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 abrev	/iaturas y acrónimos	vii
1. Cue	erpo intro	ductorio	1
1.1.	Introduc	cción	1
1.2.	Objetivo	DS	2
1.3.	Alcance		2
1.4.	Hipótesi	is	2
2. Cue	erpo princ	cipal	3
2.1.	Certifica	ados Digitales	3
2.2.	Gestión	de certificados digitales	4
2.3.	Escenai	rios de autenticación	5
2.4.	Tipos de	e certificados	5
2.5.	Estructu	ura estándar de Certificados	5
2.6.	Especifi	icaciones del modelo	8
2.6.	1. Der	nominación	8
2.6.	2. Arq	quitectura	9
2.6.	3. Dia	igrama de flujo de procesos	9
2.7.	Diseño	del prototipo experimental implementado	14
2.7.	1. Lim	nitaciones	14
2.7.	2. Pru	iebas de concepto	14
2.7.	3. Pre	errequisitos	14
2	.7.3.1.	Requisitos de software	15
2	.7.3.2.	Requisitos de hardware	15
2.7.	4. Ope	eración	15
2.8.	Casos c	de prueba	19
2.8.	1. Ent	torno 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	. Ent	torno 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	2.8.2.17	7.1. Consulta de certificados cliente	68
2	2.8.2.17	7.2. Revocar certificados cliente	69
2	2.8.2.17	7.3. Nuevo certificado cliente	70
2	2.8.2.17	7.4. Creación de Cliente: Manual – Humano	70
2	2.8.2.17	7.5. Revocación de Cliente	75
2	2.8.2.17	7.6. Re carga de CRL con revocaciones	78
2	2.8.2.17	7.7. Distribución de Cliente: Manual – Puesto	82
2	2.8.2.17	7.8. Distribución de Cliente: CSR – Humano	87
2	2.8.2.17	7.9. Creación de certificado Servidor	92
2.8	.2.18.	Alertas y notificaciones	96
2.8	.2.19.	Certificados de terceros	104
2	2.8.2.19	0.1. CSR: Pedido de certificado	106
2	2.8.2.19	0.2. 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. 1	[empla	tes SSL	124

2.9.1. cC S	Sub-CA RA - Puesto	124
2.10. Config	uración global	127
2.10.1. Cont	fig.ini: cC Sub-CA RA	127
2.11. Archive	os dinámicos	133
2.12. Contro	I de versiones	135
2.13. Aporte	s principales	135
2.14. Futuro		136
3. Conclusiones	;	137
4. Anexo		138
4.1. Ampliacio	ón de Configuración Global	138
4.1.1. Cont	fig.ini: cC CA	138
4.2. Ampliacio	ón de Templates SSL	140
4.2.1. cC S	Sub-CA RA – Humano	141
4.2.2. cC S	Sub-CA RA – Servidor	143
4.2.3. cC S	Sub-CA RA – Monitoreo	145
4.2.4. cC S	Sub-CA RA	146
4.2.5. cC C	CA	150
4.3. Tipos de	uso de claves públicas	153
5. Índices espec	cíficos	154
5.1. Índice de	Figuras	154
5.2. Índice de	P Tablas	161
6. Bibliografía g	eneral	162
7. Bibliografía es	specífica	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:

- <u>Confianza de única fuente</u>: un único recurso despliega sobre el entorno correspondiente el escenario adecuado y customizado según corresponda, evitando su configuración e interacción manual.
- <u>Control centralizado de permisos de acceso</u>: 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.
- <u>Control de pérdidas:</u> permite mitigar las pérdidas de certificados al ubicarse en el almacén correspondiente con su política de resguardo según corresponda.
- <u>Revocación, expiración y destrucción controlada:</u> permite realizar la gestión correspondiente gracias a su organización unificada.
- ✓ <u>Distribución</u>: 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

10



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:

- <u>cC CA:</u>
 - S.O.: Centos v6.5 o superior (Se recomienda utilizar v7)
 - Paquetes: net-tools, nano, vim-enhanced, system-configfirewall-tui, system-config-keyboard, dpkg-reconfigure tzdata, system-config-language, openssl, sshpass
- <u>cC Sub-CA:</u>
 - S.O.: Centos v6.5 o superior (Se recomienda utilizar v7)
 - Paquetes: net-tools, nano, vim-enhanced, system-configfirewall-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

- <u>VM / VA CA:</u>
 - 1 CPU
 - o 1 GB Memoria
 - o 16 GB Disco
 - o vLan Adaptador de red
- VM / VA Sub-CA:
 - 1 CPU
 - 1 GB Memoria o superior
 - o 16 GB Disco o superior
 - o 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 onpremise (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

ß	root@ccca:~/scripts/centralizerCert - 🗆	×
Sel	eccionar la opción correspondiente dentro de las acciones disponibles a ejecutar sobre centralizerCert CA:	^
1.	Instalar centralizerCert_CA (primera vez)	
2.		
з.	Realizar BKP de centralizerCert_CA actual	
4.	Actualizar FUENTES CA CORE con instalación actual de centralizerCert CA	
5.	Actualizar FUENTES SUBCA_CORE con instalación actual de centralizerCert_SUBCA	
б.		
7.		
The	resar opción a ejecutar: 1	U U

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

🖉 roedbeces-heripticentraliserCet_CA		×
Señal SIGINT restrablecida a modo activo (permite: CTRL+C)		^
dP dP oo abbete, dP BB BB BB AD		
199 190 190 190 190 190 190 190 190 190		
Es un wrapper para la construcción de un entorno integral, sencilio y confisble, preconfigurado y centralizado de acuerdo a los estándares correspondientes para la creación y mantenimiento de una CA / Entermedia CA SUB-CA		
Es diseñado, creado e implementado por Ing. Matias Varquer Hess AB & 2018-2015 - Todos los derechos reservado. Diseñado en Adgentina pars el MHNO0!		
Consector anianythmail.com builter / syme / Lastapran mailanyth Presidon califyrer feid pars consistant		

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

Archivo de Configuración CentralizerCert CentralizerCert CA by Eng. MRV2N
/ ARCHIVE OF CONFIGURATION OF centralizerCert ROOT-CA / ARCHIVO DE CONFIGURACION DE centralizerCert RAIZ by Eng, NNVEH / Ing. Naties Verquer Ness
#Copyright (n) 2018 - 2019 Ing. Matias Vasques Heas / Eng. HQViH
j Comment beginning uits '/'
; Simple definitions for 'prefix option' (change the INI_ prefix to the indicated prefix)
second valances / valances / volonces
CORE_VERSION=*version*
<pre>#01C081_THP="tep" -> Default: sino se incluye la barra al inicio y al final ('tmp'), se le agrega por codiço ('/tmp/'), sino queda como esta. 0LOBAL_THP="tmp"</pre>
fíndica la ubicación del path de las CA-root a generar(mientras que la ejecución de la estructura sera desde donde estoy parado y relativo) GLOBAL_CERT***
<pre>ADDAL_EREDP-VDT* -> Default genera denire de BLOBAL_TOP los reportes con los errores capturados, que no secesariamente son todos los errores que se pueden product. El esta en OTT, al finalizer se horrars el archivo deno. ELORAL_EREDP-VDT ELORAL_EREDP-VDT Hol on DECADAT, ERED PTLI-VDT ELORAL_EREDP-VTLI-VDT ELORAL_EREDP-VTLI-VDT ELORAL_ERED_FTLI-VDT ELORAL_ERED</pre>
CATEZENINGUE ATTANA TITEZENINGUE ATTANA CATEZENINGUE ATTANA
SICORL GUI / INTEFRA GRAFICA GLORL ITTL=""CentralizesCets CA by Kng. MAVAM" MACTITL="CentralizesCets to as creation del Ing. Matias Yazquez Hess / Eng. MAVAH - Copyright (c) 2018 - 2019 [AA]*
«Aceptar»

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

Archivo de Configuración CentralizerCert CentralizerCert CA by Eng. MSV28
007+"Malptal"
El estado de salida de "MEIFFALL" es 0 si se sale presionando al botón Yes u OK, y 1 si se presiona el botón No o Cancel. # De lo contratio, si se producem errores entro de esto, o se sale presionando la tecida 255, el estado de salida es 255.
UT_TIL_COBRCTION*4*
725.878*54 NO.578**140*
OK 511**Aceptat* CAXCLL 51**Canetat*
FACTOR_REVIEWONNELT-S
FGLORAL MESSAGES / MENSAGES GLORALES
B
eror. For esta razón, a pesar de tomar el cuidado necesario en su escritura, puede quedarse atascado en una pantalla sin poder cancelar. Esto puede forzario a cancelar una sesión SSN o matar el proceso zombie.
IMPORTANTE: ¡Las acciones a realizar a partir de este momento, no son reversibles!
¿Desea continuer?" Mission Continuer a continuer "
#SCCIONES / SECCIONES #Importante no incluir '-' en el nombre de cada seccion pues dara error la lectura de esta. Etemplo de error: '(ca-root)'
fervironnes)
Barregar dimantcammente por cada entorno, la cantidad de variables segun FACTOR_ENVIRONMENT: "ENVAT! + '_€'. ENVAT! →= MENOCOCCON+
ENVIENVI
EXMT_e**validacion*
[resulted]
TEMPLATE_BOOT_CA+*root-ca.cnf*
[caroot]
CA ACRIVIT DEFAULT-VAL-GEDA* CA PREIN-**
CA_MSM=*CA+coc* CA_DXYSTLP*cAAva,cocf*
CA NO FILE="caMD_cont" -> Los valores 128 y 234 (o cualquiera menor a 512) da error: ' ras routines/838 signidigest too big for ras keyiras sign.c'
(Acettat)

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

fff Cre	ando archivo: debug_audit-20190715_145105_menu_CA, con la marca: 20190715_145105 ###
*** Ins	210 ***
	Funcion: INICIAR
	Funcion: VALIDAR ENTORNO
	>> Se seteo el path inicial: /root/scripts/centralizerCert_CA/scripts//CA-root/
	>> Se seteo el dateStampi 20190715
	(>> Se seteo el timeStamp: 145105
	Funcion: DEBUG_SETEOS
	I>> Seteos: CA_INP del config.ini: tmp - Correction: /root/scripts/centralizerCert_CA/scripts//tmp/
	Funcion: INICIALIZAR_ENTORNO
	>> Seteos: Se activa bloqueo de señal SIGINT (CIRL+C / CIRL+Z) para evitar cancelar ejecución NORMAL de CentralizerCert
	Sector Sector Se desective Eloqueo de Senar Stolar (Claure / Claure) por sobo subar Lebos Fola activo:
	Publication (RECARDAN)
	FUNCTION: READ-GAR
	Funcional HEAD_CONFECTMENT_LAD
	Funcion: MENU SISTERA
	Funcion: EJECUIAE COMMIDD (cat config.ini)
	Funcion: MERU SISTERA
	Funcion: MENU CA
	Funcion: MENU SEGURIDAD
	Funcion: MENU_CA
	Funcion: MENU_SEGURIDAD
	Funcion: MERU_CA
	Funcion: HERU_SISTENA
	Funcion: MENU_CA
	Funcion: ACERCA DE
	Funcion: MERU CA
	FUNCION MENU SISTERA
	FUNCION RENU LA
	Supprise Information and Annual Ann
	Functions MERI STATENA
	Funcion: EDITAR ARCHIVO
	>> Se genera backup: config.ini previo a edición
	>> Se editai config.ini
iles c	onfig.ini and /root/scripts/centralizerCert_CA/scripts/.//BacKuP/BKP_20190715_145108_config.ini are identical
	(<<< Diferencias >>>
	Funcion: MENU_SISTEMA
	Funcion: NAVEGAR_DIRECTORIO_VISUALIZAR_ARCHIVO
	Funcion: EJECUIAR COMANDO (cat /root/scripts/centralizerCert CA/scripts//tmp/debug audit-20190715 145105 menu CA.log)

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

	Autoridades Corti	
2 1-2	Nueva Autoridad C	ertificante Raiz
3 <-1	Volver	
	A	
	<pre><aceptar></aceptar></pre>	<cancelar></cancelar>

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

CentralizerCert Configuración de CA-Root: CA-CCRBA del Ingrese provincia de origen de la CA pa Raiz	A by Eng. MOVEM entorno de: EEMO - 5 de 11 rra la nueva Autoridad Certificante
<aceptar></aceptar>	<cancelar></cancelar>

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

2 → Viscalizar CoN 3 → Gustomizar (ED 4 → Gustomizar (ED 5 → Gustomizar (ED 5 → Liscar BD (pla 6 → RFVOCAR (innah 7 → SENOVAR (actua 8 → SaNoV (respute 9 → Eliminar → [Ro 10 → Eliminar (Data 1) → Desplegar remo 12 <-1 Volver	IIFIGUACIADO ADSOTIASA FIGURACIÓN SAL Auto ITAR) configuración (Autocadad Certión na) SSL Autoridad Ce IItar) Autoridad Ce IItar) Autoridad Ce dar) (DetaStamp) Autoridad Stamp] Autoridad Ce tammente (Root-CA: C	Certificante Raiz reidad Certificante Raiz stil Autoridad Certificante Ra certificando Raiz ertificando Raiz norsidad Certificante Raiz norsidad Certificante Raiz rrificante Raiz rrificante Raiz CA-CECBA en SUB-CA sobre Raj	

Figura 50. Paso 23 - Creación de CA



Figura 51. Paso 24 - Creación de CA


Figura 52. Paso 25 – Creación de CA

V 290715180006Z 0100 C1127AAA	CA Bair Index.db Y=Yalido / B=Terpirado estormo EDD0 - Roos-CAI (L-CECEA - Deredtamp) 2018/015 Centralises/Cers CA by Eng. MBYER unknown //C=AB/JT=CABA/0=Colegio de Escribanos de la Cladad de Buenos Aires/CD=COmputos, Operaciones/CD=CA - Colegio de Escribanos de la CABA/postalAddress=Las Heres 1833,
	chesptar>

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

HOME = .	
RANDFILE - SENV:	:HOME/.rnd
oid_section = ne	w olds
#Extra OBJECT ID	entifier info
[new_oids]	
postalAddress =	2.5.4.16
1.00.1	
default_ca = CA_	default
[CA default]	
# Directory and	file locations.
dir	· ,
certs	= \$dir/certs
crl dir	= \$dir/crl
new_certs_dir	= \$dir/newcerts
funique subject	= no (permite subject's duplicados)
unique_subject	- yes
database	= \$dir/index.db
serial	= \$dir/serial
RANDFILE	= \$dir/private/.rand
# The root key a	nd root certificate.
private_key	= \$dir/private/ca.key.pem
certificate	= \$dir/certs/ca.cert.crt.pem
# For certificat	e revocation lists.
crinumber	= \$dir/crlnumber
crl	= \$dir/crl/ca.crl
crl_extensions	= crl_ext
default_crl_days	- 30
# SHA-1 is depre	cated, so use SHA-2 or SHA-3 instead.
default_nd = sha	256
name_opt	= ca_default
cert_opt	= ca_default
default_days = 3	653
preserve	= no
policy	- policy_strict
	(Aceptar)



Figura 55. Paso 2 – 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

Configuración equipo rem	stralizerCert CA by Eng. MRVzH oto - 1 de 6:
Ingrese el nombre del eq especiales:	sipo remoto a vincular sin espacios ni caracteres
Ejemplo: equipo.dominio.	com.az
cC_Sub-CA	
CACE.	star> <cancelar></cancelar>

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

Configuración	equipo remoto - 2 de 6:	A by Eng. MRV2H	
Ingrese la dir Ejemplo: 10.10	ección ip del equipo remo .1.101	to a vincular:	
10.10.0.104			_
	<aceptar></aceptar>	<cancelar></cancelar>	





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



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

Configuración equipo remoto - 5 de 6r Ingrese la password del usuario root jp 10.10.0.0104, la cual será utilizad remotamente sin persistir la misma.	CA by Eng. MRVIN para el equipo / host cC_Sub-CA con la la para copiar la llave publica
<aceptar></aceptar>	<cancelar></cancelar>

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

Configuración equipo	CentralizerCert remoto - 6 de 6:	CA by Eng. MRVzH	
Ingrese descripción (del equipo remoto	a vincular:	
Ejemplo: Sub-CA (RA)			
	(Aceptar>	<cancelar></cancelar>	

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

- 1	Centrals	perCert CA	by Eng. 3	SKV2H
Esta detall	punto de ado a con	denunciar tinuación:	el equipo	remoto
-Equip -Ip: 1 -Puert -Deuct -Deuct	c (Host): 0.10.0.10 c: 22 ic: root ipción: S	ಂದ್ತತೆಯ-ರಸ ಕ ಯ-ರಸಿ		
2Deper	Continue	27 DC182	Gaper	llar

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

1 I-> Conexiones totales	
2 (-> Conexiones activas	
3 -> Conexiones inactivas	
4 1-> Denunciar vinculo remoto / Relat	ción de confianza
5 -> Visualizar vinculo remoto / Rela	ción de confianza
6 (-> Eliminar vinculo remoto / Relaci	ión de conflanza
7 (-> Desplegar (Instalar / Actualiza: 8 <-) Volver	r) remotamente CORE en SUB-CA sobre R
	(Canadan)

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

Equipo / Host	Ip	Puerto	Usuario	Descripciós
oC_Sub-CA	10.10.0.104	22	root	Sub-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:

cheeptar>	<cancelar></cancelar>
<- Volver	
(-> Eliminar vinculo remoto / Relaci	on de conflanza
-> Visualizar vinculo remoto / Rela	ción de confianza
-> Denunciar vinculo remoto / Relac	ión de confienze
-> Conemiones inactivas	
-> Conexiones activas	
1-> Coneviones totales	
rectioner is operation a realizer:	

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

	CentralizerCert	CA by Eng. MRVaH
NO se pudo Centralize /zoot/scri del equipo	detectar la existen rCert SUB-CA RA ub pts/centraligerCert / host: cC_Sub-CA.	oria del CORE del entorno de biosdo en: SUBCA para la IP: 10.10.0.104
(Confirma Centralize	el desplieque por pr rCert?	rimera vez del CORE de
	Rospitar	Cancelar

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

1 2 3 4	I-> Visualizer CERTIFICADO Autoridad Certificante Raiz I-> Visualizer CONFIGURACIÓN SIS Autoridad Certificando Raiz I-> Customizer (EDITAR) configuración SSL Autoridad Certificante Raiz I-> Visua derallas Autoridad Certificante Dala
5	-> Listar BD (plana) SSL Autoridad Certificando Rais
5	(-> REVOCAR (inhabilitar) Autoridad Certificandte Raiz
2	(-> RENOVAR (actualizar) Autoridad Certificandte Raiz (-> ReNuE (resentander) (Carafree) Autoridad Certificante Raiz (BVD)
2	(-> Eliminar [Root-CA] Autoridad Certificante Raiz
20	0 -> Eliminar (DataStamp) Autoridad Certificante Rais
	1 -> Desplegar remotamente (Root-CA: CA-CECBA en SUB-CA sobre RA)
2	
11	2 <-) Volvez
11	2 <-) Volvez
11	2 <-) Volvez
1.4	2 <-) Vülves

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

las siguientes colecciones de sof en la instalación actual.	tware predefinidas, las cuales no se encuentran
<pre>(*) #ystem-config-firewall-tui (*) #ystem-config-firewall-tui (*) #ystem-config-language () update () upgrade () upgrade () wim-enhanced</pre>	007 Firewall 007 Feeboard 007 Leopard Actualizar 80 Actualizar 90 Actualizar 90 Actual
Instalar	Cancellar

