puesto manual 85
Figura 283. Paso 15 – Distribución de certificado cliente puesto manual 85
Figura 284. Paso 16 – Distribución de certificado cliente puesto manual 85
Figura 285. Paso 17 – Distribución de certificado cliente puesto manual 85
Figura 286. Paso 18 – Distribución de certificado cliente puesto manual 86
Figura 287. Paso 19 – Distribución de certificado cliente puesto manual 86
Figura 288. Paso 20 – Distribución de certificado cliente puesto manual 87
Figura 289. Paso 21 – Distribución de certificado cliente puesto manual 87
Figura 290. Paso 1 – Distribución de certificado cliente CSR humano 88
Figura 291. Paso 2 – Distribución de certificado cliente CSR humano 88
Figura 292. Paso 3 – Distribución de certificado cliente CSR humano 88
Figura 293. Paso 4 – Distribución de certificado cliente CSR humano 89
Figura 294. Paso 5 – Distribución de certificado cliente CSR humano 89
Figura 295. Paso 6 – Distribución de certificado cliente CSR humano 89
Figura 296. Paso 7 – Distribución de certificado cliente CSR humano 89
Figura 297. Paso 8 – Distribución de certificado cliente CSR humano 89
Figura 298. Paso 9 – Distribución de certificado cliente CSR humano 90
Figura 299. Paso 10 – Distribución de certificado cliente CSR humano 90
Figura 300. Paso 11 – Distribución de certificado cliente CSR humano 90
Figura 301. Paso 12 – Distribución de certificado cliente CSR humano 91
Figura 302. Paso 13 – Distribución de certificado cliente CSR humano 91
Figura 303. Paso 14 – Distribución de certificado cliente CSR humano 91
Figura 304. Paso 15 – Distribución de certificado cliente CSR humano 92
Figura 305. Paso 16 – Distribución de certificado cliente CSR humano 92
Figura 306. Paso 1 – Creación de certificado Servidor 93
Figura 307. Paso 2 – Creación de certificado Servidor 93
Figura 308. Paso 3 – Creación de certificado Servidor 93
Figura 309. Paso 4 – Creación de certificado Servidor 93
Figura 310. Paso 5 – Creación de certificado Servidor 93
Figura 311. Paso 6 – Creación de certificado Servidor 93
Figura 312. Paso 7 – Creación de certificado Servidor 94
Figura 313. Paso 8 – Creación de certificado Servidor 94
Figura 314. Paso 9 – Creación de certificado Servidor 94
Figura 315. Paso 10 – Creación de certificado Servidor 94
Figura 316. Paso 11 – Creación de certificado Servidor 94
Figura 317. Paso 12 – Creación de certificado Servidor 94
Figura 318. Paso 13 – Creación de certificado Servidor 95
Figura 319. Paso 14 – Creación de certificado Servidor 95
Figura 320. Paso 15 – Creación de certificado Servidor 95
Figura 321. Paso 16 – Creación de certificado Servidor 95
Figura 322. Paso 17 – Creación de certificado Servidor 96
Figura 323. Paso 18 – Creación de certificado Servidor 96
Figura 324. Alertas y Notificaciones - Configuración 97
Figura 325. Alertas y Notificaciones - Vencimientos externos 97
Figura 326. Paso 1 - Agregar Vencimiento externo 98
Figura 327. Paso 2 - Agregar Vencimiento externo 98
Figura 328. Paso 3 - Agregar Vencimiento externo 98
Figura 329. Alertas y Notificaciones – Edición de Configuración 99
Figura 330. Alertas y Notificaciones – Alerta activa por previsión de alerta en días 100
Figura 331. Alertas y Notificaciones – Alerta de Vencimiento externo 100