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

Prostdecuulex-recipticentaiserCet_SMCA	- 1	۰.	×
Señal SIGNNT restrablecida a modo activo (permite: CTRL+C):			^
dP dP no 4305836. dP 60 63 69 69			
.488580. 488580. 688589 688689. 48889 6886880. 488680. 488680. 488680. 488580. 48859 1 *** #86000489 **88 88 88 **88 **88 88 488 88 4.887 888 88 4.887 88 88 88 80,80,80 88 88 88 8880 88 480 8880 8880 8880 88 40,80 480 88 88 88 88			
occorrectore and the second se	/ RA		
Re diseñado, creado e implementado por Ing. Matina Vanguez Ress AR & 2018-2019 - Todos los derechos reservado.			
Utseñado en Añgentina para el MUNDO!			
Contecto: matlasvz@pmal.com twitter / skype / instagram: matlasvzh Presione cualquier tecla para continuar			v

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:

SUB-CA CentralizerCert SUBCA RA by Eng. MRV2H Seleccionar la operación a realizar:
1 Red
2 Sistema
3 Seguridad
4 Conexiones
5 Autoridad de Registro [RA]
6 Acerca de centralizerCert
/ 20111
Aceptar Cancelar

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



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

Archivo de Configuración CentralizerCert CentralizerCert SUBCA RA by Eng. HNVEN
) ARCHIVE OF CONFIGURATION OF CentraliserCert SUB-CA / ARCHIVO DE CONFIGURACION DE CentraliserCert Intermedio by Eng. MBViH / Ing. MBViH / Ing. Heise Varguez Hess
#Copyright (c) 2018 - 2019 Ing. Hatias Vanquez Hess / Eng. HBVzH
r Comment Registrating vita '1' C Comment Registrating vita '1'
/ Simple definitions for 'prefix option' (change the INI_ prefix to the indicated prefix)
HUDBALTS / HADLATS <td< td=""></td<>
CORE_VERSION="version"
PECABL_DEG="top" -> Defmilt: sino se incluye la barra al inicio y al final ("top"), se le agrega por codigo ("/top/"), sino queda como esta. ELCEBL_DEG="top"
Finites la ubication del path de las 578-58 a generar(mientras que la ejecution de la estructura sera desde donde estoy parado y relativo) ELOBAL_CERT=**
HELDER_IEIDEN-OFF -: Default penets destro de GLOBAL_TBP los reportes con los errores capturados, que to necesariamente en todos los errores que se paeden producir. Si esta en OFF, al finalizar se horras el archive HELDER_IEIDEN-THP HELDER HE
DATETIDESTAN-sate +4Y4mbd_VENthS
deeptar>

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

Archivo de Configuración CentralizerCert CentralizerCert SUBCA RA by Eng. NEV2N
<pre>sticuture (or /) referent entries const. Title="constantion" File" (File" File" File</pre>
PACTOR_DIVISIONDT->
ELONAL MESSAGE / MENLINE COMMISSION MARKET MESSAGE / MENLINE COMMISSION MARKET MESSAGE / MENLINE COMMISSION AND A MERLINE COMMISSION OF AN ADMINISTRATION OF AN ADMINISTRATION OF A MENLINE MESSAGE AND A MERLINE ADMINISTRATION OF A MERLINE COMMISSION OF A MERLINE ADMINISTRATION OF A MERLINE ADMINISTRATION OF A MERLINE MESSAGE ADMINISTRATION OF A MERLINE ADMINISTRATION OF A MERLINE ADMINISTRATION OF A MERLINE ADMINISTRATION OF A MERLINE ADMINISTRATION OF A MERLINE ADMINISTRATI
(Derse continuat)* NGU SUT 10 CONTING*Tration cualquier teols para continuat *
escrions / socioses Esperanent ou incluir '' en el nombre de cada seccion pues data error la lectura de esta. Ejemplo de error: '[sub-ca]' (environnent) Regregar financiones por cada entorno, la canidad de variables sepon FACTON_EDVIRONNETT: 'EFORT' + '_t'. ENVEL-variant ENVEL-variant ENVEL-variant
Inspired TBFSLAT_NOC CA**cost-ca.cd* TBFSLAT_ST_20C CA**cost-ca.cd* TBFSLAT_ST_20C ca**cost-ca** TBFSLAT_ST_20C ca**cost-ca** TBFSLAT_ST_20C ca**cost-ca**
despus

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

Archivo de Configuración CentralizerCert CentralizerCert SUBCA RA by Eng. MSV28
[auboaroot]
Annual Rations / Configuration
article and the second and a second and as
SUDA FEILAN
SUDLA BADED RUDI CA RISA"-CA-FOOD"
SUBCA_M3X**Sub-CA*
SUBCA_LOG=*log*
SUBCA_CSR+*CSR*
SUBCA REPO CSR EXTERNO**REPO Int SUBCA*
SUBCA LOG CLIENTS LOTE ABORT-"abort"
SUBCA LOG CLIENTS LOTE PROCESS="AP"
ATTING TO CITERINE TOFF STRADDY A STRADDY A
and a final state of the state
aven introductanta - film user
SUBLA FILENAME ALT SON ALROITS"IG FDA"
SUBCA FILENAME FET 35H KENUTE HOST-35H DOST.CONT
SUBCA_FILENDAE_TIFE_CLIENT="subcaTypeClient.conf"
SUBCA_FILENAME_STATUS_CERT_TYPE="subcaStatus.conf"
SUBCA_BASED_ON_CA+*CA_BASE*
SUBCA BASED SERVICE**SERVICE SUBCA*
#SUBCA UNIQUE SUBJECT -> UniqueSubjet = Fermite duplicados EN / Subject - DEFAULT: OFF
SUBCA UNIQUE SUBJECT-*OFF*
STRY'S NEWS STRUCT
CTRUE WINDAW WINDAW
and the second s
SURVA_INDE_CYATA* FARESV
ANNUA MANDE MANAIAVAINUT MANAIAVAINUT ANNUALANUT ANNUALA
soura anne inv a -> "veline en nombre dei tag existente en la configuración sei de la subca, para firmar el tipo de certificado correspondiente"
SUBLA RANE IAD SERVER" SETVET
SUBCA_HAME_TAG_HUNGAN="person"
SUBCA_NAME_TAG_POINT*
SUBCA_NAME_TAG_MONITORING="monitor"
8 Valores sugeridos
SUBCA ACRONYM DEFAULT=*SUBCA-CECBA*
SUBCA COUNTRIES FILE="subcaCountry.conf"
SUBCA DAYS FILE="subcaDava.conf"
SUSCA NO FILE="wheat0 conf"
ATTENTS THE SUBJECT AND A STATE AND A STAT
HIGH STRETTE THE ADDRESS CONTRACTOR IN THE CONTRACTOR MINES IN THE CONTRACTOR AND ADDRESS CONTRACTOR AND ADDRESS CONTRACTOR ADD
over-n osta zako - navena versa - navena versa - navena
SVDA VAL VAL VAL VIJA TILA "SUVSKALVUT
SUGLA REVURE REASON FILE* FUECARESSONEVORE.CONT
#SUBCA DAYS ON DEFAULT x**NN* -> Define el valor por suguerido a utilizar. Si este no existe dentro del archivo de configuracion 'CA_DAYS_FILK', se omite sin problema y no hay sugerido en el menu.
SUBCA DAYS ON DEFAULT LIST="3653"
SUBCA_DAYS_ON_DEFAULT_LIST_SERVER=*1461*
SUBCA_DAYS_ON_DEFAULT_LIST_MONITORING=*1461*
SUBCA_DAYS_OW_DEFAULT_LIST_CLIENTS="751"
SUBCA DAYS ON DEFAULT CRL=#40*
SUBCA ND ON DEFAULT=*=sha256*
SUBCA BITS OF DEFAULT=*2048*
STRICA SEVICES SEARCH ON DEFAULTERVISIONAL FIRST
denter
-weekset>

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



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

Archivo de Configuración CentralizerCert CentralizerCert SUBCA SA by Eng. MEVER
<pre>4 Corificado esteres de feriescie de feriescie de termine determine determine determine de termine de</pre>
100 0.050**core* 0.050**core
(ve) BSINTEL_BOLT=*Corts:*Cort* WEINTEL_CORT=*Cort*Cort* SINTEL_CORT_*Corts:*Cort*Cort*Cort*
<pre>(mail) (mail) Mail Mail(IIII) on is counts deads https://myscount.pools.com/lassecuremegs (-> %creat de apps mance sepura : 31 DBLT_MERAUMET*OCT counts listedent Mail DBLT_MERAUMET*OCT counts listedent Mail DBLT_MERAUMET*OCT counts listedent DBLT_DBL**counts departs listed DBLT_DBL**counts departs listed DBL**counts departs departs listed DBL**counts</pre>
caspash

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

1 (-> Configurar (por pri 2 (-> Visualizar Archivo	de Configuración
3 (-> Customizar (EDITAR)	Archivo de Configuración
4 -> Ejecutar CLIENTE de	COLLED
5 -> Enviar correc de po	ueba a matiasvz§gmail.com
e c-1 ADTAGE	
<pre><hosptar></hosptar></pre>	<cancelar></cancelar>

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

CentralizerCert SUBCA RA by Eng. NEVEN
ATENCIÓN: Esta opción configura el cliente de correo electrónico por primera vez.
¡Deres continuar con la configuración inicial de la cuenta de correc electrónico a utilizar para la distribución de certificados desde contrelisarCert?
Esto podria causar el mal funcionamiento de la cuenta, dado que sobresoribe la configuración actual, en el caso de existiera previsante.

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

CentralizerCert SUBCA	RA by Eng. MRV28
	dio>

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:

C Registración	× +		-	×
← → C ③ No	es seguro 10.10.0.104		\$	0 0 0
	Registrarse ¿Ya eres usuario? Iniciar sesión			
	Usuario			
	Correo electrónico			
	Contraseña	Confirmar contraseña		
	Registrarse			
	© 2019 <mark>[cC]</mark> - centrali	zerCert by Eng. MRVzH		

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

C Registración	× +		-	C	ב	×
	o es seguro 10.10.0.104		07	☆		:
	Registrarse ¿Ya eres usuario? Iniciar sesión					
	mvazquezhess					
	matiasvz@gmail.com					
		••••••)			
	Registrarse					
	© 2019 [cC] - centra	lizerCert by Eng. MRVzH				

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

C Registración	× +	- 🗆 X
← → C ① N	o es seguro 10.10.0.104/index.php?action=joined	०न 🚖 🕵 :
	Registrarse ¿Ya eres usuario? Iniciar sesión	
	El registro se realizó con éxito, comprueba su correo electrónico para activar su cuenta.	
	Usuario	
	Correo electrónico	
	Contraseña Confirmar contraseña	
	Registrarse	
	© 2019 [cC] - centralizerCert by Eng. MRVzH	

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

M Gmail - Confirmacion de registro X +	– 🗆 X
← → C	ch=all&permthid=thread-f%3A164873784337275029 🖈 💲 :
M Gmail	Matias R. Vazquez Hess ≺matiasvz@gmail.com≯
Confirmacion de registro 1 mensaje	
noreply@centralizercert.hq.colegio-escribanos.org.ar <noreply@centralizercert.h Para: matiasvz@gmail.com</noreply@centralizercert.h 	q.colegio-escribanos.org.ar> 29 de octubre de 2019, 11:22
Estimado usuario,	
Para activar su cuenta, haga clic en el siguiente enlace: http://centralizerCert/activa	te.php?x=101&y=4f97c723d754e4d892f4d8937063aaea
Gracias,	
[cC] centralizerCert	

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

	Inicio × +	_		×
÷	→ C ③ No es seguro 10.10.0.104/editar_usuario.php?id=1	☆	1	:
	Inicio Buscar certificado Q & Conexiones + > Seguridad +	nvazquezhess	-	
	EDITAR USUARIO			
	Usuario			
	admin			
	Contraseña			
	Correo			
	centralizercert@gmail.com			
	Administrador			
	SI			
	Perfil			
	O Operaciones			
	O Desarrollo			
	O Super Desarrollo			
	Usuano			
	Actualizar			
	© 2019 [cC] - centralizerCert by Eng. MRVzH			

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 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:

el entorno: DENO	Intermedia (Bibordinada) a gestionar
	A ROLLA
<aceptar></aceptar>	<canoelar></canoelar>

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

CentraliserCert SUBC	N I RA by Eng. 18748
Seleccionar la Autoridad Certificante	Rair a culliar para el entorno:
DEND para avanzar con la generación de	la 578-CA
23-650	2016
<aceptar></aceptar>	<cancelar></cancelar>

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

	Dian and a second se
	Dian J Man
	Dise all the state of the state
	Diss - mayor invial a 2 Means
	Dias - mayor iqual a 3 Mases
	Dias - mayor igual a 3 Meses
	Dias - mayor igual a 6 Meses
	Diag - mayor iqual a 12 Meses - mayor iqual a 1 Años
	Diss - mayor iqual a 24 Meses - mayor iqual a 2 Años
	Dias - mayor igual a 36 Meses - mayor igual a 3 Años
	Dias - mayor igual a 48 Meses - mayor igual a 4 Años
	Diss - mayor igual a 60 Meses - mayor igual a 5 Años
	Dias - mayor igual a 73 Meses - mayor igual a 6 Años
	Dias - mayor igual a 97 Meses - mayor igual a 8 Afics
3653	Dias - mayor igual a 121 Meses - mayor igual a 10 Años
	7 10 31 62 93 99 103 366 731 1095 1461 1827 2192 2922 3653

Figura 150. Paso 7 – Creación de Sub-CA

tific	ados) [Va	alor sug	erido -	60]:	
() 3	Dias	- 1 Mes			
					<mark></mark>
			igual (a 3 Mese	2
			igual (a 3 Mese	3
			igual (a 4 Mean	
			igual (a 4 Meau	
	50 Dias		igual (a 5 Meze	a
	65 Dias	- mayor	igual (a 5 Mean	

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:

C Inicio	× + - □ ×					
← → C () M	lo es seguro 10.10.0.104/info_mecanica.php 🖈 👔 :					
Resun	nen de Mecánica de funcionamiento del circuito de estados de certificados cC					
Marca	Comportamiento					
Activo	Tabla: Certs Certificado generado					
Deprecado	Tabla: Cris CRL previa a la/s ultima/s generada/s					
Eliminado	Eliminado Tabla: Certs El certificado cliente fue marcado como eliminado porque se elimino el DS asociado, no siendo que el servicio siga publicado.					
Expirado	Tabla: Certs - PENDIENTE! El certificado supero su fecha de validez y no se encuentra revocado					
	Tabla: Cris Corresponde a la ultima CRL creada y vigente, la cual puede o no encontrarse publicada					
	Tabla: Revocations El certificado fue revocado e incluido en una CRL pero aun no se encuentra publicado					
Invalido	Tabla: Revocations - PENDIENTEI El certificado es inutilizable, dado que fue incluido en una CRL y ademas se encuentra publicado					
	Obsoleto Tabla: Certs-Revocations El certificado revocado fue incluido en una CRL (se incluiye el numero de CRL que lo incorpora a partir de ahora), lo que no quiere decir que el mismo se encuentre publicado. Para verificar ello, se debe verificar la tabla revocations confirmando el campo invalido=publicado, incluido=en crl sin publicar					
	Tabla. Revocations El certificado se encuentra revocado y pendiente de incluir en una CRL					
	Tabla: Certs Certificado revocado sin incluir en CRL					
Tipos	de Certificados existentes					
	Tipo de Certificado					
	CA					
	Humano					
	Monitoreo					
	Puesto					
	SUBCA					
	© 2019 [cC] - centralizerCert by Eng. MRVzH					

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

Seleccionar el (subordinada):	CentralizerCert 308 Date Stemp de la Auto SUBCA-CECBA a gestion	CA RA by Eng. 1887281	
	Gosptary	clanoslar>	

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

I → Visualizer	ERTIFICADO Autoridad Certi Comprohado A de Santoria (EDTAR) configuración 35. A les Autoridad Certificane aliantar Autoridad Certifican abilitar Autoridad Certifica Parte Autoridad Certifica Parte Autoridad Certifica Santoria (Carta de Revocanción de totulizar) CRL Lista de Re Normalizar) CRL Lista de Re Santoria Cartino Cartifica (RETERICADOS cliente [Servido	ients Datermella (rubordinada) Cettificado factorella (nabordinada) unaziad Cettificante ilcontentia (nabordinad cettificante ilcontentia) cante Intermedia (rubordinada) cante Intermedia (rubordinada) nate Intermedia (rubordinada) (NFT) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado) Cettificado Cett
	4	(Paratan)

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

# OpenSSL SUBCA	Root configuration file	
HOME -		
RANDFILE - SENT:	::BONE/.rnd	
oid_section = ne	ev_cida	
SExtra OBJECT IS	Dentifier info	
[new_oids]		
postelAddress =	2.5.4,16	
Log 1		
default ca = Ch	default.	
[CA_default]		
# Directory and	file locations.	
gra.	***	
Cerca	* \$017/Certs	
cel_dir	= \$dir/crl	
new certs dir	- FOIL/DEVOELTS	
#unique_subject	- uo (bezarze sublecz.a unbrzcegos	
unique_subject	* 30	
Gatebase	= Pdir/index.db	
Sefiel	* solr/serial	
RADADATTE	<pre>= vair/private/.rana</pre>	
# The most her a	and most cartificate	
mrivers key	m Edit/orivara/athos hav nam	
certificate	= #dir/certs/subca.cert.crt.pem	
# for certificat	te revocation lists.	
crinumber	= \$dir/crlnumber	
crl	= \$dir/crl/subce.crl	
crl extensions	= crl_ext	
default_crl_days	s = 60	
# SHA-1 1# depre	costed, so use SH1-2 or SH1-3 instead.	
default_nd = sha	4256	
name_opt	= cs_default	
cert_opt	* CB_GETAULC	
merents dels = 3	1633	
proserve	· no	
Pervel	- lorsel"score	
	ckceptar>	

Figura 180. Paso 5 - SSL de Sub-CA

Configuracion SEL enternoi 0	HHO - SUB-CA: SUBCA-CECEA - DeteStamp: 20190722 Centes
# Optionally, specify some de	faults.
countrySame min= 2	
countrySame_max= 2	
countrySame_default = AR	
stateOrFrovinceName_default *	CABA
localityName_default = CABA	
0.organizationName_max	- 70
0.organizationName_default = commonName_max= 80	Colegio de Escribence de la Cludad de Buence Aires
commonName_default = 50BCA	Intermediate CA - nombre de SERVICIO SubCA
organizationalUnitHame_defaul	t = Computos, Operaciones
emailAddress max = 64	
emailAddress_default = pRi@co	legio-escribanos.org.ar
postalAddress_default = Las 3	eres 1833, C1127AAA
f wh with on 1	
A Paramations for a reminal in	tarmadiate (3. I'man widded config').
ShastoConstraints = oritical.	CA:FALSE
hastofinations a priving) /	Artone mathianto
Epartiana a privinal any	an a strong parameters of
subject Eavidentifier a hash	
authorituWeuldentifier = keut	dialuses, issuer
Paullance a critical, distrali	limature, pauFanishgrmant, rDLSins, baccarttion
extendedZevCsade = serverAuth	
#mrlDistributionPoints - Seri	section
subtecthitHame - Balt names	
#authorityInfoAccess * Boosp	rection
1 vs sub ca nas san 1	and a second second second second second
· excensions for a subject to	Deliveriane on I and Antry County 1.
Basicounternance - oraciona,	PAIR and a second second
fractions a critical any	Pertence' berutente
with any fault dent if inc. a hash	
authoritoWayTdestifter a key	distance design
partiana a printer distral	timatory barbarishgragan stition, barbartian
Reyonage - Criticar, ungroan	admasaras walamerhoarmans, careerdos waloareardo
or ThistributionEnints = Berl	agent Long
achterrileName - Bair sames	Para and a second se
authoritofatologaa a force a	and the
autoracylicomoutes - poorp_s	
Party Constraints - Constraints	
[crl_est]	
# Extension for CRLs ('man x3	(9v3_config).

Figura 182. Paso 7 - SSL de Sub-CA



Figura 184. Paso 9 – SSL de Sub-CA



Figura 181. Paso 6 - SSL de Sub-CA



Figura 183. Paso 8 - 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:

California evaluation for a second se	IDEAL DA by Day MOVE
«Aceptar»	«Cancelar»

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:

1 (-> Información de Discos	
2 -> Zona Horaria	
3 1-> Configurar Iona Horaria	
4 (-> Configurar Teclado	
5 -> Configurar Idioma	
6 -> Visualizar Archivo de Confi	guración CentraliserCert
7 -> Customizar (EDITAR) Archivo	de Configuración CentralizerCert
8 -> LOG CentraliserCert	
9 -> Reiniciar Equipo	
10 (-> Apagar Equipo	
11 (-> Base de Datos	
12 (-> Correo Electrónico	
13 -> Servidor WEB	
14 -> Visualizar Tareas Programad	tas [CROB's]
15 -> Customizar (EDITAR) Tareas	Programadas MANUALMENTE [CRON's]
16 <-1 Volver	
(losotar)	«Cancelar»
	"TERMONAULT

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



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

CentralizerCert SUBC ATENCIÓN: ¿Desea continuar con el BacKuP	A RA by Eng. MRVzH
centralizerCert?	

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



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

1 -> Configurar [por 2 -> Estado MySQL 3 -> Iniciar MySQL 4 -> Detemer MySQL 5 -> LOG MySQL	primera vez)
T I-> CREAN Targes Proc 5 (-> Restaurar 15 con 9 <- 1 Volver	innen (CRON) NCP DO DKP
(Aceptar>	<cancelar></cancelar>

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

2	1->	Información de Discos
2	1->	Zona Horaria
3	1->	Configurer Ione Moreria
4	1->	Configurar Teclado
5	1->	Configurar Idioma
	1->	Vigualizar Archivo de Configuración CentralizerCert
3	1->	Customirar (EDITAR) Archivo de Configuración CentralizerCer
	1->	LOG CentralizerCert
2.	1->	Reiniciar Equipo
20	1->	Apagar Squipo
22	1-5	Dane de Datos
20	125	COFFED Electronico
12	1-2	SELATOR HEB
100	1.52	VIRGALIZATE LARGES Programmings (CRONES)
20	2.1	Solver
	221	TOATEL
		and a second sec

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

Atención:	
Está a punto de regener SUBCA-CECBA basado en e	ar la CRL de la SUB-CA: 1 DS: DateStamp 20199722.
Continua con la CRL?	
288 B	<no></no>

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

🚰 roet@ccsubcar-/scripts/centralizerCent_SUBCA — 🗖	
Para mayor información, consultar el archivo: /root/scripts/centralizerCert_SUBCA/scripts//tmp/debug_audit_20190722_194912_VRCAC.log	^
> Se crea la CRL (Lista de Revocación de Certificados) SUBCA (subordinada): /root/scripts/centralizerCert_SUBCA/scripts//Sub-CA/DEMO/SUBCA-CECBA/20190722/crl/subca.cl	
Using configuration from conf/sub-ca.cnf	
OW No. Revolved Certificates	
e regenero la IRL de la SublA.	
Certificate Revocation List (CRL): Version 2 (0x1)	
Signature Algorithm: sha256%ithRSAEncryption	
Issuer: /~RAP/ST=CABB/Om-Colegio de Escribanos de la Ciudad de Buenos Aires/OU=Computos, Operaciones/CN=SUBCA Intermediate CA - nombre de SERVICIO SubCA/postalAddress=Las Heras 1833, C1127AAA	
Last Update: Jul 22 22:52:36 2019 GMT	
Next uptate: sep 20 2/15/156 2019 uni	
VRU VARUARANA	
email:pki@colegio=escribanos.org.ar	
X509v3 Authority Key Identifier:	
keyid:48:B0:4C:94:82:A6:6D:12:2C:6A:EE:96:BC:47:DD:63:SB:06:18:14	
X509v3 CRL Number:	
1	
No Revoked Certificates.	
Signature Algorithm: sha256WithRSAEncryption	
ScitorisU192/361231/91921371801401401401401401401221321 Thread 20 bits 27, 75, 75, 75, 75, 75, 75, 75, 75, 75, 7	
05:bb:e4:74:72:e8:70:d0:2b:0c:3b:0c:3b:0c:3c:8d:15c:	
f2+e1:20:67:73:91:8e:63:14:d9:6f:29:48:d2:73:fa:e0:a2:	
£7:a8:d9:83:0f:2a:3e:eb:40:26:76:d7:c6:98:a2:30:fe:a2:	
3d:41:33:cf:8c:a2:55:2a:76:31:a5:06:9d:ac:f3:53:a8:20:	
94:ca:36:57:5e:d5:63:d2:7a:b2:41:e2:07:fb:c1:8b:33:72:	
3b:41:68:47:ce:95:2b:c6:0f:7f:ca:e0:42:ce:be:	
f4:22:bb:21:73:bb:08:cb:54:b0:d1:50:4d:17:48:41:d0:bf:	
TTING1991581//1831181//1581991818315810810010010918015T1 #8:000701145:00176501726545501014650510148407	
13;a=:a=:77;d8;27;c1:5d:01;cd:07;40;a2;19:80;51;14;e1;	
0e:50:ec:eb:93:ad:72:a5:87:27:9d:64:2e:£3:9b:7a:56:60:	
3d:f9:74:41	
I> Atención: La CRL # 01 (0x01 exa 1 dec) NO incorpora certificados revocados!	
The second advantage of the second	
Verfiands on Solar Andreas and Solar Andreas and Andreas	
ATENCIÓN: La conexión a la BD ubicada en localhost en el puerto: 3306 con el usuario: cosra ha sido exitosa!	
Presione cualquier tecla para continuar	~

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

C Inicic	× +										-		×
\leftrightarrow \rightarrow	C (i) No es seguro 10.10.0.104/ver_crls.php										☆	1	:
	Inicio Buscar CRL Q	& Cone	tiones + → Se	eguridad -						mvazquezi	ness 🗸		
	CRL's existentes desde	centrali	zerCert										
	Fuente	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Serie	Тіро	Cantidad Certificados Incluidos	Marca		
	/C=AR/ST=CABA/O=Colegio de Escribanos de la Ciudad de Buenos Aires/OU=Computos, Operaciones/CN=SUBCA Intermédiate CA - nombre de SERVICIO SubCA/postalAddress=Las Héras 1833, C1127AAA	subca.crl	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO		Sep 20 22:52:36 2019 GMT	Jul 22 22:52:36 2019 GMT	1	CRL	0	2019- 07-22 19:52:36		
			© 2019 [cC] - ca	entralizerCe	ert by Eng. M	IRVzH							

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

6	Inicio	cio × +	-		×
~	\rightarrow	C O No es seguro 10.10.0.104/info_lote.php	\$	1	:
		Inicio Buscar certificado Q & Conexiones + ≻_ Seguridad +	mvazquezhess -		
		Resumen de SUBJ's sugeridos por tipo de certificado			
		Subject sugerido Tipo de Canti certificado certificado	lad Cantidad os campos ales obligatorios		
		/C=Pais (2)/ST=Provincia/L=Localidad/O=Organizacion/OU=TIPO/CN=Nombre y Apellido/SN=DNi/emailAddress=correolpostalAddress=Direccion 1234/dateOfBirth=Fecha de Humano 1 nacimiento/countryOfCitizenship=Nacioniidad/[O=Delegacion - OPCIONAL]	12		
		/C=Pais (2)/ST=Provincia/L=Localidad/O=Organizacion/OU=TIPO/CN=Puesto/SN=CUIT/emailAddress=correo/postalAddress=Direccion Puesto 1 1234/[O=Delegacion - OPCIONAL]	9		
		SUBJ's existentes y habilitados para generar lote [TIPO = Humano / Puesto	9]		
		No hay resultados!			
		© 2019 [cC] - centralizerCert by Eng. MRVzH			

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:

Contrainance of the second sec	CA 1 84 92 E02, 202762 ECO 10800 para la GESTIÓN E CENTIFICADOS CLIENTE de SECO por 1100 9 - Cado APREDUIZADO 9 - Cado APREDIZADO 9 - Cado APREDUIZADO 9 - Cado APREDUIZADO 9 - Cado APREDUIZADO 9 - Cado APREDUIZADO 9 - Cado APREDUIZADO 1 - CADO APREDU
Chospitari	Canoelaro

Figura 212. Paso 1 – Consulta de certificados cliente



Figura 213. Paso 2 - Consulta de certificados cliente

LA SUB existe inconv	A (subordinada o tiene 0 bit miente al crea) NO fue lo s, o no se r la SubCA.	ralizada! O 1 generó por al	lgún
Acción	CANCELADA			
		Acepta	•	

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:

-> Certificados existen	ntes BD (por tipo y esta	10) 207 1100)
<pre>>> Outropy Continues(IDECAD) >> Outromar(IDECAD) >> Outromar(IDECAD) >> Outromar(IDECAD) >> Outropy / Inplemen >> Publicar / Implemen >> Publicar / Implemen >> Publicar / Implemen >> Terrory Analisa <</pre>	(a) [Doi hapo] 2000er: 4 [Display] 2000er: 4 [Display] tar remotamence a demon tar nenovación CRL a demon tar nenovación CRL demota a nuevo Victual Not a coreción CRL sutomatica : novación CRL automatica ;	-Choch JERUTILAD: -CA Is en SERVICA Semunciado- No implementado! Masia en SERVICA Genunciado- No implementado! (tal Nort en SERVICA Semunciado- No implementado! remote en SERVICA Genunciado- No implementado!

Figura 215. Paso 1 – Revocar certificados cliente

Seleccion () LO	entrelizerCert SUBC ar el modo de emisi 2024 FE	A RA by Eng. HOVes
	<aceptar></aceptar>	<cancelar></cancelar>

Figura 216. Paso 2 – Revocar certificados cliente

Seleccionar el tipo () Humano () Monitoreo () Fuesto () Servidor () Todos	CentralizerCert 3000	ca 9a by Eng. NOVis /wlor superido - Jin esigner]:	
	<pre><kceptar></kceptar></pre>	<cancelar></cancelar>	

Figura 217. Paso 3 – Revocar certificados cliente

_	CentralizerCert SUBCA RA by Eng. MRVER
Ates	ción: No se pudo localizer la D8 de la SUBCA (subordinada proceder con la revocación de clientes.
A001	dn CANCELADA)
	Aceptar

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		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

Selectionar la c la SUB-CA: SUBCA 1 (-> Certifica 2 (-> Revocar C 1 -> Custonia 5 (-> Custonia 5 (-> Custonia 6 (-> Custonia 6 (-> Cenplegar 7 (-> Cenplegar 8 (-> Fublicar 9 (-> Fublicar 1 (-> Cenplegar 1 (-> Cenplegar	Conversions of the second seco	 I. WA DY TES, MONH I. WA DY TES, MON
	«Aceptar»:	«Cancelar»

Figura 219. Nuevo certificado cliente por tipo

2.8.2.17.4. Creación de Cliente: Manual – Humano²

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

(*) 10380AL (*) LOTE (*) CSR	
<pre><hoeptar></hoeptar></pre>	<cancelar></cancelar>

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

	Pia -
	Diag
	Dian - 1 Men
	Diss - mayor a 1 Mes
	Dias - mayor igual a 2 Meses
	Diam - mayor igual a 3 Meses
	Diss - mayor iqual a 3 Meses
	Dias - mayor igual a 6 Meses
	Dias - mayor igual a 12 Meses - mayor igual a 1 Años
	Dias - mayor igual a 24 Meses - mayor igual a 2 Años
	Dias - Mayor igual a 36 Meses - mayor igual a 3 Años
	Dias - mayor igual a 48 Meses - mayor igual a 4 Años
	Dias - mayor igual a 60 Meses - mayor igual a 5 Años
	Dias - mayor igual a 73 Meses - mayor igual a 6 Años
	Diss — mayor igual a 97 Meses — mayor igual a 8 Años
1 3653	Dias - mayor igual a 121 Meres - mayor igual a 10 Años

Figura 222. Paso 3 - Crear certificado cliente humano manual

Configuración general de 2 de 3	CentralizerCert Cliente para: SUB	SUBCA RA by Eng CA-CECBA del entors	. MRV2H no de: DENO bajo el DS: 20190722 -
Seleccionar la precisión () 512 bits () 1024 bits () 2036 bits () 4096 bits () 8192 bits	en bits de la cla	we del certificado	de Humano [Valor sugerido - 2048]:
	<hosptar></hosptar>		<cancelar></cancelar>

Figura 223. Paso 4 - Crear certificado cliente humano manual

Configuración general 3 de 3	de Cliente para: :	SUBCA-CECBA del entors	to dei DENO bejo el Ddi 20190722 -
Seleccionar el algorit sha254): (*) sha254 hash (*) sha254 hash () sha354 hash () sha354 hash	umo de cifrado de :	firma del certificado	de Humano [Valor superido -
	<a>choeptar>		<cancelar></cancelar>

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

Configuración común de Cliente paras el DS: 20190722 - 4 de 6	BCA RA by Eng. MRV2H SUBCA-CECBA del entorno de: DEMO bajo
Ingrese el nombre de la organización	: para el certificado Humano a emitir
<pre><hceptar></hceptar></pre>	<cancelar></cancelar>

Figura 228. Paso 9 - Crear certificado cliente humano manual

Configuración cossión de Cliente paras el DS: 20190722 - S de 6 Ingrese correo electrónico asociado tatlesrzignes1.com	BCA BA by Eng. MEVER SURCA-CECEDA del entorno de: DEMO bajo al certificado Humano a emitir
(Aceptar)	<cancelar></cancelar>

Figura 229. Paso 10 - Crear certificado cliente humano manual

Configuración común de Cliente el DS: 20190722 - 6 de 6	rt SUBCA RA by Eng. MRVzM para: SUBCA-CECBA del entorno de: DEMO bajo
Ingrese la dirección asociada e N. Gandhi 3405	l certificado Numano a emitir
<pre><koeptar></koeptar></pre>	<cancelar></cancelar>

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

Configuración comú al DS: 20190722 -	n de Cliente para: Sī € de €	JBCA-CECBA del entorno de: DEMO bejo
Ingrese la delegac fumano a emitir. D	ión correspondiente a ejar en blanco para f	e la organización para el certificado so incorporarla.
	chemptary	classelars

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

C Inicio		× +									-		×
$\leftarrow \rightarrow$	C O No es	seguro 10.10	.0.104/ver_certificados.php								☆	(2)	:
	Inicio E	Buscar certificad	io Q & Conexiones -	≻ Seguridad	-					mvazquezi	hess -	l	
	SSL Ce	rtificado	os emitidos desde cen	tralizer	Cert								
	Organización	Nombre Común	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Herencia	Serie	Тіро		
	Colegio de Escribanos de la Ciudad de Buenos Aires	CA - Colegio de Escribanos de la CABA	ca.cert.crt.pem	CA - Colegio de Escribanos de la CABA	DEMO	Activo	Jul 15 18:00:06 2029 GMT	Jul 15 18:00:06 2019 GMT	-	256	СА		
	Colegio de Escribanos de la Ciudad de Buenos Aires	SUBCA Intermediate CA - nombre de SERVICIO SubCA	subca.cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Jul 22 22:43:54 2029 GMT	Jul 22 22:43:54 2019 GMT	CA- CECBA	257	SUB-CA		
	іт	Matias Roman Vazquez Hess	persona_30406007_10588251.cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Jul 22 23:02:48 2021 GMT	Jul 22 23:02:48 2019 GMT	SUBCA- CECBA	10588251	Humano		
			© 2019 [c	C] - centralizer	Cert by En	g. MRVzH							

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:

detections is generation a settine role a different settine a different settine	ucies: SOCA: Ak y Eng. WVM a mesonic Departs in definition int CENTIFICADO CLIENTE de GO (C) (C) (C) (C) (C) (C) (C) (C)
<aceptar></aceptar>	<cancelar></cancelar>

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

Ces Seleccionar la razón por la cu Sin especificar Clave compro Sustituido/Reemplazado Puest unspecified]:	tralizerCert SUBCJ al se solicita la metida CA compro o desvinculado S	FA by Eng. NEVER revocación: metida Puesto modificado uesto Suspendido [Valor sugerido -	
 CACompromise affiliationChanged certificateMold cessationOfOperation keyCompromise superseded unspecified 			
cko	ptar>	<cancelar></cancelar>	



Atención:		
Està a punto SUBCA-CECBA b	de revocar el c asado en el DS:	liente Humano de la SUBCA: DeteStamp 20190722.
Tenga en cuer Per restaurac	ita que la opera- la a su estado aj	sión no es reversible y no podr nterior.
Continue cor	la revocación (del cliente Humano?
	1000	clina

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

🚾 Inicio	6	× +								-		×
$\leftarrow \ \rightarrow$	C ① No es s	seguro 10.10.	0.104/buscar_certificados.php?s=								*) I
	Inicio	Buscar certificad	io Q 🖉 Conexiones 🗸 🚬	Seguridad -					mva	zquezhess -		
	BUSCA	R CER	TIFICADOS									
	Organización	Nombre Común	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Herencia	Serie	Tipo	
	Colegio de Escribanos de la Ciudad de Buenos Alres	CA - Colegio de Escribanos de la CABA	ca.cert.crt.pem	CA - Colegio de Escribanos de la CABA	DEMO	Activo	Jul 15 18:00:06 2029 GMT	Jul 15 18:00:06 2019 GMT	-	256	СА	
	Colegio de Escribanos de la Ciudad de Buenos Aires	SUBCA Intermediate CA - nombre de SERVICIO SubCA	subca.cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Jul 22 22:43:54 2029 GMT	Jul 22 22:43:54 2019 GMT	CA- CECBA	257	SUB-CA	
	IT	Matias Roman Vazquez Hess	persona_30406007_10588251.cert.crt_revoke- A1905B.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO		Jul 22 23:02:48 2021 GMT	Jul 22 23:02:48 2019 GMT	SUBCA- CECBA	10588251	Humano	2
			© 2019 [cC] -	centralizerCert	by Eng. N	IRVzH						

Figura 256. Paso 15 – Revocar certificado cliente humano manual

	Inicio	,	× +											-		×
~	\rightarrow	C () No	es seguro 10.10.0.1	04/ver_revocaci	iones.php									☆	1	
		Inicio	Buscar Revocacion	nes Q	S Cor	nexiones - >_ 9	Seguridad -						mvazquez	hess 🗸		
		Certifi	cados SSL	. revoca	ados											
			Certificado		Se	ervicio	Entorno	Тіро	Situación	# Serie CRL	Número de Serie	Generación	Vencimiento	Marca		
		persona_30	0406007_10588251.ce A1905B.pem	rt.crt_revoke-	SUBCA In nombre de S	ntermediate CA - SERVICIO SubCA	DEMO	Humano			10588251	Jul 22 23:02:48 2019 GMT	Jul 22 23:02:48 2021 GMT	2019- 10-07 09:04:25		
						© 2019 [cC] - c	centralizerC	ert by Eng	. MRVzH							

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:

Seleccionar la acción a realizar sobre el entor 20190722	NO: DEMO - SUB-CA: SUBCA-CECBA - DateStamp:
 i >> Vinsilar CBSTITIANO Autorida Curifi i >> Vinsilar CBSTITIANO Autorida Curifi i >> Vinsilar CMSTIDIANO Autorida 	ants Incernedia (rebotilada) verticando Torenadia (rebotilada) botidad (verticanto Torenadia) anto Distretedia (rebotilada) anto Distretedia (rebotilada) esti (rebotilada) estificanto (rebotilada) estificanto (rebotilada) estificanto (rebotilada) estificanto (rebotilada) esti (rebotilada) esti (rebotilada) (rebotilada)
Glosptar>	<cancelar></cancelar>

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

CentralizerCert SUBCA RA by Eng. MRVAN
IMPORTANTE: El Certificado subca.cert.ort.pen, contiene los siguientes datos:
-Balyect: //OAAJ7+CABA/OHCleipid de Earthanes de la Cluded de Benrik Jares (Procepurso, Speschonor/OHCHGE). Histemediste CA - nombre de BENVICO duaCA/portalAdores-Las Heras 1835, Cli7XAA -Berail 04213 (tes) (237 (der) -Valiese: Jul 22 22:43:54 2019 (BCT -Raera: Jul 22 22:43:54 2019 (BCT
Registre

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

CentralizerCert BUBCA RA by Eng. NOVan
INFORTANTE: La CRL subca.crl con el número de serie (CLR Number): 01, contiene los siguientes datos:
-Onier (Issuer): (-OAU/IS-CABL/O-Colego de Serimon de la Ciudad de Banes Aires/O-Compues, generales/O-MONG. Insemediate (A nombre de BEVICI SaCA/persiladores-Las Ferse ISS, CIITADA - Banes de seres (CEL Banes): Seri (esc.) (1 (dec) - Auto: banes: Page 10 2010): 000 - Onie (Indes Page 10 2010): 001 - Onie (Indes Page 10 2010):

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

CentralizerCert SUBCA RA by Eng. MRV2N
Atención:
Está a punto de regenerar la CRL de la SUB-CA: SUBCA-CECBA basado en el DS: DateStamp 20190722.
¿Continua con la CRL?