Figura 332. Alertas y Notificaciones – Alerta de Vencimientos SSL 101
Figura 333. Paso 1 - Alerta por tarea programada 101
Figura 334. Paso 2 - Alerta por tarea programada 101
Figura 335. Paso 3 - Alerta por tarea programada 101
Figura 336. Paso 4 - Alerta por tarea programada 102
Figura 337. Paso 5 - Alerta por tarea programada 102
Figura 338. Paso 6 - Alerta por tarea programada 102
Figura 339. Paso 7 - Alerta por tarea programada 102
Figura 340. Paso 8A - Alerta por tarea programada 103
Figura 341. Paso 9A - Alerta por tarea programada 103
Figura 342. Paso 8B - Alerta por tarea programada 104
Figura 343. Paso 9B - Alerta por tarea programada 104
Figura 344. Paso 1 - Certificados de terceros 105
Figura 345. Paso 2 - Certificados de terceros 105
Figura 346. Paso 3 - Certificados de terceros 105
Figura 347. Paso 4 - Herramientas 105
Figura 348. Paso 5 – Verificar vencimiento On-Line 105
Figura 349. Paso 6 – Ejemplo verificación de vencimiento On-Line 105
Figura 350. Paso 7A – Ejemplo de operación sin implementar 106
Figura 351. Paso 7B – Ejemplo de operación sin implementar 106
Figura 352. Paso 1 - Pedido de certificado 106
Figura 353. Paso 2 - Pedido de certificado 106
Figura 354. Paso 3 - Pedido de certificado 107
Figura 355. Paso 4 - Pedido de certificado 107
Figura 356. Paso 5 - Pedido de certificado 107
Figura 357. Paso 6 – Pedido de certificado 107
Figura 358. Paso 7 – Ejemplo de Subjets CSR pre cargados 107
Figura 359. Paso 8 – Edición de Subjets CSR pre cargados 107
Figura 360. Paso 9 – Ejemplo de edición de Subjets CSR pre cargados 107
Figura 361. Paso 10 - Pedido de certificado 108
Figura 362. Paso 11 - Pedido de certificado 108
Figura 363. Paso 12 - Pedido de certificado 108
Figura 364. Paso 13 - Pedido de certificado 108
Figura 365. Paso 14 - Pedido de certificado 108
Figura 366. Paso 15 - Pedido de certificado 109
Figura 367. Paso 16 - Pedido de certificado 109
Figura 368. Paso 17 - Pedido de certificado 109
Figura 369. Paso 18 - Pedido de certificado 110
Figura 370. Paso 1 – Recepción y composición de certificado final 110
Figura 371. Paso 2 – Recepción y composición de certificado final 111
Figura 372. Paso 3 – Recepción y composición de certificado final 111
Figura 373. Paso 4A – Recepción y composición de certificado final 111
Figura 374. Paso 4B – Recepción y composición de certificado final 111
Figura 375. Paso 5 – Recepción y composición de certificado final 111
Figura 376. Paso 6 – Recepción y composición de certificado final 112
Figura 377. Paso 7 – Recepción y composición de certificado final 112
Figura 378. Paso 8 – Recepción y composición de certificado final 112
Figura 379. Paso 9 – Recepción y composición de certificado final 112
Figura 380. Paso 10 – Recepción y composición de certificado final 113
Figura 381. Validaciones varias – Text box campo vacío 113
Figura 382. Validaciones varias – Text box Mensaje 113
Figura 383. Validaciones varias – Text box correo electrónico 114
Figura 384. Validaciones varias – Text box Mensaje 114
Figura 385. Validaciones varias – Text box Documento de Identidad 114
Figura 386. Validaciones varias – Text box Mensaje 114
Figura 387. Validaciones varias – Check list tipo certificado 114

Figura 388. Validaciones varias – Check list Mensaje 114
Figura 389. Validaciones varias – Nombre de usuario duplicado..... 115
Figura 390. Validaciones varias – Días mínimo y máximos permitidos 116
Figura 391. Validaciones varias – Días mínimo y máximos permitidos 117
Figura 392. Validaciones varias – Campo vacío..... 118
Figura 393. Validaciones varias – Correo electrónico 119
Figura 394. Validaciones varias – Dominio on line 119
Figura 395. Paso 1 - Auditoria y manejo de errores 120
Figura 396. Paso 2 - Auditoria y manejo de errores 120
Figura 397. Paso 3 - Auditoria y manejo de errores 120
Figura 398. Paso 4 - Auditoria y manejo de errores 121
Figura 399. Paso 5 - Auditoria y manejo de errores 121
Figura 400. Paso 6 - Auditoria y manejo de errores 121
Figura 401. Paso 7 - Auditoria y manejo de errores 121
Figura 402. Paso 1 - Modo aprendizaje 122
Figura 403. Paso 2 - Modo aprendizaje 122
Figura 404. Paso 3 - Modo aprendizaje 122
Figura 405. Paso 4 - Modo aprendizaje 122
Figura 406. Paso 5 - Modo aprendizaje 123
Figura 407. Paso 6 - Modo aprendizaje 123
Figura 408. Paso 7 - Modo aprendizaje 123
Figura 409. Paso 8 - Modo aprendizaje 123
Figura 410. Paso 9 - Modo aprendizaje – Customización de Subject 124
Figura 411. Paso 10 - Modo aprendizaje – Customización de Subject 124
Figura 412. Control de versiones 135