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

Front@ccsubca~/scripts/centralizerCert_SUBCA	- 0 X	
> Fara mayor información, consultar el archivo: /root/scripts/centralizerCert SUBCA/scripts//tmp/debug audit RevocateClientsFromID 13 20151007 090335.log		i^
Verificando conexión a MySQL		1
ATENCIÓN: La conemión a la BD ubicada en localhost en el puerto: 3306 con el usuario: cosra ha sido emitosa!		1
Verificando conexión e MySQL		4
ATENCION: La conexión a la BD ubicada en localhost en el puerto: 3306 con el usuario: cosra ha sido exitosa!		4
Presione cualquier tecla para continuar «Lertificados revocados: La CRL actual, NO incorpora certificados revocados:		4
> La CRL bajo el número (crlNumber) fue re-generada y renombrada como /root/scripts/centralizerCert_2UNCA/scripts//Sub-CA/DEMO/SUNCA-CECBA/20191007/crl/subca.reloaded-01.crl		í.
		1
> Se crea la CRL (Lasta de Revocación de Certificados) SUSCA (subordinada): /root/scripts/centralizerCert_SUBCA/scripts//Sub-CA/DEMO/SUBCA-CECEA/Z0191007/crl/subca.crl		4
Using configuration from cont/sub-ca.cnt		1
DE: No Revoked Certificates		1
Je regenero la CVL de la SubCA.		1
Certificate Revocation List (CRL):		1
Version 2 (0x1)		4
Signature Algorithm: sha256WithRSAEmcryption		4
Issuer: /C=AR/ST=CABA/O=Colegic de Escribanos de la Ciudad de Buenos Aires/OU=Computos, Operaciones/CN=SUBCA Intermediate CA = nombre de SERVICIO SubCA/postalAddress=Las Heras 1833, C1127AAA		1
Last Update: Oct 7 12:09:21 2019 GMT		4
Next Update: Dec 6 12109121 2019 GHT		1
VK.004 Taylar Lirarariya Nawa-		4
email: hki #colorio-escribanos.org.ar		1
X509v3 Authority Key Identifier:		4
keyid:48:B0:4C:94:82:A6:6D:12:2C:6A:EE:96:BC:47:ED:63:5B:06:18:14		1
		1
X509v3 CRL Number:		4
2		4
Reverse Certificates:		1
DELANG PRIMITY FAITURE Banchaston Bata (Net 7, 13) (A:15, 2019 /2MT		4
CRI entry extension:		1
X509v3 CRL Reason Code:		4
Unspecified		1
Signature Algorithm: sha256WithRSAEncryption		4
32:e2:28:a8:1a:cf:b6:37:48:01:71:e1:d5:06:b2:41:b3:cb:		1
al:e0:44:df:cd:2d:3e:70:78:1b:f9:4d:b6:7f:65:02:b4:4d:		1
e2:15173:171 a6:151310:121071 d017b:1ee:94:1e71e2:163:1e31 db1		1
aatee state water at the state of the state		4
		4
12:11:1c:bb173:36:b3:4b:53:90:98:14:a3:42:58:17:5c:4a:		1
1a:05:1e:05:b7:92:46:b7:90:e9:d3:99:be:b5:b0:4e:0a:d1:		1
85:b1;a6:60;68:a0;28:5e:f0;40:d6:70:b8:66:f4:4b:ee:e4:		1
a2:aa:60:2f:8d:0f:61:af:e2:0f:30:1c:db:a0:ff:8b:c7:11:		4
961ac189:f91b61a019e15913f14e1f311b1f91341061931331b21		4
59:f3:02:06:9e:e6:45:a6:a4:57:e0:49:25:a7:33:dd:0f:8b:		1
Uerzularius zurealisti Sisul esi salearizzi del		4
(D):a:12410/12/11010/0014616616/16016116/10D1 6/1-4-78-4/8		1
> Certifiador revoador:		£.
		1
		1
> Tera Bayor información, consultar el archivo: /rcot/scripts/centralirerCert SUBCA/scripts//tmp/dabug audit reloadedCELEVECA 7 20191007 050921.100		1
Verificande conexión a MySQL		£.
ALIANJUST LA COMERION A LA BU UDICADA EN LOCALNOST EN EL DUETTO: 3306 CON EL USUATIO: COSTA NA SIGO EXITOSA!		£
Ana Ananania any Anna a Reina an Ionalhost an al Nuarto. 9906 con al usuario: ecera ha sido avirosal		£
Verificando conexión a MVSQL		£
ATENCIÓN: La conexión a la BD ubicada en localhost en el puerto: 3306 con el usuario: cosra ha sido exitosa!		£
Verificando comexión a MySQU		£.
ATENCION: La conexión a la BD ubicada en localhost en el puerto: 3306 con el usuario: cosra ha sido exitosa!		1

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

🚾 Inicio	× +										-	×
\leftrightarrow \rightarrow	C ① No es seguro 10.10.0.104/ver_crls.p	hp									☆	:
	Inicio Buscar CRL	Q & Cone	exiones + > ≥ S	Seguridad -						mvazquez	ness -	
	CRL's existentes desc	le central	izerCert							Cantidad		
	Fuente	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Serie	Тіро	Certificados Incluidos	Marca	
	/C=AR/ST=CABA/O=Colegio de Escribanos de la Cludad de Buenos Alres/OL=Computos, Operaciones/CN=SUBCA Intermediate CA - nombre de SERVICIO SubCA/postalAddress=Las Heras 1833, C1127AAA	subca.reloaded- 01.crl	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Deprecado	Sep 20 22:52:36 2019 GMT	Jul 22 22:52:36 2019 GMT	1	CRL	0	2019- 10-07 09:09:21	
	/C=AR/ST=CABA/O=Colegio de Escribanos de la Ciudad de Buenos Alres/OU=Computos Operaciones/CN=SUBCA Intermediate CA - nombre de SERVICIO SubCA/postalAddress=Las Heras 1833, C1127AAA	subca.crl	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO		Dec 6 12:09:21 2019 GMT	Oct 7 12:09:21 2019 GMT	2	CRL	1	2019- 10-07 09:09:21	
			© 2019 [cC] - c	centralizerC	ert by Eng. M	IRVzH						

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

💽 Inicio	× +									-	×
$\leftarrow \rightarrow$	C O No es seguro 10.10.0.104/ver_revocad	ciones.php								☆	:
	Inicio Buscar Revocaciones	Q & Conexiones - ≻ S	Seguridad -						mvazquez	hess 🗸	
	Certificados SSL revoc	ados									
	Certificado	Servicio	Entorno	Тіро	Situación	# Serie CRL	Número de Serie	Generación	Vencimiento	Marca	
	persona_30406007_10588251.cert.crt_revoke- A1905B.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Humano		0x02	10588251	Jul 22 23:02:48 2019 GMT	Jul 22 23:02:48 2021 GMT	2019- 10-07 09:09:21	
		© 2019 [cC] - (centralizerC	ert by Eng	. MRVzH						

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

🖸 Inicio		× +								-		×
$\leftarrow \ \rightarrow$	C ① No es s	seguro 10.10.	0.104/buscar_certificados.php?s=								☆ 💈	1
	Inicio	Buscar certifica	do Q & Conexiones + ≻_	Seguridad -					mv	azquezhess	•	
	BUSCA	R CER	TIFICADOS									
	Organización	Nombre Común	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Herencia	Serie	Тіро	
	Colegio de Escribanos de la Ciudad de Buenos Alres	CA - Colegio de Escribanos de la CABA	ca.cert.crt.pem	CA - Colegio de Escribanos de la CABA	DEMO	Activo	Jul 15 18:00:06 2029 GMT	Jul 15 18:00:06 2019 GMT	-	256	CA	
	Colegio de Escribanos de la Ciudad de Buenos Aires	SUBCA Intermediate CA - nombre de SERVICIO SubCA	subca.cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Jul 22 22:43:54 2029 GMT	Jul 22 22:43:54 2019 GMT	CA- CECBA	257	SUB-CA	
	IT	Matias Roman Vazquez Hess	persona_30406007_10588251.cert.crt_revoke- A1905B.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO		Jul 22 23:02:48 2021 GMT	Jul 22 23:02:48 2019 GMT	SUBCA- CECBA	10588251	Humano	
			© 2019 [cC] -	centralizerCert	by Eng. N	IRVzH						

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

Seleccionar MANUU () LOTE () CSR	el modo de emisió	n de certificados clie	nte:
	<aceptar></aceptar>	<cancelar></cancelar>	

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



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

Dia
Dies
Diss - 1 Mes
Dias - mayor a 1 Mes
Dias - mayor igual a 2 Heses
Diss - mayor iqual a 3 Meses
Dias - mayor igual a 3 Heses
Diss - mayor iqual a 6 Neses
Dias - mayor igual a 12 Meses - mayor igual a 1 Años
Dias - mayor igual a 24 Meses - mayor igual a 2 Años
Dias - mayor igual à 36 Meses - mayor igual à 3 Años
Dias - mayor igual a 48 Mases - mayor igual a 4 Años
Dias - mayor igual a 40 Meses - mayor igual a 5 Ados
Diss - mayor igual a 73 Meses - mayor igual a 6 Años
Dias - mayor igual a 97 Meses - mayor igual a 8 Años
Dias - mayor igual a 121 Neses - mayor igual a 10 Años

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

Configuración general de 2 de 3	CentralizerCert SUBCA RA by Eng Cliente para: SUBCA-CECBA del ento:	no de: DEMO bajo el DS: 20191007 -
Seleccionar la precisión 512 bite () 1024 bite () 2048 bite () 4096 bite () 8192 bite	en bits de la clave del certificad	o de Puesto [Valor sugerido - 2048]:
	<hoeptar></hoeptar>	<cancelar></cancelar>

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

Configuración general de 3 de 3	CentralizerCert SUBCA RA by Eng Cliente para: SUBCA-CECBA del entor	. MRV2H no de: DENO bajo el D3: 20191007 -
Seleccionar el algoritmo sha256]: () sha224 hash () sha224 hash () sha24 hash () sha512 hash	de cifrado de firma del certificado	de Puesto (Valor sugerido -
	<hceptar></hceptar>	<cancelar></cancelar>

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

	do Puesto a es	mitir (Valor
rugerido	- AR]:	
	Afghanistan	
() 24		
\bigcirc A	Anguilla	
	Armenia	
() A3		
() M	Angola	
	Antarctica Argentina	

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



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

Configuración común de Clien el DS: 20191007 - 3 de 6	Cert SUBCA Le para: SUBC	RA by Eng. MRV A-CECEA del ent	orno de: Di	EMO bajo	
Ingrese localidad de origen para el certificado Puesto a emitir Divez					
<aceptar< td=""><td>></td><td><cancel< td=""><td>ar></td><td></td></cancel<></td></aceptar<>	>	<cancel< td=""><td>ar></td><td></td></cancel<>	ar>		

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



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

Configuración común el DS: 20191007 - 5 Ingrese correo elec	entralizerCert SUBCA RA by de Cliente para: SUBCA-CECBA de 6 trónico asociado al certifica	Eng. HSV2H del entorno de: DEMO bajo do Puesto a emitir
	<aceptar></aceptar>	<cancelar></cancelar>

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

ngrese la dirección asociada al certificado Puesto a emitir
<aceptar> <cancelar></cancelar></aceptar>

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

C Inicio	× +		-		×
$\epsilon \rightarrow \mathbf{C}$ (i) No es se	guro 10.10.0.104/memberpage.php		☆	1	-
	Inicio Buscar certificado Q 🖉 Conextones + 🛬 Seguridad +	mvazquezhess 👻			
	Tablero de control - cC: centralizerCert				
	(112) (112) (112)				
	Gratico de torta: Certificados cC Totales Revocarlos Totales T	Gratico de barras: Certificados cC			
	9.1% 18.2% CAs Expir	idos			
	Sub-CA Ven Clientes Porve Fotomos	ncer CAs			
	13.6% Servicios Sut Tipos Clie				
	9 1% CRLs Line Distribución III				
	Distribu	ción 0 1 2 3 4			
	© 2019 [cC] - centralizerCert t	y Eng. MRVzH			

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

Inicio		× +									-
\rightarrow C	No es seguro	0 10.10.0.104	/ver_certificados.php								☆
	Inicio E	Buscar certifica	do Q ⊘ Conexiones- ≥	.seguridad₊	ert				mv	vazquezhess	
	Organización	Nombre Común	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Herencia	Serie	Тіро
	Colegio de Escribanos de la Ciudad de Buenos Aires	CA - Colegio de Escribanos de la CABA	ca.cert.crt.pem	CA - Colegio de Escribanos de la CABA	DEMO	Activo	Jul 15 18:00:06 2029 GMT	Jul 15 18:00:06 2019 GMT		256	CA
	Colegio de Escribanos de la Ciudad de Buenos Aires	SUBCA Intermediate CA - nombre de SERVICIO SubCA	subca cert.ort.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Jul 22 22:43:54 2029 GMT	Jul 22 22:43:54 2019 GMT	CA- CECBA	257	SUB-CA
	IT	Matias Roman Vazquez Hess	persona_30406007_10588251.cert.crt_revoke- A1905B.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO		Jul 22 23:02:48 2021 GMT	Jul 22 23:02:48 2019 GMT	SUBCA- CECBA	10588251	Humano
	MRVzH Inc.	Puesto 1	puesto_123456789_10588252.cert.crt.pem	SUBCA Intermediate CA - nombre de	DEMO	Activo	Oct 7 12:57:44 2021 GMT	Oct 7 12:57:44 2019 GMT	SUBCA- CECBA	10588252	Puesto

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

🖸 Inicio 🗙 +										- 🗆 ×
← → C ④ No es seguro 10.10.0.104/v	er_pfx.php									x 2 ()
	Inicio Buscar distribución	٩	ØCo	nexiones -	≥ .Segu	nisad + mvazqu	iezhess •			
	Certificados SSL	distribu	iidos (desde	e centr	alizerCert				
	Certificado	Servicio	Entorno	Tipo	de Serie	Digesto	Algoritmo	Correo Notificado	Clase	Marca
	persona_30406007_10588251.pfx	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Humano	10588251	2543ba850186a6b86cbb85cc3bc029e024eec411eeed7dd001b72dd562c3cc	SHA256	matiasvz@gmail.com	pfx	2019- 07-22 20:02:48
	puesto_123456789_10568252.ptx	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Puesto	10588252	62a8dx0c1e58eax2eb655c14bab3cc0e1f59f00fe8c581338e77fe2dc37c77c3	SHA256	matlasvz@gmail.com	pfx	2019- 10-07 09:57:45
				© 201	9 (cC) - centra	alizerCert by Eng. MRVzH				

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



Belestonar is operación a realizar sobre is SUR-AS SURA-CICRA hego el DES 2013100 1 -> Gercificados existences DE (por 14) 2 -> Bercos (Cortificados existences/ A 1 -> Cartos (COTAN) SURA-CIC (Lice 1 -> Cartos (COTAN) SURA-CIC (Lice 1 -> Cartos (COTAN) SURA-CIC (Lice 1 -> Deployar / Inglementar mereo Virtue 8 -> Publicar / Inglementar mereo Virtue 1 -> Portugant (Chel) resourcedo CL au 1 -> Portugant (Chel) resourcedo CL au 1 -> Portugant (Chel) resourcedo CL au	el encomo IDHO para la GESTIÓN DE CENTIFICADOS CLIENTE de y estado) sufirad por tipo) global dodo AFRENCILARES 10000 AFRENCILARES 100000 AFRE
(Aceptar)	<cancelar></cancelar>

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



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

Seleccionar el sipo de ce international internati	- CentralizerCert SUBCA RA by Kos ttificado a emitir: [Valor sugerid	. 1997at [- - Sin esigner]:
	<aceptar></aceptar>	<cancelar></cancelar>

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

() 1	Dia
617	Dass
() 30	Diss - 1 Mes
() 31	Dias - mayor a 1 Mes
() 62	Dias - mayor igual a 2 Meses
(2) 93	Dias - mayor igual a 3 Heses
() 99	Diss - mayor igual a 3 Meses
() 153	Dias - mayor igual a 6 Meses
() 366	Dias - mayor igual a 12 Meses - mayor igual a 1 Años
() 791	Dias - mayor igual a 24 Meses - mayor igual a 2 Años
() 1095	Dias - mayor igual a 36 Meses - mayor igual a 3 Años
() 1661	Dias - mayor igual a 48 Meses - mayor igual a 4 Años
() 1827	Dias - mayor igual a 60 Meses - mayor igual a 5 Años
() 2192	Dias - mayor igual a 73 Meses - mayor igual a 6 Años
() 2922	Diss - mayor igual a 97 Meses - mayor igual a 8 Años
() 3653	Dias - mayor igual a 121 Meses - mayor igual a 10 A5cs