5.2. Índice de Tablas

Tabla 1. Especificación de modalidades por tipo y multiplicidad 70
Tabla 2. Especificación de SUBJ's sugeridos por tipo de certificado 88
Tabla 3. Ejemplos de máscaras de validación en controles cC 115
Tabla 4. Templates existentes y pre configurados por cC..... 124
Tabla 5. Configuraciones globales existentes y pre configuradas incluidas en cC 127
Tabla 6. Datos dinámicos parametrizables resistentes a la obsolescencia programada 135
Tabla 7. Tipos de uso de claves publicas SSL 153

6. Bibliografía general

Apache Tomcat 8 Configuration Reference, Version 8.5.35, https://tomcat.apache.org/tomcat-8.5-doc/config/http.html (consultada el 09/11/2018)

Apache, HTTP Server Version 2.4, https://httpd.apache.org/docs/2.4/mod/mod_ssl.html (consultada el 29/01/2019)

Autoridad certificante, Guía para gestión de certificados digitales, AFIP, https://acn.afip.gob.ar/docs/AC_AFIP_GUIA_GESTION_DE_CERTIFICADOS_V2.09.pdf (consultada el 20/03/2019)

Brian Komar, Windows Server 2008 PKI and Certificate Security eBook, https://kvazar.files.wordpress.com/2008/12/unencrypted.pdf (consultada el 01/05/2018)

Buenas prácticas TLS / SSL, https://ciberseguridad.blog/buenas-practicas-tls-ssl/ (consultada el 17/11/2018)

Buenas Prácticas, CCN-CERT BP-01/17, Recomendaciones de Implementación de HTTPS, https://www.rediris.es/tcs/doc/ccncert/CCN-CERT_BP-01-17_Recomendaciones_implementacion_HTTPS.pdf (consultada el 27/03/2018)

Certificate Transparency v2.1a, https://www.links.org/files/CertificateTransparencyVersion2.1a.pdf (consultada el 06/06/2019)

CSIRT-CV, Guía de uso seguro de certificados digitales, https://concienciat.gva.es/wp-content/uploads/2018/03/info_guia_uso_seguro_certificados_digitales.pdf (consultada el 09/03/2019)

Firma Digital, Poder Judicial de la Provincia de Buenos Aires, https://firmadigital.scba.gov.ar/Default.aspx (consultada el 24/01/2019)

Fundamentos sobre certificados digitales, https://www.securityartwork.es/2014/02/21/fundamentos-sobre-certificados-digitales-declaracion-de-practicas-de-certificacion-ii/ (consultada el 11/10/2019)

Gestión de certificados digital, Colegio de Abogados, http://www.casm.org.ar/material/GESTIONDECERTIFICADOSDIGITALAGOSTO2016.pdf (consultada el 07/04/2019)

Guía para tramitar firma digital, Colegio de Abogados, Versión 3, http://www.casm.org.ar/material/GUIA%20PARA%20TRAMITAR%20FIRMA%20DIGITAL%20COLEGIO%20DE%20ABOGADOS%20VERSION%203.pdf (consultada el 11/05/2019)

Guía rápida para la generación de un certificado digital, https://www.owasp.org/images/e/ed/GenerateCertificate.pdf (consultada el 17/06/2019)

Guía sobre riesgos y buenas prácticas en autenticación online, Inteco, https://northsecure.es/wp-content/uploads/2013/05/guia_inteco_autenticacion.pdf (consultada el 07/06/2019)

How can I watch the current connections on my Apache webserver?, https://askubuntu.com/questions/239631/how-can-i-watch-the-current-connections-on-my-apache-webserver (consultada el 21/07/2019)

How to read the SSL certificate info from the CLI, https://ma.ttias.be/how-to-read-ssl-certificate-info-from-the-cli/ (consultada el 11/02/2019)

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.ietf.org/rfc/rfc5280.txt (consultada el 10/07/2018)

Internet X.509 Public Key Infrastructure Certificate and CRL Profile, https://tools.ietf.org/html/rfc2459 (consultada el 12/09/2018)

Internet X.509 Public Key Infrastructure Qualified Certificates Profile, https://tools.ietf.org/html/rfc3039 (consultada el 03/08/2018)

ITU-T X.509 Public-Key and Attribute Certificate Frameworks Recommendation, http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-200811-S!!PDF-E&type=items (consultada el 02/09/2019)

OpenSSL, CA, https://www.openssl.org/docs/man1.1.1/man1/ca.html (consultada el 19/02/2019)

OpenSSL, CRL, https://www.openssl.org/docs/man1.1.1/man1/crl.html (consultada el 27/02/2019)

OpenSSL, PKCS12, https://www.openssl.org/docs/man1.1.1/man1/pkcs12.html (consultada el 08/04/2019)

OpenSSL, PKCS7, https://www.openssl.org/docs/man1.1.1/man1/pkcs7.html (consultada el 09/03/2019)

OpenSSL, Req, https://www.openssl.org/docs/man1.1.1/man1/req.html (consultada el 17/02/2019)

OpenSSL, x509, https://www.openssl.org/docs/man1.1.1/man1/x509.html (consultada el 11/02/2019)

OpenSSL commands, https://www.openssl.org/docs/manmaster/man1/ (consultada el 05/02/2019)

OpenSSL example configuration file, http://web.mit.edu/crypto/openssl.cnf (consultada el 20/08/2018)

OpenSSL, Cryptography and SSL/TLS Toolkit, https://www.openssl.org/ (consultada el 02/10/2018)

PKI Secrets Engine, https://www.vaultproject.io/docs/secrets/pki/index.html (consultada el 13/10/2019)

Recommendation X.509, https://www.itu.int/rec/T-REC-X.509/en (consultada el 22/04/2019)

Representation and Verification of Domain-Based Application Service, Identity within Internet Public Key Infrastructure Using X.509 (PKIX), Certificates in the Context of Transport Layer Security (TLS), https://tools.ietf.org/html/rfc6125.html (consultada el 22/08/2019)

SSL / TLS Best Pactices, Deploy SSL with Confidence, https://www.entrust.com/lp/wp-content/uploads/sites/2/2016/07/Entrust-eGuide-SSL-Best-Practices-V2-WEB.pdf (consultada el 17/06/2019)

SSL and TLS Deployment Best Practices, https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices (consultada el 17/06/2019)

SSL Certificate PIN, Safe Appliance, How to Guide, https://kb.swivelsecure.com/w/index.php/SSL_Certificate_PINsafe_Appliance_How_to_Guide (consultada el 01/07/2019)

SSL/TLS Best Practices for 2019, https://www.ssl.com/guide/ssl-best-practices/ (consultada el 27/08/2019)

The Transport Layer Security (TLS) Protocol, Version 1.2, https://tools.ietf.org/html/rfc5246 (consultada el 07/07/2018)

Tipos de certificados, Agencia de Tecnologia y Certificacion Electronica, https://www.accv.es/ (consultada el 23/10/2019)

Trabajo con los certificados en Java keystore, https://www.sslmarket.es/ssl/help-trabajar-con-los-certificados-en-java-keystore/ (consultada el 19/10/2018)

Usando certificados SSL de cliente como sistema de autenticación web, Jesus Iglesias, http://blog.osusnet.com/2008/10/11/usando-certificados-ssl-de-cliente-como-sistema-de-autenticacion-web/ (consultada el 22/06/2019)

Web-based SSH in your browser, Web Console, http://web-console.org/ (consultada el 25/11/2019)

Whiptail, Linux man page, Display dialog boxes from shell scripts, https://linux.die.net/man/1/whiptail (consultada el 13/11/2018)