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

Configuración general de 2 de 3	Ciiente para: SUBCA-CECBA del	by Eng. HRVzH entorno de: DEMO bajo el DS: 20191007 -
Selectionar la precisión () 512 bite () 1024 bite () 406 bite () 406 bite () 6162 bite	en bits de la clave del certi	ficado de Humano [Valor superido - 2048]:
	<hoeptar></hoeptar>	<cancelar></cancelar>

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:





Con CSR existente dentro del repositorio:

🛃 root@ccsu	bca:	~/script	s/centr	alizerCert	_SUBC	A/so	ripts	- 🗆 >	<
drwxr-xr-x	2	root	root	203	Oct	29	12:13	BacKuP	^
drwxr-xr-x		root	root	18	Jul	22	19:20		
-rwxrwxrwx		root	root	3600	Jul	21	15:06	launcher	
drwxr-xr-x		root	root	34	Oct	29	12:43	REPO_externo	
drwxr-xr-x		root	root	34	Oct	29	12:56	REPO_int_SUBCA	
drwxr-xr-x	14	root	root	4096	Oct	29	12:16		
drwxr-xr-x		root	root	88	Oct	29	08:00		
drwxr-xr-x		root	root		Jul	16	17:16		
drwxr-xr-x		root	root	18	Jul	22	19:43	Sub-CA	
drwxr-xr-x		root	root	18	Jul	15	14:42		
drwxr-xr-x		root	root	18	Oct	29	12:12	TERCEROS	
drwxr-xr-x		root	root	16384	Oct	29	12:47		
[root@ccsub	oca	scrip	pts]#	11	REP)_i1	nt_SUBC	CA/	
total 4									_
-rw-rr	1 :	coot 1	root :	1123 00	st 29	9 1:	2:56 PI	RU_YTZ1Y2Y_2K19.csr	
[root@ccsuk	oca	scrip	pts]#						\sim

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



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

🖉 root@ccsubca:-/scripts/centralizesCert_SUBCA/sc		×
Se selecciona certificado tipo HUMAN	NO bajo MATIAS VAZQUEZ para crear.	^
> No se encontro CN en index.db o		
> E de Serie (Serial Number) a an		
> Atención: Se detecto -multivalu Directorio de trabajo actual: /root/	um-rdn en subject activo: /C=AB/ST=Buenos Aires/L=San Higuel/O=LTDA/OD=Bumano/CH4Matias Varquer/SD=30466007/emailAdiress=matiasvz8gmail.com/postalAdiress=Belgrano 134/ /scripts/centralizerCert_UTDCA/cBd=CA/CBDA/SUTCA-ECDA/20131007	
> Se crea el certificado cliente Using configuration from /root/scrip Check that the request matches the s	firmedo por la SUBCA en /rooc/scripts/centralizerCert_SUBCA/scripts/]Sub-CA/DDDD/SUBCA-CECEA/20131007/end-user/certs/persona-CSMext_30404007_10583156.cert.crt.pem ps/centralizerCert_SUBCA/seripts//Sub-CA/DDDO/SUBCA/CECEA/20191007/cmf/sub-es.onf submature	
Signature ok		
Serial Number: 10588259 (Owa	10.00	
Validity		
Not Before: Oct 29 15:47 Not After : Jan 30 15:47	7.44 229 GMT	
Subject:		
et at aDr ProvinceName	# AK # Rushing Lives	
localityName	- San Niguel	
organizationName		
organizationalUnitName	= Runano	
commonstance email 12 dd ynger	n mart and Variginal	
postalAddress	Belgrand 13d	
X509v3 extensions:		
X509v3 Basic Constraints CA:FALSE		
Netscape Cert Type:		
SSL Client, S/MIME		
Retadape Commenti	appendix most	
X509v3 Subject Key Ident	standard Course	
5B:A8:A8:55:14:8£:EF		
X509v3 Authority Rey Ide keyid:40:B0:40:94:82 D1:Name:/C=AB/ST=CAB serial:01:01	entfrer: JähésbilozénikEikélkölefibbkaihBidéiBilé BAV-Golegio de Esribanos de la Cudad de Buenos Alres/OD-Computos, Operaciones/OD-CA - Colegio de Escribanos de la CABA/postalAdiress-Las Heras 1833, CI127AAA	
X509v3 Kev Usage: critic		
Digital Signature, S	Non Repudiation, Kay Encipherment	
X509v3 Extended Key Usag		
TLS Web Client Authe	entrotion, E-mail Protection	
CA Issuers - URIthts	users (/ocsp.colegio-escribanos.grg.sr/secba.grt	
CA Issuers - URIshtt		
OCSP - URI:https://c	odsp.colegio-escribanos.org.ar/ocsp/	
ocs# = umrinttpa://d	desp=alternative.dolegio=escribados.org.ar/desp/	
X509v3 CRL Distribution		
Full Name:		
URI:https://pki.co		
Full Name:		
URI:https://pki-al		
Certificate is to be certified until		
Write out database with 1 new entrie Data Base Opdated		

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

🖉 notl@couber_/sript/entailorCet,SBCA/soripts	-	٥	×
Data Base Updated			^
2 2013/31/31/31/31/31/31/31/31/31/31/31/31/3			
> Verificación certificado creado:			
Version: $3 (0x2)$			
Seria winner 1 1350239 (VRA19063)			
argustuit argustein sunatenvargeraton			
Validizy			
Not Before: Oct 29 15:47:44 2019 GMT			
Not After : Jan 30 15:47:44 2020 GMT			
Subject: "=AR, ST=Buenos Aires, L=San Miguel, O=LTDA, OD=Humano, CN=Matias Vazquez/emailAddress=matiasvz8gmail.com/postalAddress=Belgrano 134			
subject rubic sey into: Duble for 3 location, rankerwation			
rwate org nagotations additional golation Public-Rever (2048 bit)			
Nodulusi			
el:53:8b:57:63:c2:d6:12:4f:7diff:3b:51:36:26:			
dite:b7:ff:0e:e9:1f:00:e6:23:3f:7f:e8:23:1b:			
05:6a:04:ff:Fa:N0:4ff:30:ff:00:16:10:10:16:10:10:16:10:10:16:10:10:16:10:10:16:10:10:16:10:10:16:10:10:10:16:10:10:10:10:10:10:10:10:10:10:10:10:10:			
01153149134101483140101169122188110910219010031 14/08/15/11/06/07/47/28/08/09/16/21/08/16/01			
e8 rc010 ar 62 / 22 33 11 ar 12 / 42 16 ba 41 f G1 bb 16 3 r 51 r			
do:fb:d9:40:d0:01:c0:f0:a0:ed:45:16:01:a2:ea:			
531b5			
xRonenti essi (UxiUUU) VinDun avranti na:			
X50478 Garciantes:			
SSL Client, S/MIME			
Netroape Comment:			
UETGIIGGUU GLEARIE FERNOMAL COOL VETGIIGGUU GLEARIE FERNOMAL COOL			
501071 01051 14108178122101271641171081C31A216C1CC164178185			
X509v3 Authority Key Identifier:			
key1d:48:80:4C:94:82:A6:6D:12:2C:6A:EE:96:8C:47:DD:63:58:06:18:14			
Disfimar/C=AH/3F=CBAH/0=Colegio de Escribanos de la Ciudad de Buenos Aires/OD=Computos, Operaciones/CM=CA - Colegio de Escribanos de la CABA/postalAddress=Las Neras 1833, C1127AAA serial:01101			
X309v3 Rev Usage: critical			
Digital Signature, Non Repudiation, Key Encipherment			
713 Web Client Authentication, E-mail Protection			
Authority Information Access:			
CA issues - waintep://ourp.co.mg.co.mg.co.mg.ar/ecoa.co. CA issues - URIntsch/comp.stc.mative.co.logic=escribano.com_ar/ecobs.ct			

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

🕝 rost@ccubca~/scripts/contaileerCen_5UBCA/scripts		×
X59by Exceeded By Dags: critical TL5 Mb Cliest Automication, F-call Fortection Authority Information Access: Call Forter: Call Forter: <tr< td=""><td></td><td>^</td></tr<>		^
X309v3 CRL Distribution Points:		
Full Hase: UKihteps://pki.colegio-escribancs.org.ar/cecha.crl		
rull Mame! Wilhtchry://pki-alternative.colegio-escribanos.org.ar/cecba.crl		
Standarder Algerichen and 2000 (SSSMAnorganian L155100 (SSS101737) STORT END (STDRS 2000) EXC HER HARD Charles Construction (SSSMAnorganian) Charles Construction (SSSMAnorganian) Standarder Construction (SSSSMAnorganian) Stand		
Se creo la cadena de certificación (chain file) en //root/scripts/centralizerCert_SUSCA/scripts//Sub-CA/DEMS/SUSCA-CZCBA/20191007/end-user/public/chain.persona-CSBext_30404007_1055529.cert.crt.pem		
ner fen and forestelle particule el antice el participarte del antice el participarte del antice del forestella della d Intercone della d Intercone della d Intercone della de		

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

C Inicio × +					- C	ו	×
← → C ① No es seguro 10.10.0.104/memberpage	e.php				☆		:
Tablero de control - cC: co	entralizerCert						*
Gráfico de torta: Certificados cC	Totales Revocados Activos Por vencer CAs Sub-CA Clientes Entornos Servicios Tipos CRLs Distribución	Gráfico de barran Totales Revocados Activos Expirados Vencidos Vencidos Vencer CAs Sub-CA Clientes Entornos Servicios Tipos CRLs Distribución	s: Certificados cC	6			
	© 2019 [cC] - centralize	erCert by Eng. MRVzH					

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

M Gmail - Documentación importa: x +	נ	×
C n mail.google.com/mail/u/0?ik=74ba41d3f9&view=pt&search=all&permthid=thread-f%3A1648743235361591521&simpl=msg-f%3A1648743235361591521	(2)	:
Matias R. Vazquez Hess «matiasvz@gr	nail.c	:om>
Documentación importante - Emisión de CERTIFICADOS SSL de DEMO del servicio SUBCA Intermediate CA - nombre de SERVICIO SubCA desde el s <<< ccsubca.hq.colegio-escribanos.org.ar >>> 1 mensaje	ervi	dor
Cc: centralizerCert <centralizercert@gmail.com> 29 de octubre de 2 Para: matiasvz@gmail.com</centralizercert@gmail.com>	019, 1	2:47
Estimado/a LTDA,		
Mediante la presente, se adjunta certificado solicitado de acuerdo a los procedimientos vigentes, para el uso único e intransferible de Matías Vazquez, en su entorno de DEMO del servicio de SUBCA Intermediate CA - nor SERVICIO SUBCA.	1bre d	le
Referido a esto, se detalla a continuación los datos del mismo: - Certificado: chain persona-CSRext_30406007_10588259 cet.crt.pem - Denominación: Mattes Vazquez - Tipo: Humano - DNI: 3040607 - Dirección: Belgrano 134, San Miguel, Buenos Aires, AR - Digescio [SHA256]: 3a 1=4cea5cdol5hb790abe5edae048931254810103b6d219400063678625d526 - Validez: - >>> desde: 29-10-2019 - >>> hasta: 30-01-2020 - URL de acceso: 'URL nm'		
Atento a ello, se solicita respuesta de correcta recepción. Tenga en cuenta que la aceptación de la misma reviste en carácter de declaración jurada, confirmando la correspondencia de la información contenida. En el caso o error u omisión en los mismos, se deberá solicitar la rectificación según corresponda.	e exis	stir
IMPORTANTE: En el caso de no recepcionar acuse de recibo dentro de las 48hs hábiles de enviada la presente comunicación, el certificado adjunto será inhabilitado y el trámite deberá ser iniciado nuevamente sin excepci	ón.	
Gracias.		
Alle		
centralizerCert es una creación del Ing. Matias Vazquez Hess / Eng. MRVzH - Copyright (c) 2018 - 2019 [AR] - [cC 3_19.10.25]. Tue Oct 29 12:47:44 -03 2019		
□ chain.persona-CSRext_30406007_10588259.cert.crt.pem 6K		

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





-ocroser	re concrean dhe prisis en miss et celetitogro de pervisor (varor anderido - 1401)
0.1	Die
	Dias
	Dias - 1 Mes
	Dias - mayor a 1 Mes
	Dias - mayor igual a 2 Meses
	Dias - mayor igual a 3 Meses
	Dias - mayor igual a 3 Meses
	Dias - mayor igual a 6 Meses
	Dias - mayor igual a 12 Meses - mayor igual a 1 Años
	Dias - mayor igual a 24 Meses - mayor igual a 2 Años
	Dias - mayor igual a 36 Meses - mayor igual a 3 Años
	Diss - mayor igual a 48 Meses - mayor igual a 4 Años
	Dias - mayor igual a 60 Meses - mayor igual a 5 Años
	Dias - mayor igual a 73 Meses - mayor igual a 6 Años
	Dias - mayor igual a 97 Meses - mayor igual a 8 Años
() 3653	Dias - mayor igual a 121 Meses - mayor igual a 10 Años



Configuración general 2 de 3	de Cliente para: SUBCA-(ECEA del entorno de: DEMO bajo el DS:	20191007 -
Seleccionar la precis 2048]:	ión en bits de la clave o	iel certificado de Servidor [Valor sug	erido -
 () 512 bits () 1024 bits (*) 2048 bits () 4096 bits () 8192 bits 			
	<pre><aceptar></aceptar></pre>	<cancelar></cancelar>	

Figura 310. Paso 5 – Creación de certificado Servidor

Configuración general de 3 de 3	CentralizerCert SUBCA RA by Eng Cliente para: SUBCA-CECBA del entor	. MRV2N no de: DEMO bajo el D5: 20191007 -
Seleccionar el algoritmo : sha256]: () sha224 hash (*) sha256 hash () sha384 hash	ie cifrado de firma del certificado	de Servidor [Valor sugerido -
() sha512 hash	<pre><aceptar></aceptar></pre>	<cancelar></cancelar>

Figura 311. Paso 6 - 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

🗈 rootti (coubca-/soripti/contraliaerCon_SUBCA	- ø x
lo:ee:ab:5f:7b:05:6a:93:of:22:a5:38:b1:f6:e9:	•
4f:f7:5b:10:46:da:20:25:d5:7b:c1:bb:65:64:83:	
f3:db:e6:fe:93:46:f7:64:bc:a1:bd:2c:d0:55:ca:	
59ra9/1721b1/27rc1134147roa.99ra8/1497d148/1011	
ECIWI30:00:T0:D0:461DC:45:93:C9:07:12:r0:158:	
W///A	
X509v3 extensions:	
X509v3 Basic Constraints: critical	
CA: FALSE	
Netscape Cert Type:	
SSL Server	
Netscape Comment:	
Lettinodo Szkvikuk UJSL	
AUDYO DUDJECU MEY IDERITIETI FM-84-7-58-26-75-76-78-76-76-06-60-40-40-40-48-05-21-02-87-25-82-42	
X509v3 Authority Key Identifier:	
keyid:48:80:4C:94:82:A6:6D:12:2C:6A:EE:96:8C:47:DD:63:5B:06:18:14	
DirName:/C=AR/ST=CABA/O=Colegio de Escribanos de la Ciudad de Buenos Aires/CU=Computos, Operaciones/CN=CA - Colegio de Escribanos de la CABA/postalAddress=Las Heras 1833, C1127AAA	
serial:01:01	
X509v3 Rey Usage: critical	
Digital Signature, Non Repudiation, Key Encipherment, Kay Agreement	
XSO9v3 Extended Key Usage: critical	
TLS Web Server Authentication	
Authority Information Access:	
CA 1880279 - UKIATCHSI//OCB/CDIEGIO-BOCHOROS.CCT.	
un issuers - unintops://org-naturnia.ure.outegio-wartisens.org.ar/orgoa.cr. OPSD - IBTistration://orgo.colegioastosseria.ure.outegiar/orgoa/	
OCSP = URL:https://com-alternative.coledio-escribanos.crg.ar/ocsp/	
X309v3 CRL Distribution Points:	
Full Name:	
URI:https://pki.colegia-escribanos.org.ar/cechs.crl	
Market Martines	
ruii Mame:	
okihtepi//pri-sidensiive.coregid-esorianos.org.sr/decas.cri	
X509v5 Subject Alternative Name:	
DNS:CECBA Intermidiate CA 1, DNS:CECBA CA Intermidiate 1	
Signature Algorithm: sha256WithRSAEnoryption	
ll:25:b5:e6:e4:le:63:3a:f3:51:of:b5:e6:f2:e5:t3:	
16:39:09:d3:39:21:10:15:c1:1e:2a:c1:f8:37:09:60:e1:	
101/9100100110311031011091001041001041001/011041001030310410001 101/91041041041010110110310410001041040104010	
3h 2f + of + of + 5h - 3h + of + 45 + 45 + 45 + 45 + 46 + 7h + 7h + 0 + 10 + 10 + 10 + 10 + 10 + 10 + 10	
05:db:10:317a:5b:49:d8:83.09:20:5e:5a:27:77:76:f1:143:	
3c:58:cd:8b:65:76:9e:5b:f5:1d:ed:54:9b:8f:78:c6:c8:a1:	
bd:3c:f0:71:81:c7:f1:b4:72:5b:2e:51:f0:06:b9:50:be:ac:	
36:1d:1d:87:87:97:93:1d8:f8:71:3d:91:af:67:20:33:14:87:	
f5:6crdd:15:fcr42:68:e9:d0.16:1cr53:26:97:29:2d:db:c4:	
Seres:/Std/14%UA:AD10K1AC1A616019/1001961/011016616/	
be:bdf0f1be:fa:201b2:ree:4b171:00:rem:4d136150:0415b1cb;	
bb:00:9a:7a	
Se creo la cadena de certificación (chain file) en: /root/scripts/centralizerCert SUBCA/scripts//Sub-CA/BEMO/SUBCA-CECBA/20191007/end-user//end-user/public/chain.server.cert.pem	
> Para mayor information, consultar al archivor /rect/actions/centralise=Cert 300c2/spripca//tmp/debug audit_Eignnerve=Certificate Dm 20181007_100540.100	
Versitäendo coneston e Wykywara	
Animatriar La cuitezani a la ma dalada di la cuitata di di pueteco 3396 con el usustici costa na sido exitosari Diratone gradinate real nere constituez	
	×

Figura 320. Paso 15 - Creación de certificado Servidor



Figura 321. Paso 16 - Creación de certificado Servidor

← → C O No es seguro 10.100.104/memberp Inicio Buscar ce	igephp rillificado Q & Conexiones - 2.	Seguridad -	mvazquezhess +	¢	2 :
Inicio Buscar o	rtificado Q & Conexiones+ 2	Seguridad -	mvazquezhess 🕶		
Tablero de c	control - cC: centralizerCert				
Criffico 20%	e orac Certificados c e toras: Certificados c e de la de la de la de e de	Gráfico de barras: Certificados a C Totales Revocados Explados Par vencios Por	4 6		

Figura 322. Paso 17 - Creación de certificado Servidor

0 100				-	_							
	Organización	Nombre Común	Certificado	Servicio	Entorno	Estado	Vencimiento	Generación	Herencia	Serie	Тіро	
	Colegio de Escribanos de la Cludad de Buenos Aires	CA - Colegio de Escribanos de la CABA	ca.cert.crt.pem	CA - Colegio de Escribanos de la CABA	DEMO	Activo	Jul 15 18:00:06 2029 GMT	Jul 15 18:00:06 2019 GMT		256	СА	
	Colegio de Escribanos de la Ciudad de Buenos Aires	SUBCA Intermediate CA - nombre de SERVICIO SubCA	subca.cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Jul 22 22:43:54 2029 GMT	Jul 22 22:43:54 2019 GMT	CA- CECBA	257	SUB-CA	
	π	Matias Roman Vazquez Hess	persona_30406007_10588251.cert.crt_revoke- A1905B.pem	SUBCA Intermediate CA - nombre de SERVICIO SUBCA	DEMO	Obsoleto	Jul 22 23:02:48 2021 GMT	Jul 22 23.02:48 2019 GMT	SUBCA- CECBA	10588251	Humano	
	MRVzH Inc.	Puesto 1	puesto_123456789_10588252 cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Oct 7 12:57:44 2021 GMT	Oct 7 12:57:44 2019 GMT	SUBCA- CECBA	10588252	Puesto	
	CECBA	CECBA	server cert.crt.pem	SUBCA Intermediate CA - nombre de SERVICIO SubCA	DEMO	Activo	Oct 7 13:05:40 2023 GMT	Oct 7 13:05:40 2019 GMT	SUBCA- CECBA	10588253	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:

C Inicio × +			- 🗆 X
← → C () No es seguro 10.10.0.104/alertas.php			□ ☆ () :
Inicio Buscar certificado Q	& Conexiones → Seguridad →		mvazquezhess 👻
Alertas y potificaciones	Certificación Certificados SSL Jostribución Ý CRL's Revocación Ý Lotes F Mecànica Vencimientos SSL		
Alertas y notificaciones	E Vencimientos Internos		
Vencimientos en general	Vencimientos Externos Vencimientos Externos Vencimientos de CSR's Composición do CSR's		
20			
Externos			
Internos -1.0 -0.5 0.0	0.5 1.0		
Configuración			
Previsión de Alerta Previsión de Notificación en días en días	Correo Leyenda	Asunto Marca Usuario	Acción
5 2	matiasvz@gmail.com Estimado Administrador de cC, IM	Aviso 2019-10-25 IPORTANTE 16:58:25 mvazquezhes	ss Editar Eliminar
	© 2019 [cC] - centralizerCert by Eng. M	RVzH	

Figura 324. Alertas y Notificaciones - Configuración

💽 Inicio	× +				- 0	×
$\ \ \leftarrow \ \ \rightarrow \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	No es seguro 10.10.0.104/ver_vencimientos_externos.php				\$	1 (1)
	Inicio Buscar vencimientos EXT Q & Conexiones +	≻ Seguridad -		mvazquezhess -		
	VER VENCIMIENTOS EXTERNOS	Certificación Certificados SSL Distribución CertL's Revocación Certos Mecánica Vencimientos SSL				
	Agregar	Vencimientos Internos				
	No hay resultados!	 Pedidos de CSR's Composición de CSR's 				
	© 2019 [cC] - centralizerCert by Eng. MR	VzH			

Figura 325. Alertas y Notificaciones - Vencimientos externos

🖸 Inicio X +		- 🗆 ×
← → C ③ No es seguro 10.10.0.104/ver_vencimi	entos_externos.php	☆ 😩 :
Inicio Buscar vencimie	Agregar vencimiento	× mvazqueztiess -
	Servicio Detaile	
	NTC Validez dd/mm/aaaa	
No hay resultados!	Vencimiento do/mm/aaaa	

Figura 326. Paso 1 - Agregar Vencimiento externo

C Inicio	× +		- 0	×
$\epsilon \rightarrow C$ (A No es	seguro 10.10.0.104/ver_vencimientos_exter	nos.php	\$	1 E
	Inicio Buscar vencimientos EXT	Agregar vencimiento × mvazquezhess •		
		Servicio Servicio de ejemplo a vencer		
		Detaile Detaile del servicio de ejemplo a vencer		
	VER VENCIMIENTO	Validez 20/10/2019		
	Agregar	Vencimiento		
	No hay resultados!	31/10/2019		
		Octubre 2019 • • • dem lun. mat. mat. 30 1 2 3 4 5 7 8 9 11 13 14 15 16 17 18 20 21 22 24 25 26 27 28 29 36 31 1		

Figura 327. Paso 2 - Agregar Vencimiento externo

(© 10.10.0.104/agregar_vencimiento × +		-			×
← → × © No es seguro 10.100.104/agregar_vencimientos_externos.php					
	10.10.0.104 dice Agregado exitosamente. Aceptar				

Figura 328. Paso 3 - Agregar Vencimiento externo

	Inicio x +	-	×
\leftarrow	→ C A No es seguro 10.10.0.104/editar_alertas.php?id=92	☆	:
	Inicio Buscar certificado Q & Conexiones → > Seguridad → mvazquez	zhess -	
	EDITAR CONFIGURACION DE		
	ALERTAS Y NOTIFICACIONES		
	Previsión de Alerta en días		
	90		
	Previsión de Notificación en días		
	7		
	Correo		
	Leyenda Completa este campo		
	Estimado Administrador de CC.		
	la de		
	Asunto		
	Aviso IMPORTANTE		
	Marca		
	2019-10-25 16:58:25		
	Usuario		
	mvazquezhess		
	Actualizar		

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

- A.	(-> Información de Discos							
2	(-> Zone Horeria							
3	Configurar Zona Horaria							
4	Configurar Teclado							
5	-> Configurar Idioma							
4	-> Visualizar Archivo de Configuración CentralizerCert							
7	-> Customizar (EDITAR) Archivo de Configuración CentralizerCer							
8	-> LOG CentralizerCert							
9	-> Reiniciar Equipo							
10	(-> Apagar Equipo							
11	(-> Base de Datos							
22	(-> Correo Electrónico							
13	1-> Servidor WEB							
14	(-> Visualizar Tareas Programadas (CBON's)							
2.5	[-> Customizar (EDITAR) Tareas Programadas MANDALMENTE [CRON's]							
16	<- Volver							

Figura 338. Paso 6 - Alerta por tarea programada

B root@ccsubca:~/scripts/centralizerCert_SUBCA/scripts	-		×
0 00 */7 * * /root/scripts/centralizerCert_SUBCA/scripts//scripts/source/Check_automaticSchedule_Alerta_Notifi ~	cacion	es	^
			~

Figura 339. Paso 7 - Alerta por tarea programada

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

C Inicio × +		×
← → C ① No es seguro 10.10.0.104/alertas.php		:
Inicio Buscar certificado Q & Conexiones + ≥ Scolumento mvazquezho	ess 🔻	
Alertas y notificaciones		
Vencimientos en general		
Externos		
Internos		
0.00 0.25 0.50 0.75 1.00		
Configuración		
Previsión de Alerta Previsión de Notificación Correo Leyenda Asunto Marca Usuario Acció en días en días	n	
90 7 matiasvz@gmail.com Estimado Aviso 2019-10-25 Administrador de cC, IMPORTANTE 17:22:00 mvazquezhess Editar E	liminar	
© 2019 [cC] - centralizerCert by Eng. MRVzH		

Figura 340. Paso 8A - Alerta por tarea programada

M Gmail - Advertencia: Proceso de 🛛 🗙 🕂	-		×
← → C a mail.google.com/mail/u/0?ui=2&ik=74ba41d3f9&view=Ig&permmsgid=msg-f%3A1648397778037117612&ser=1	\$:
Matias R. Vazquez Her	ss <matiasvz(< td=""><td>@gmail.</td><td>com></td></matiasvz(<>	@gmail.	com>
Advertencia: Proceso de notificación automático de Alertas <<< ccsubca.hq.colegio-escribanos.org.ar >>> [Fri Oct 25 17:16:52 -03 2019] - Aviso IM	MPORTAN	TE	
cC: centralizerCert <centralizercert@gmail.com> 2 Para: matiasvz@gmail.com</centralizercert@gmail.com>	25 de octubre d	le 2019,	17:16
Estimado Administrador de cC,			
Existen certificados dentro de los cuales, opera su vencimiento en los próximos 90 días.			
Detalle:			
-> Vencimientos SSL detectados:			
toertificado organizacion nombre ¹ uesto tipo servicio estructo generacion serieDec			
immitoreo.cert.crt.pem CECBA Nagios Monitoreo SUBCA Intermediate CA - nombre de SERVICIO SubCA Activo DEMO Oct 30 19.00.48 2019 GMT Oct 23 19.00.48 2019 GMT 10588258			
-> Vencimientos externos agendados:			
ter terricio internali interna			
3] Servicio de ejemplo a vencer Detalle del servicio de ejemplo a vencer 2019-10-20 2019-10-31 2019-10-33 15.55.08			
1			
Para mayor mormaciono consultar el tabero de control de cu.			
centralizero tes una deacon dei ing. manas vazquez riess / Eng. mir vzn - Colyngin (C) z016 - 2019 [riv] v3_1310.25			
□ 25.10.19_1/.16.52 2K Var Descargar			

Figura 341. Paso 9A - Alerta por tarea programada

Mensaje enviado sin vencimientos próximos a operar con configuración



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



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

La accie	on solicitada	se encuer	ntra SIN 1	MPLEMENTAJ	t aún f
Acción (CANCELADA				
			Aceptar		
		- 1			

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

BIL Gentralisector FML Balescinaria (Service) estimates FUERA 1 -> Vasalises DEDuct's para CB (Peak 1 -> Canadian DEDuct's para CB (Peak 1 -> Canadian CB (Peak 1 -> Canadian CB (Peak 1 -> Canadian CB results) (Peak 1 -> Canadian CB results) (Peak 1 -> Canadian CB results) 5 -> Deployer CB (responses) (Perilinad 5 -> Deployer CB (responses) 5 -> Deployer CB (responses) 5 -> Deployer CB (responses) 7 <-> Volves	Carl Day Dev. Boys Rev 4. encoder Dev Days at Companismo Corrulness EXTERN Corrulness EXTERN Corruption External Control (Control Control) (Control Control (Control Control) (Control Control (Control EXTERN) - No Inglementado EXTERNO - No Inglementado
<pre> <&ceptar></pre>	<cancelar></cancelar>

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

💽 Inicio		× +		-		×
$\leftarrow \rightarrow$	C () No es	seguro 10.10.0.104/ver_cs	php	☆	1	:
	Inicio	Buscar certificado		-		
	CSR's	externos exis	tentes			
	Organismo	Certificado	Subject Entorno Nota M	larca		
	PRUEBA	PRU_YTZIY2Y_2K19.csr	/C=AR/ST=Buenos Aires/L=San Miguel/O=LTDA/OU=Humano/CN=Matias DEMO 11 Vazquez/SN=30406007/emailAddress=matiasvz@gmail.com/postalAddress=Belgrano 134/ 12	019- 0-29 :20:43		
			© 2019 [cC] - centralizerCert by Eng. MRVzH			

Figura 367. Paso 16 - Pedido de certificado



Figura 368. Paso 17 - Pedido de certificado

	Inicio	× +				-		×
÷	\rightarrow G	No es seguro 10.10.0.104/member	page.php			\$	1	:
	Inicic	Buscar certificado Q	🖉 Conexiones 🗸 🚬 Segu	idad≁		mvazquezhess 🗸		
	Tabl	ero de control - cC:	centralizerCert					
	Orga	nismos						
		Gráfico de torta: Certificados cC		Gráfico de barı	ras: Certificados cC			
			 Totales Revocados 	Totales Revocados				
		11.5% 19.2%	 Activos Por vencer 	Activos Expirados				
			 CAs Sub-CA 	Vencidos Por vencer				
		15.4%	 Clientes Entornos 	CAs Sub-CA				
		19.47	ServiciosTipos	Clientes Entornos				
		7.7%	 CRLs Distribución 	Tipos				
				Distribución				
				0	2 4	6		
			© 2019 [cC] - centra	alizerCert by Eng. MRVzH				

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:

(-> Visualize (-> Customize (-> General)	ar SUBJect's para CSR (Fed ar (EDITAR) SUBJect's para NUEVO CSR (Pedido Certific	ido Certificado EXTERNO) CSR (Pedido Certificado EXTERNO) ado EXTERNO)
1-> Componer	CSR recibido (Certificado	EXTERNO solicitado / pedido previamente)
<- Volver	CHURCH PARTY FAULUR	

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:

🧬 root@ccsu	bca:	~/script	ts/centr	alizerCert	_SUBC	A/so	ripts	- 0	×
drwxr-xr-x	2	root	root	203	Oct	29	12:13	BacKuP	^
drwxr-xr-x		root	root	18	Jul	22	19:20	CA-root	
-rwxrwxrwx		root	root	3600	Jul	21	15:06	launcher	
drwxr-xr-x		root	root	59	Oct	29	13:35	REPO_externo	
drwxr-xr-x		root	root	34	Oct	29	12:56	REPO_int_SUBCA	
drwxr-xr-x	14	root	root	4096	Oct	29	12:16	scripts	
drwxr-xr-x	2	root	root	88	Oct	29	08:00	sql	
drwxr-xr-x		root	root		Jul	16	17:16		
drwxr-xr-x		root	root	18	Jul	22	19:43	Sub-CA	
drwxr-xr-x		root	root	18	Jul	15	14:42	template	
drwxr-xr-x		root	root	18	Oct	29	12:12	TERCEROS	
drwxr-xr-x	2	root	root	16384	Oct	29	13:34		
[root@ccsub	ca	scrip	pts]#	11	REP()_e;	kterno/		
total 4									
-rrr		root 1	root 2	2 <u>5</u> 94 00	ct 29	9 1:	3:35 pe	ersona-CSRext_30406007_10588259.cert.crt.pem	
[root@ccsub	ca	scrip	pts]#						\sim

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

30 el entorno: DEMO del organismo:	PRUERA

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

Sin PEM existente dentro del repositorio:

CentralizerCert SUBCA RA by Eng.	MRVzH
ATENCIÓN: No existen Certificados externos el proveedor / organismo de competencia en repositorio general: /REFO_externo	remitidos por el
eAceptar2	

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

	nicio	×	+				- 0	×
← -	> C (No es seguro 10	.10.0.104/ver_composicion.php				\$	1 i
	Inicio	Buscar certifica	do Q & Conexione:	s• ≿ Segundad•			mvazquezhess •	
	Com	posicion a	e CSR's externos r	ecididos				
	Org	anismo	Certificado	DTS	Entorno	Nota	Marca	
	PR	UEBA	humano_prueba_CSR.pem	20191029_121919	DEMO		2019-10-29 13:44:03	
			© 21	019 [cC] - centralizerCert by Eng.	MRVzH			

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:

Configuración común de Cliente para: 3 el DS: 20191007 - 2 de 6 Ingrese provincia de origen para el ce	CA RA by Eng. NEV2H
<aceptar></aceptar>	<cancelar></cancelar>

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

Configuración común de Cliente para: SUBCA Configuración común de Cliente para: SUB el DS: 20191007 - 2 de 6 Ingrese el DNI / DNU sin puntos ni espac certificado Rumano a emitir	RA by Eng. HRVEH - ICA-CECEA del entorno de: DEMO bajo ilos de la persona para el
<aceptar></aceptar>	<cancelar></cancelar>

Figura 385. Validaciones varias - Text box Documento de Identidad

CentralizerCert SUBCA RA by Eng. MRVzH
ERROR: La entrada ingresada no es soportada!
Ingreso: hbgrfd siendo la mascara: [0-9]+8 con largo maximo: 8
Acción CANCELADA!
Choopen to

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	Correo	Correo electrónico		
]+\.[A-Za-z]{2,4}\$	electrónico	valido <u>z@n.l</u>		
[[:space:]]*\$ [[:alnum:]]*\$	Espacio o	No permite espacios o		
	números	números		

Tabla 3. Ejemplos de máscaras de validación en controles cC

C Registración	× +	-			×
\leftrightarrow \rightarrow C (D No es seguro 10.10.0.104	07	☆	1	:
	Registrarse ¿Ya eres usuario? Iniciar sesión				
	El nombre de usuario proporcionado está en uso.				
	mvazquezhess				
	matiasvz@gmail.com				
	Contraseña Confirmar contraseña				
	Registrarse				
	© 2019 [cC] - centralizerCert by Eng. MRVzH				

Figura 389. Validaciones varias - Nombre de usuario duplicado

C Inicio × +	-		×
← → C ▲ No es seguro 10.10.0.104/editar_alertas.php?id=92	7	۲ (£	:
EDITAR CONFIGURACION DE ALERTAS Y NOTIFICACIONES Previsión de Alerta en días			•
1	\$		
Previsión de Notificación en días El valor debe ser superior o igual a 7			۰.
7			
Correo			
matiasvz@gmail.com			
Leyenda			
Estimado Administrador de cC,			
Asunto			/
Aviso IMPORTANTE			
Marca			
2019-10-25 17:22:00			
Usuario			
mvazquezhess			
Actualizar © 2019 [cC] - centralizerCert by Eng. MRVzH			

Figura 390. Validaciones varias – Días mínimo y máximos permitidos

C Inicio	• × +	-	×
$\leftarrow \ \rightarrow$	C A No es seguro 10.10.0.104/editar_alertas.php?id=92	☆	:
	EDITAR CONFIGURACION DE ALERTAS Y NOTIFICACIONES Previsión de Alerta en días		^
	90		
	Previsión de Notificación en días		١.
	99	\$	
	Correo		
	matiasvz@gmail.com		
	Leyenda		
	Estimado Administrador de cC,	11	
	Aviso IMPORTANTE		
	Marca		
	2019-10-25 17:22:00		
	Usuario		
	mvazquezhess		
	Actualizar © 2019 [cC] - centralizerCert by Eng. MRVzH		-

Figura 391. Validaciones varias - Días mínimo y máximos permitidos

C Inici	io × +	-	×
$\leftarrow \rightarrow$	C A No es seguro 10.10.0.104/editar_alertas.php?id=92	☆	:
	EDITAR CONFIGURACION DE ALERTAS Y NOTIFICACIONES Previsión de Alerta en días		•
	90		
	Previsión de Notificación en días		۰.
	7		
	Correo		
	1		
	Leyenda Completa este campo		
	Estimado Administrador de cC,	11	
	Aviso IMPORTANTE		
	Marca		
	2019-10-25 17:22:00		
	Usuario		
	mvazquezhess		
	Actualizar © 2019 [cC] - centralizerCert by Eng. MRVzH		•

Figura 392. Validaciones varias - Campo vacío

C Inicio	• × +	-	×
$\leftarrow \rightarrow$	C A No es seguro 10.10.0.104/editar_alertas.php?id=92	☆	:
	EDITAR CONFIGURACION DE ALERTAS Y NOTIFICACIONES Previsión de Alerta en días		*
	90		
	Previsión de Notificación en días		
	7		
	Correo		
	matiasyz		
	Leyenda Estimado Administra Incluye un signo "@" en la dirección de correo electrónico. La dirección "matiasvz" no incluye el signo "@".		
	Asunto		1
	Aviso IMPORTANTE		
	Marca		
	2019-10-25 17:22:00		
	Usuario		
	mvazquezhess		
	Actualizar © 2019 [cC] - centralizerCert by Eng. MRVzH		·