7. Bibliografía específica

[1] Infraestructura de clave pública, Wikipedia, https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica (Consultada el 12/10/2019)
[2] Código Abierto, Wikipedia, https://es.wikipedia.org/wiki/C%C3%B3digo_abierto (Consultada el 03/11/2019)
[3] Open Source Iniciative, https://opensource.org/ (Consultada el 03/11/2019)
[4] Añadir certificados CA al almacén de claves JRE, IBM https://www.ibm.com/support/knowledgecenter/es/SSEP7J_10.2.2/com.ibm.swg.ba.cognos.adm_ba_pattern.1.2.0.doc/t_biblu_add_cacert.html (Consultada el 29/11/2019)
[5] Certificados digitales, Guía sobre riesgos y buenas prácticas en autenticación online, https://northsecure.es/wp-content/uploads/2013/05/guia_inteco_autenticacion.pdf#page=29&zoom=100,0,841 (Consultada el 19/07/2019)
[6] D. Cooper, Certificate and Certificate Extensions Profile, https://tools.ietf.org/html/rfc5280#section-4 (Consultada el 02/04/2019)
[7] X.509 Certificate, https://www.securityartwork.es/wp-content/uploads/2014/04/Certificados-Digitales-Imagen-1.png (Consultada el 21/08/2019)
[8] https://www.fehcom.de/images/figure_11.png (Consultada el 28/11/2019)
[9] UTC, Wikipedia, https://es.wikipedia.org/wiki/Tiempo_universal_coordinado (Consultada el 03/11/2019)
[10] GeneralizedTime, Wikipedia, https://en.wikipedia.org/wiki/GeneralizedTime (Consultada el 03/11/2019)
[11] Root CA Configuration File, OpenSSL PKI Tutorial, https://pki-tutorial.readthedocs.io/en/latest/simple/root-ca.conf.html (Consultada el 28/05/2019)
[12] D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc5280.html (Consultada el 28/12/2018)
[13] D. Cut y a, Fundamentos sobre certificados digitales (IV): Mecanismos de validación de certificados, Security Art Work, https://www.securityartwork.es/2013/07/24/fundamentos-sobre-certificados-digitales-iv-mecanismos-de-validacion-de-certificados/ (Consultada el 05/01/2019)
[14] PFX Tutorial de Exportar Importar Certificados SSL en IIS 7, https://www.digicert.com/es/apoyo-tecnico/importar-exportar-archivo-pfx-iis-7.htm (Consultada el 12/09/2018)
[15] PKCS 12, Wikipedia, https://en.wikipedia.org/wiki/PKCS_12 (Consultada el 12/10/2019)
[16] x509v3_config, https://www.openssl.org/docs/manmaster/man5/x509v3_config.html (Consultada el 04/04/2018)
[17] Autoridad de sellado de tiempo, Wikipedia, https://es.wikipedia.org/wiki/Autoridad_de_sellado_de_tiempo (Consultada el 13/08/2019)
[18] C. Adams y D. Pinkas, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), https://tools.ietf.org/html/rfc3161 (Consultada el 19/11/2019)
[19] SID - Sistema de Identidad Digital, https://www.argentina.gob.ar/sid-sistema-de-identidad-digital (Consultada el 29/11/2019)
[20]Taxistas deben usar nueva identificación, http://www.defensoriaturista.org.ar/oldweb/index.php/noticias/34-taxistas-deben-usar-nueva-identificacion (Consultada el 16/10/2019)
[21] Advanced PKI, OpenSSL PKI Tutorial, https://pki-tutorial.readthedocs.io/en/latest/advanced/index.html (Consultada el 11/06/2019)
[22] TLS Client Certificate Request Configuration File, OpenSSL PKI Tutorial, https://pki-tutorial.readthedocs.io/en/latest/expert/client.conf.html (Consultada el 11/06/2019)
[23] TLS Server Certificate Request Configuration File, OpenSSL PKI Tutorial, https://pki-tutorial.readthedocs.io/en/latest/expert/server.conf.html (Consultada el 11/06/2019)
[24] Software CA Configuration File, OpenSSL PKI Tutorial, https://pki-tutorial.readthedocs.io/en/latest/advanced/software-ca.conf.html (Consultada el 13/06/2019)
[25] Root CA Configuration File, OpenSSL PKI Tutorial, https://pki-tutorial.readthedocs.io/en/latest/advanced/root-ca.conf.html (Consultada el 18/06/2019)