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

debug_audit=2013 debug_audit=2013 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019 debug_audit=2019	011.144.00_mem_CA.log E3 0715.145.00_mem_CA.REPAG 0715.145.00_mem_CA.REPAG 0715.145.01_mem_CA.REPAG 0715.10719_VRCA.log 0715.10719_VRCA.log 0715.13954_mem_CA.log 0715.13954_mem_CA.log 0719_14033_mem_CA.log 0719_14033_mem_CA.log 0719_14033_mem_CA.log 0719_14033_mem_CA.log 0719_14033_mem_CA.log	R. K.log Llog	File File File File File File File File
	<aceptar></aceptar>	<cancelar></cancelar>	

Figura 397. Paso 3 - Auditoria y manejo de errores

AFGNIVG LOG CENTRALIZERCEFT CENTRALIZERCEFT CA BY ENG. NAVIR
Creando archivo: debug audit-20190715 145105 menu CA, con la marca: 20190715 145105
*** Inicio ***
Funcion: INICIAR
Funcion: VALIDAR_ENTORNO
>> Se seteo el path inicial/ /root/scripts/centralizerCert_CA/scripts//CA-root/
>> Be seteo el datestampi 20190715
>> Se seteo el timestamp: 195005
FUNCIONI MEDVU SALAVS
Final on Final Stream Stre
innuent interenzene miterent In
i>> Seterat Se desantiva biome de aréal SIGUT (CTRI-C / CTRI-C) par mode GLOBAL DRENE ULL activa
Funcion: RECARGA
Funcioni MENTI CA
Funcion: MENU CONFIGURACION RED
Funcioni MENU CA
Funcion: MENU_SISTEMA
Funcion: EJECUTAR_COMANDO (cat config.ini)
Funcion: MENU_SISTEMA
Funcion: MENU_CA
Funcion: MENU_SEGURIDAD
Funcioni MENU CA
Function MEMU SECURIDAD
Fundadi i Refu_aaatem
runusuni nantu_sa Funcioni affetta NF
Fundation Particles
Funcion: MENU SISTEMA
Funcioni MENU CA
Funcion: MENU SISTEMA
Funcion: EJECUTAR_COMANDO (cat config.ini)
Funcion: MENU_SISTEMA
Funcion: EDITAR_ARCHIVO
>> Se genera backup: config.ini previo a edición
>> Se edita: config.ini
Function: MENU SISTEMA
FUNCIONI NAVEGAR DIRECTORIO VISUALIZAR ARCHIVO
Funcion: EJECUTAR COMANDO (cat /root/scripts/centralizerCert Ck/scripts//tmp/debug audit-20190715 145105 menu CA.log)
<aceptar></aceptar>

Figura 398. Paso 4 - Auditoria y manejo de errores



Figura 399. Paso 5 - Auditoria y manejo de errores

intrust audis-20	191010_150640_menu_CA_REFL	ACE.log	File
Sebug audit-30	191015 133947 menu CA.log	our sou	File
Sebug audit-20	191015 133947 menu CA.log.	ENR	File
sebug_audit-20	191016_102623_menu_CA.log		File
debug multi comyfempiatelearchdadegniaeg 20190715,10005, c7584, 109 debug multi comyfempiatelearchdadegniaeg 20190715,10005, c7584, DEFLACT.log debug multi comyfempiatelearchdadegniaeg 20190715,10005, c7684, DEFLACT.log debug multi comyfempiatelearchdadegniaeg 20191015,110015, c7684, DEFLACT.log debug multi comyfempiatelearchdadegniaeg, 20191015,110015, c7684, DEFLACT.log debug multi comyfempiatelearchdadegniaeg, 20191015,110015, c7684, DEFLACT.log debug multi comyfempiatelearchdadegniaeg, 20191015,110015, c7684, DEFLACT.log			File
			File
sebug_sudit_Cr	eatech 1 20190715 150005.1	99	2118
IFF debug aud	it copyTemplateSearchAndHer	place 20190715 150005 cTSaR.log	File
IFF_debug_sod	it_copyTemplateSearchAndRep	place_20191010_182031_cTSaR.log	File

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

() 1	Dia
	Dian
	Diam - 1 Nos
	Dias - mayor a 1 Mes
	Dias - mayor igual a 2 Meses
	Dias - mayor igual a 3 Meses
	Dias - mayor iguel a 3 Meses
	Dian - mayor igual a 6 Meses
	Dias - mayor igual a 12 Meses - mayor igual a 1 Años
	Dias - mayor igual a 24 Meses - mayor igual a 2 Años
	Dias - mayor igual a 36 Neses - mayor igual a 3 Años
	Dias - mayor igual a 40 Meses - mayor igual a 4 Años
	Dias - mayor igual a 60 Meses - mayor igual a 5 Años
	Dias - mayor igual a 73 Meses - mayor igual a 6 Años
	Dias - mayor igual a 97 Meses - mayor igual a 8 Años
() 3653	Diam - mayor igual a 121 Meses - mayor igual a 10 Años

Figura 405. Paso 4 - Modo aprendizaje



Figura 406. Paso 5 - Modo aprendizaje



Figura 407. Paso 6 - Modo aprendizaje

IMPORIANTE en la BD, generación activa la serà emito Ademas, si	I Se detectó que el 1 por lo cual se advie: del Certificado si o opción de no permiti se hasta tanto no se el certificado tien	Sombre Común (CH): -Puesto 1- ya existe te que si continua, podris fallar la 11 mimmo no se escuentra revocado y está e subject duplicados, la generación no revoque el certificado involucrado, e el mismo DHI / Cuit, se pisara.
(Desea con descripto?	tinuar con la genera	tion aunque esta pueda fallar por lo
	_	1000

Figura 408. Paso 7 - Modo aprendizaje

🖉 rent@caukar./sapsi/rentsianCert.308Ck/saps
CkiPASE Cet Type Cet
Retropp Committies Cortificado CLEMER PERIO COSI.
X309v3 huljser Hwy I descilier 2014 (3416)36121(7)(7)(13)03,012(7)(66)33,120(7)(66)
Assystantisty of partition: hypiditisty-first-indepiristed birls-indepiristed fischeruseries Damimmer/CAMA/OFC-Dispice de Escribance de la Ciudad de Buence Aires/OB-Computos, Operaciones/CH-CA - Colegio de Escribance de la CABA/postalAddress-Las Meres 1853, Ciir7AAA serial/First serial/First
X1997 Rey Larger critical Digital Signery, Row Reputation, Ker Encloherment
X509v3 Extemded Key Dauge: critical
TL3 Web Claent Authentication Authoristy Information Access:
CA Issuers = URI:https://ocsp.colegio-escribanos.org.ar/cecba.crt
CA Issuers - URINttps://ocgp-alternative.collegio-escribands.org.ar/oedba.crt OC3P - URINtps://ocgs.collegio-escribands.org.ar/oedba/
0C39 - URIthtps://ocsp-alternative.colegic-escribanos.org.az/ocsp/
X309v9 CRL Distribution Points:
Pill News / (Nichtgs//glu-shegie-strikates.crg.st/ostba.crl
Pill News/ /Wintspi//pi-alternative.olegit-storikanko.org.as/oseba.ori
<pre>figurature Algorithm: #mailWeinBASMnorpyInion Ast@0.46.717 bashBashBaSMnorpyInion bipTodeLTTTmailDooldellStreetedBoorDentetEdBashEatTTBashEatTTBashEatTBa</pre>
3b (40) dub (35) 5c) (47) (47) (10) (10) (47) (47) (47) (47) (47) (47) (47) (47
96 (11) (16) (21) (21) (21) (21) (21) (21) (21) (21
07104331484364414335417413314614801011114548401451964 97104045454990201294297481115911314840101451394481014548201
414:9136:080 Se greb la cadema de certificación (chain file) en: /root/scripts/centraliserCert_SUBCA/SCREA/JO1010007/end-user//end-user/public/chain.puesto_123454789_105882460.cert.ert.pem
- 2 Ana angle Information, constants i sconiver Accessibility Accessibility (MCA Accessibility and Capital Section Sec
Mendisando operation e la DS Winne MINICOM La Concentión e la DS Winned en localhort en el puerto: 3306 con el usuario: cozza ha zido exitoza/ Diguzo: Tofé/Rece5576aeedddeff2d55275ber3555ca6474of455245bbd9bb18ff
->> Fais mayor information, computer at anothive; /coot/accipts/centraliseicer JUDGA/accipts/./rep/datog music ExportLientsCertificates 10 20101029 [152820.lpg
Marificado consido a fadoloxí Marifición i consiste a la del unicada en localhost en al puerto; 5506 con al unuario; corre ha sido exitores!
MININE I Sentificador en tapo Sente elicitoria de las des de Sente de Sen
18 Profess 14 generalis 48 PRA / Competence Analysis 16 / Coheney Press, 19 Profess 14 Profession Press, 20 Pro
Presione cuaiquier tecia para continuar

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	Тіро	
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
 - o postalAddress = 2.5.4.16 # Dirección postal
 - o serialNumber = 2.5.4.5 # Número de serie
- [ca] # Sección: CA

- o default ca = CA default # Denominación de sección CA default
- [CA default] # Sección: CA default
 - o dir = . # Ruta relativa
 - o certs = \$dir/certs # Ruta certificados
 - o crl dir = \$dir/crl # Ruta CRL
 - o new certs dir = \$dir/newcerts # Ruta certificados firmados
 - o database = \$dir/index.db # Archivo Base de Datos ssl
 - o serial = \$dir/serial # Archivo serial
 - o RANDFILE = \$dir/private/.rand # Archivo pseudo aleatorio leer /
 escribir
 - o private_key = \$dir/private/puesto.key.pem # Archivo clave
 privada
 - o certificate = \$dir/certs/puesto.cert.pem # Archivo de certificado
 - o default_md = sha384 # Algoritmo de cifrado de firma por defecto
 - o name_opt = ca_default # Define la forma en que el nombre del certificado se verá antes de firmar
 - o cert_opt = ca_default # Define la forma en que la información del certificado se verá antes de firmar
 - o default_days = 732 # Días por defecto de vida predeterminados del certificado
 - o 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
 - o countryName = match # Campo obligatorio
 - o stateOrProvinceName = match # Campo obligatorio
 - o organizationName = match # Campo obligatorio
 - o organizationalUnitName = optional # Campo opcional (no obligatorio)
 - o commonName = supplied # Campo necesario
 - o emailAddress = match # Campo obligatorio
 - o postalAddress = match # Campo obligatorio
 - o serialNumber = match # Campo obligatorio
- [req] # Sección: req Solicitud de certificado (CSR)
 - o default bits = 4096 # Tamaño predeterminado de bits para la clave
 - o distinguished_name = req_distinguished_name # Denominación
 de sección DN

- o string mask = utf8only # Definición del tipo de cadenas a aceptar
- o default md = sha384 # Algoritmo de hash
- o 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
 - o countryName min = 2 # Tamaño máximo de país predeterminado
 - o countryName max = 2 # Tamaño mínimo de país predeterminado
 - o countryName = Pais (Codigo de 2 letras ISO 3166) # Nombre
 del país
 - o stateOrProvinceName = Provincia # Provincia
 - o localityName = Localidad # Localidad
 - o 0.organizationName = Nombre de la Organizacion # Nombre de la organización
 - o organizationalUnitName = Tipo de certificado # Tipo de
 certificado
 - o commonName = Nombre del PUESTO # Nombre del certificado
 - o emailAddress = Email # Correo electrónico
 - o postalAddress = Dirección # Dirección postal
 - o serialNumber = C.U.I.T. (sin puntos ni guiones) # CUIT de la
 organización
 - o countryName_default = AR # Valor predeterminado de país
 - o stateOrProvinceName_default = CABA # Valor predeterminado de
 provincia
 - o localityName_default = CABA # Valor predeterminado de localidad
 - o 0.organizationName_default = Organizacion # Valor
 predeterminado de Organización
 - o organizationalUnitName_default = Puesto # Valor predeterminado
 de área o departamento
 - o emailAddress_default = correo # Valor predeterminado de correo
 electrónico
 - o postalAddress_default = Direccion # Valor predeterminado de dirección postal
- [usr_cert_point_has_san] # Sección: x509v3 [16] con parametrización del certificado a firmar
 - o basicConstraints = CA:FALSE # Indica que el certificado no podrá ser utilizado como CA
 - o nsCertType = client # Tipo de certificado

- o nsComment = "POINT client Certificate to centralizerCert"
 # Comentario del certificado
- o subjectKeyIdentifier = hash # Método de identificación de llave
 publica
- o authorityKeyIdentifier = keyid,issuer # Forma de identificación
 de llave publica
- o keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment # Uso de clave
- o 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_copyTemplateSea rchAndReplace" # 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
 - o SUBCA_COUNTRIES_FILE="subcaCountry.conf" # Archivo países
 - o SUBCA_DAYS_FILE="subcaDays.conf" # Archivo días
 - o SUBCA MD FILE="subcaMD.conf" # Archivo cifrado
 - o SUBCA_BITS_FILE="subcaBits.conf" # Archivo bits
 - o SUBCA_CRL_DAYS_FILE="subcaCRL.conf" # Archivo días
 - o 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
- o SUBCA_REVOKE_REASON_ON_DEFAULT="unspecified" # Razón de revocación sugerida por defecto
- o 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
- o SUBCA_ORGANIZATION_NAME_DEFAULT="Colegio de Escribanos de la Ciudad de Buenos Aires" # Organización sugerido por defecto
- o 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
- o SUBCA_EMAIL_ADDRESS_DEFAULT="pki@colegioescribanos.org.ar" # Correo sugerido por defecto
- SUBCA_POSTAL_ADDRESS_DEFAULT="Las Heras 1833, C1127AAA" #
 Dirección sugerida por defecto
- o SUBCA_DNS_PRIMARY_DEFAULT="CECBA Intermidiate CA 1" # DNS
 primario sugerido por defecto
- o SUBCA_DNS_SECONDARY_DEFAULT="CECBA CA Intermidiate 1" #
 DNS secundario sugerido por defecto
- SUBCA_URI_CRL_PRIMARY_DEFAULT="https://pki.colegioescribanos.org.ar/cecba.crl" # CRL primaria sugerida por defecto
- SUBCA_URI_CRL_SECONDARY_DEFAULT="https://pkialternative.colegio-escribanos.org.ar/cecba.crl" # CRL secundaria sugerida por defecto

- SUBCA_URI_OCSP_CRT_PRIMARY_DEFAULT="https://ocsp.coleg io-escribanos.org.ar/cecba.crt" # CRT primario sugerido por defecto
- SUBCA_URI_OCSP_CRT_SECONDARY_DEFAULT="https://ocspalternative.colegio-escribanos.org.ar/cecba.crt" # CRT secundario sugerido por defecto
- SUBCA_URI_OCSP_PRIMARY_DEFAULT="https://ocsp.colegioescribanos.org.ar/ocsp/" # OCSP primario sugerido por defecto
- o SUBCA_URI_OCSP_SECONDARY_DEFAULT="https://ocspalternative.colegio-escribanos.org.ar/ocsp/" # OCSP secundario sugerido por defecto
- SUBCA_SERIAL_NUMBER="A1905B" # Número de serie hexadecimal de inicio
- o 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 --
 - o RA APPLICATION PREFIX="" # Prefijo
 - o RA APPLICATION MSK="applicacion" # Mascara
 - o RA APPLICATION NAME="Aplication" # Nombre
- #--- Certificados externos de facturación electrónica --
 - o RA_ELECTRONIC_BILLING_PREFIX="" # Prefijo
 - o RA ELECTRONIC BILLING MSK="facElectronica"#Mascara
 - o RA ELECTRONIC BILLING NAME="Facturacion" # Nombre
- #--- Certificados externos de servidor --
 - o RA SERVER PREFIX=""# Prefijo
 - o RA_SERVER_MSK="servidor" # Mascara
 - o RA SERVER NAME="Servidor" # Nombre
- #--- Certificados externos de validación de dominios (wildcard)--
 - o RA_DOMAIN_VALIDATION_PREFIX="" # Prefijo
 - o RA_DOMAIN_VALIDATION_MSK="validaDominio" # Mascara

- o RA_DOMAIN_VALIDATION_NAME="Validacion" # Nombre
- #---REPOSITORIO EXTERNO DE CERTIFICADOS RECIBIDOS DE ORGANISMOS / PROVEEDORES...
 - o 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:58 7/"#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:

P root@ccca-/scripts/centralizerCent	-	o x	
(rootBoca entralize/Grt)8 pwd //root/entral/ie/ontralize/Grt			^
[rootBocca centralizerCert]# 11			
torel 24			
winararara ta toto toto u do va a ta			
INATURINA I DOG DOG DOT 5718 JUL 24 17:39 FELERE CELTALIZATORIO			
drwar-ar-x 7 root root 253 Oct 17 18:20 Releases CORE old			
drwxr-xr-x 4 root root 53 Jul 15 14:42 SUBCA core			
<pre>[root@ccca centralizerCert]# ./release centralizerCert core</pre>			
****** -> INICIO: Proceso de control de fuentes / versiones (releases) del CORE de CentralizerCert - Procesado: 18.21.01 <- *****			
ATENCION: Se requiere interacción:			
iste script permite seleccionar las acciones a realizar sobre el toxi de centralizercert (CA y SubtA core)			
Para mayor informacion, consultar al proveedor.			
Presione [Enter] para continuar / CTRL + C para cancelar.			
Selectionar La option correspondiente dentro de Las acciones disponibles a ejecutar sobre el CONZ de CentralizerCert:			
1. Generar Nelsens cons de CentralizerCert CA para control de Versiones (manuales)			
a. Obietas Alisando Cono de Centrassectoro Josefa para contras de versacines (mandastes) a. SITO			
Ingresar opción a ejecutar: 2			
Generar RELEASE CORE de CentralizerCert SUBCA			
Se creo el directorio: /root/scripts/centralizerCert/Releases_CORE_old/SUBCA_core_V3_19.10.17_17.10.2019_18.21.00 con los funentes del CORE V3_19.10.17 para mantener el control de version			
Fara ejecular una version anterior del CORE en casó de ser necesario, se debera tener en cuenta que cualquier accion se basa en tomar los fuentes del path /root/scripts/centralizerCert/Ch	core o	0 /root/	
seripts/dentralizerCert/Subtx Core de la ditima version disponible.			
*****1-> FIN: Process de control de fuentes / versiones (velesses) del CORE de CentralizerCert - Processado: 18.71.05 <- ******			
Iront@ccca_centralizerCertl#			~

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_copyTemplateSea rchAndReplace"
- 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.colegioescribanos.org.ar/queCRL"
- CA_URI_OCSP_CRT_DEFAULT="https://ocsp.colegioescribanos.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]
•
     o postalAddress = 2.5.4.16
     o serialNumber = 2.5.4.5
     o dateOfBirth = 1.3.6.1.5.5.7.9.1
     o countryOfCitizenship = 1.3.6.1.5.5.7.9.4
 [ ca ]
     o default ca = CA default
  [ CA default ]
     o dir = .
     o certs = $dir/certs
     o crl dir = $dir/crl
     o new_certs_dir = $dir/newcerts
     o database = $dir/index.db
     o serial = $dir/serial
     o RANDFILE = $dir/private/.rand
     o private key = $dir/private/persona.key.pem
     o certificate = $dir/certs/persona.cert.pem
     o default md = sha384
     o name opt = ca default
     o cert opt = ca default
     o default days = 732
     o preserve = no
     o policy = policy match
  [ policy_match ]
     o countryName = match
     o stateOrProvinceName = match
     o organizationName = match
     o organizationalUnitName = optional
     o commonName = supplied
     o emailAddress = match
```

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

o 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]
 - o postalAddress = 2.5.4.16
- [ca]
 - o default_ca = CA_default
- [CA_default]
 - o dir = .
 - o certs = \$dir/certs
 - o crl_dir = \$dir/crl
 - o new_certs_dir = \$dir/newcerts
 - o unique_subject = no
 - o database = \$dir/index.db
 - o serial = \$dir/serial
 - o RANDFILE = \$dir/private/.rand
 - o private_key = \$dir/private/server.key.pem
 - o certificate = \$dir/certs/server.cert.crt.pem
 - o default md = sha384
 - o name opt = ca default
 - o cert opt = ca default
 - o default_days = 1095
 - o preserve = no
 - o policy = policy_loose
- [policy_strict]
 - o countryName = match
 - o stateOrProvinceName = match
 - o organizationName = match
 - o organizationalUnitName = optional
 - o commonName = supplied
 - o emailAddress = optional
 - o postalAddress = optional
- [policy_loose]
 - o countryName = optional
 - o stateOrProvinceName = optional
 - o localityName = optional
 - o organizationName = optional

	0	organizationalUnitName = optional
	0	commonName = supplied
	0	emailAddress = optional
	0	postalAddress = optional
[req]
	0	default_bits = 4096
	0	distinguished_name = req_distinguished_name
	0	<pre>string_mask = utf8only</pre>
	0	default_md = sha384
	0	x509_extensions = server_cert_has_san
[req_	_distinguished_name]
	0	<pre>countryName_min = 2</pre>
	0	<pre>countryName_max = 2</pre>
	0	countryName = Pais (Codigo de 2 letras ISO 3166)
	0	stateOrProvinceName = Provincia
	0	localityName = Localidad
	0	0.organizationName = Nombre de la Organizacion
	0	organizationalUnitName = Tipo de certificado
	0	commonName = Nombre del Servidor (url)
	0	emailAddress = Email
	0	postalAddress = Direccion
	0	countryName_min = 2
	0	countryName_max = 2
	0	countryName_default = AR
	0	<pre>stateOrProvinceName_default = CABA</pre>
	0	<pre>localityName_default = CABA</pre>
	0	0.organizationName_default = Colegio de Escribanos de la
		Ciudad de Buenos Aires
	0	<pre>commonName_default = *.colegio-escribanos.org.ar</pre>
	0	organizationalUnitName_default = Servidor
	0	<pre>emailAddress_default = pki@colegio-escribanos.org.ar</pre>
	0	postalAddress_default = Las Heras 1833, C1127AAA
[serv	ver_cert_has_san]
	0	<pre>basicConstraints = CA:FALSE</pre>
	0	nsCertType = server
	0	<pre>nsComment = "Server Certificate to centralizerCert"</pre>
	0	<pre>subjectKeyIdentifier = hash</pre>
	0	<pre>authorityKeyIdentifier = keyid,issuer:always</pre>
	0	<pre>keyUsage = critical, digitalSignature, keyEncipherment</pre>
	0	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]
 - o postalAddress = 2.5.4.16
- [ca]
 - o default_ca = CA_default
- [CA_default]
 - o dir = .
 - o certs = \$dir/certs
 - o crl_dir = \$dir/crl
 - o new_certs_dir = \$dir/newcerts
 - o unique_subject = no
 - o database = \$dir/index.db
 - o serial = \$dir/serial
 - o RANDFILE = \$dir/private/.rand
 - o private key = \$dir/private/monitoreo.key.pem
 - o certificate = \$dir/certs/monitoreo.cert.crt.pem
 - o default md = sha384
 - o name_opt = ca_default
 - o cert opt = ca default
 - o default_days = 1095
 - o preserve = no
 - o policy = policy_loose
- [policy_strict]
 - o countryName = match
 - o stateOrProvinceName = match
 - o organizationName = match
 - o organizationalUnitName = optional
 - o commonName = supplied
 - o postalAddress = optional
- [policy_loose]
 - o countryName = optional
 - o stateOrProvinceName = optional
 - o localityName = optional
 - o organizationName = optional
 - o organizationalUnitName = optional

	0	commonName = supplied
	0	postalAddress = optional
[req]
	0	default_bits = 4096
	0	distinguished_name = req_distinguished_name
	0	<pre>string_mask = utf8only</pre>
	0	default_md = sha384
	0	x509_extensions = monitoreo_cert_has_san
[req_	_distinguished_name]
	0	countryName = Pais (Codigo de 2 letras ISO 3166)
	0	stateOrProvinceName = Provincia
	0	localityName = Localidad
	0	0.organizationName = Nombre de la Organizacion
	0	organizationalUnitName = Tipo de certificado
	0	commonName = Nombre del servicio de monitoreo
	0	postalAddress = Direccion
	0	countryName_min = 2
	0	countryName_max = 2
	0	countryName_default = AR
	0	<pre>stateOrProvinceName_default = CABA</pre>
	0	localityName_default = CABA
	0	0.organizationName_max = 70
	0	0.organizationName_default = Colegio de Escribanos de la
		Ciudad de Buenos Aires
	0	commonName_max = 80
	0	commonName_default = Servicio de Monitoreo de SSL Web
	0	organizationalUnitName_default = Monitoreo
	0	postalAddress_default = Las Heras 1833, C1127AAA
[moni	itoreo_cert_has_san]
	0	basicConstraints = CA:FALSE
	0	nsCertType = client
	0	<pre>nsComment = "Monitoring Certificate to centralizerCert"</pre>
	0	subjectKeyIdentifier = hash
	0	<pre>authorityKeyIdentifier = keyid,issuer:always</pre>
	0	<pre>keyUsage = critical, digitalSignature, keyEncipherment</pre>
	0	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]
 - o postalAddress = 2.5.4.16
- [ca]
 - o default_ca = CA_default
- [CA_default]
 - o dir = .
 - o certs = \$dir/certs
 - o crl dir = \$dir/crl
 - o new certs dir = \$dir/newcerts
 - o unique_subject = no
 - o database = \$dir/index.db
 - o serial = \$dir/serial
 - o RANDFILE = \$dir/private/.rand
 - o private_key = \$dir/private/subca.key.pem
 - o certificate = \$dir/certs/subca.cert.crt.pem
 - o crlnumber = \$dir/crlnumber
 - o crl = \$dir/crl/subca.crl
 - o crl_extensions = crl_ext
 - o default_crl_days = 60
 - o default_md = sha384
 - o name opt = ca default
 - o cert_opt = ca_default
 - o default_days = 3653
 - o preserve = no
 - o policy = policy_loose
- [policy_strict]
 - o countryName = match
 - o stateOrProvinceName = match
 - o organizationName = match
 - o organizationalUnitName = optional
 - o commonName = supplied
 - o emailAddress = optional
 - o postalAddress = optional
- [policy_loose]
 - o countryName = optional
 - o stateOrProvinceName = optional
 - o localityName = optional

	0	organizationName = optional
	0	organizationalUnitName = optional
	0	commonName = supplied
	0	emailAddress = optional
	0	postalAddress = optional
[req]
	0	default_bits = 4096
	0	distinguished_name = req_distinguished_name
	0	string_mask = utf8only
	0	default_md = sha384
	0	x509_extensions = v3_sub_ca_has_san
[req	_distinguished_name]
	0	countryName = Pais (Codigo de 2 letras ISO 3166)
	0	stateOrProvinceName = Provincia
	0	localityName = Localidad
	0	0.organizationName = Nombre de la Organizacion
	0	organizationalUnitName = Departamento
	0	commonName = Nombre
	0	emailAddress = Email
	0	postalAddress = Direccion
	0	<pre>countryName_min = 2</pre>
	0	countryName_max = 2
	0	countryName_default = AR
	0	<pre>stateOrProvinceName_default = CABA</pre>
	0	localityName_default = CABA
	0	0.organizationName_max = 70
	0	0.organizationName_default = Colegio de Escribanos de la
		Ciudad de Buenos Aires
	0	<pre>commonName_max = 80</pre>
	0	<pre>commonName_default = SubCA nombre de SERVICIO SUB-CA</pre>
	0	<pre>organizationalUnitName_default = Computos, Operaciones</pre>
	0	emailAddress_max = 64
	0	<pre>emailAddress_default = pki@colegio-escribanos.org.ar</pre>
	0	postalAddress_default = Las Heras 1833, C1127AAA
[v3_s	sub_ca_has_san]
	0	<pre>basicConstraints = critical,CA:FALSE</pre>
	0	<pre>subjectKeyIdentifier = hash</pre>
	0	<pre>authorityKeyIdentifier = keyid:always,issuer</pre>
	0	<pre>keyUsage = critical, digitalSignature, keyEncipherment,</pre>
		cRLSign, keyCertSign

o extendedKeyUsage = serverAuth

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

- o crlDistributionPoints = @crl section
- [point]
 - o basicConstraints = CA:FALSE
 - o nsCertType = client, email
 - o nsComment = "Certificado CLIENTE PUESTO CCSSL"
 - o subjectKeyIdentifier = hash
 - o authorityKeyIdentifier = keyid:always, issuer:always
 - o keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
 - o extendedKeyUsage = critical, clientAuth
 - o authorityInfoAccess = @ocsp_section
 - o crlDistributionPoints = @crl_section
- [monitor]
 - o basicConstraints = CA:FALSE
 - o nsCertType = client
 - o nsComment = "Certificado MONITOREO CCSSL"
 - o subjectKeyIdentifier = hash
 - o authorityKeyIdentifier = keyid:always, issuer:always
 - o keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
 - o extendedKeyUsage = critical, clientAuth
 - o authorityInfoAccess = @ocsp_section
 - o crlDistributionPoints = @crl_section
- [server]
 - o basicConstraints = critical, CA:FALSE
 - o nsCertType = server
 - o nsComment = "Certificado SERVIDOR CCSSL"
 - o subjectKeyIdentifier = hash
 - o authorityKeyIdentifier = keyid,issuer:always
 - o keyUsage = critical, digitalSignature, keyEncipherment, keyAgreement, nonRepudiation
 - o extendedKeyUsage = critical, serverAuth
 - o authorityInfoAccess = @ocsp section
 - o crlDistributionPoints = @crl_section
 - o 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]
 - o postalAddress = 2.5.4.16
- [ca]
 - o default_ca = CA_default
- [CA_default]
 - o dir = .
 - o certs = \$dir/certs
 - o crl_dir = \$dir/crl
 - o new certs dir = \$dir/newcerts
 - o unique_subject = yes
 - o database = \$dir/index.db
 - o serial = \$dir/serial
 - o RANDFILE = \$dir/private/.rand
 - o private_key = \$dir/private/ca.key.pem
 - o certificate = \$dir/certs/ca.cert.crt.pem
 - o crlnumber = \$dir/crlnumber
 - o crl = \$dir/crl/ca.crl
 - o crl_extensions = crl_ext
 - o default_crl_days = 30
 - o default_md = sha384
 - o name opt = ca default
 - o cert_opt = ca_default
 - o default days = 6570
 - o preserve = no
 - o policy = policy_strict
- [policy_strict]
 - o countryName = match
 - o stateOrProvinceName = match
 - o organizationName = match
 - o organizationalUnitName = optional
 - o commonName = supplied
 - o emailAddress = optional
 - o postalAddress = optional
- [req]
 - o default_bits = 4096
 - o distinguished_name = req_distinguished_name
 - o string_mask = utf8only

- o default md = sha384
- o x509_extensions = v3_ca
- [req_distinguished_name]
 - o countryName = Pais (Codigo de 2 letras ISO 3166)
 - o stateOrProvinceName = Provincia
 - o localityName = Localidad
 - o 0.organizationName = Nombre de la Organizacion
 - o organizationalUnitName = Departamento
 - o commonName = Nombre
 - o emailAddress = Email
 - o postalAddress = Direccion
 - o countryName_min = 2
 - o countryName_max = 2
 - o countryName_default = AR
 - o stateOrProvinceName_default = CABA
 - o localityName_default = CABA
 - o 0.organizationName_default = Colegio de Escribanos de la Ciudad de Buenos Aires
 - o commonName_default = CA CECBA
 - o organizationalUnitName_default = Computos, Operaciones
 - o emailAddress_default = pki@colegio-escribanos.org.ar
 - o postalAddress_default = Las Heras 1833, C1127AAA
- [v3_ca_has_san]
 - o subjectKeyIdentifier = hash
 - o authorityKeyIdentifier = keyid:always,issuer
 - o basicConstraints = critical, CA:true
 - o keyUsage = critical, digitalSignature, cRLSign, keyCertSign
 - o subjectAltName = email:move
- [v3_sub_ca_has_san]
 - o basicConstraints = critical,CA:TRUE,pathlen:0
 - o subjectKeyIdentifier = hash
 - o authorityKeyIdentifier = keyid:always,issuer
 - o keyUsage = critical, digitalSignature, keyEncipherment, cRLSign, keyCertSign
 - o 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
Figure 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 30. Paso $13 - $ Creación de CA	26
Figure 41 Pase 14 Creación de CA	20
Figura 42 Paso 15 Creación de CA	20
Figura 42. Paso 16 - Creación de CA	20
Figura 43. Faso 10 – Creación de CA	21
Figure 45. Pase 19 - Creación de CA	27
Figura 45. Faso 16 – Creación de CA	27
Figure 47, Deep 20 Crossión de CA	21
Figure 49 Deep 21 Crossión de CA	21
FIGURA 40. FASU 21 - DIEACIUII DE DA	∠ŏ 20
Figura 49. Paso 22 – Greación de CA	28 20
Figura 50. Paso 23 – Greación de CA	28
Figura 51. Paso 24 – Creacion 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 – Depuncia de vinculo remoto desde cC CA	32
Figura 64. Paso 2 – Depuncia de vinculo remoto desde cC CA	32
Figura 65, Paso 3 – Denuncia de vinculo remoto desde co CA	32
Figura 66. Paso 4 – Depuncia de vinculo remoto desde co CA	. JZ 22
Figura 66. Paso 4 – Denuncia de vinculo remoto desde co CA	. 3Z
Figura 67. Paso 5 – Denuncia de vinculo remoto desde cC CA	. 32
Figura 68. Paso 6 – Denuncia de vinculo remoto desde cu 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
Figure 94 Paso 3 – Salir de cC CA	37
Figure 95. Paso 1 — Pre requisites de cC Sub-CA	20
Figura 96, Paso 2 – Pre requisitos de cC Sub-CA	20
Figura 90. Faso 2 – Fie lequisitos de cC Sub-CA	20
Figura 97. Faso 5 – Fie requisitos de CC Sub-CA	. 30 20
Figura 90. Paso 4 – Fie requisitos de CC Sub-CA	. 30 20
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 – Configuracion global pre existente cC Sub-CA RA	39
Figura 103. Paso 2 – Configuracion 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 – Contiguración global pre existente cC Sub-CA RA	40
Figura 106. Paso 5 – Configuración global pre existente cC Sub-CA RA	. 41
Figure 107 Paso 6 Configuración global pre existente of Sub-CA PA	. 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
Figure 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
Figure 132 Paso 6 – Servidor web cC Sub-CA RA – Access usuario sin privilegios	40 40
Figura 133 Paso 7 – Servidor web cC Sub-CA RA – Acceso usuario administrador	40 40
Figure 134 Paso 8 – Servidor web cC Sub-CA RA – Acerca de cC	50
Figure 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 130, 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 54 – Consulta de CA's disponibles desde RA	52
Figure 142 Paso 5R – Consulta de CA's disponibles desde RA	52
Figura 143, Paso 6 – Consulta de CA's disponibles desde RA	53
Figure 144. Paso 1 – Creación de Sub-CA	53
Figure 144. Laso $1 - \text{Creación de Sub-CA}$	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
Figure 140, Paso 6 – Creación de Sub-CA	54
Figure 150, Paso 7 – Creación de Sub-CA.	54
Figura 150. Paso 8 Creación de Sub-CA	54
Figura 151. Paso 0 – Creación de Sub-CA	54
	. 54
- Elduro 162 Doco 10 - Croocion do Sub (1)	66
Figura 153. Paso 10 – Creación de Sub-CA.	. 55
Figura 153. Paso 10 – Creación de Sub-CA Figura 154. Paso 11 – Creación de Sub-CA	. 55
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 12 – Creación de Sub-CA	. 55 . 55 . 55 . 55
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	55 55 55 55 55
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.	55 55 55 55 55 55
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 150. Paso 16 – Creación de Sub-CA	55 55 55 55 55 55 55
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 159. Paso 16 – Creación de Sub-CA	55 55 55 55 55 55 55 55 56
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	55 55 55 55 55 55 55 55 56 56
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 161. Paso 18 – Creación de Sub-CA	55 55 55 55 55 55 55 56 56 56
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 162. Paso 20 – Creación de Sub-CA	55 55 55 55 55 55 55 56 56 56 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
Figure 181 Paso $6 - SSI de Sub-CA$	61
Figure 182 Paso 7 – SSL de Sub-CA	61
Figure 183 Paso 8 – SSL de Sub-CA	61
Figure 184 Paso $0 = SSL de Sub-CA$	61
Figure 185 Pase 10 SSL de Sub-CA	61
Figure 196 Dese 11 Ver configuración SSL de Sub-CA	62
Figure 197 Deep 1 D plane SCL de Sub-CA	62
Figura 187. Paso 1 – BD plana SSL de Sub-CA	02
Figura 188. Paso 2 – BD piana SSL de Sub-CA	02
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
	65
Figura 201. Paso 4 – Re carga de CRL de Sub-CA	65
Figura 201. Paso 4 – Re carga de CRL de Sub-CA Figura 202. Paso 5 – Re carga de CRL de Sub-CA	00
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	65
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	65 65
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	65 65 65 65
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	65 65 65 65 65
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	65 65 65 65 66 66
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	65 65 65 65 66 66 66
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	65 65 65 65 66 66 66 66
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 Figura 210. Paso 12 – Re carga de CRL de Sub-CA	65 65 65 66 66 66 67 67
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 Figura 210. Paso 12 – Re carga de CRL de Sub-CA Figura 211. Gestión de Certificados cliente	65 65 65 66 66 66 67 67 67
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 Figura 210. Paso 12 – Re carga de CRL de Sub-CA Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente	65 65 65 66 66 66 67 68 68
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 Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente	65 65 65 66 66 66 67 67 68 68 68
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 Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente Figura 214. Paso 3 – Consulta de certificados cliente	65 65 65 66 66 66 67 67 68 68 68 68 68
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 Figura 210. Paso 12 – Re carga de CRL de Sub-CA Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente Figura 214. Paso 3 – Consulta de certificados cliente Figura 215. Paso 1 – Revocar certificados cliente Figura 215. Paso 1 – Revocar certificados cliente	65 65 65 66 66 66 66 67 68 68 68 68 68 68
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 Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente Figura 214. Paso 3 – Consulta de certificados cliente Figura 215. Paso 1 – Revocar certificados cliente Figura 216. Paso 2 – Revocar certificados cliente Figura 216. Paso 1 – Revocar certificados cliente Figura 217. Paso 1 – Revocar certificados cliente	65 65 65 66 66 66 67 67 68 68 68 68 68 68 69 69
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 Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente Figura 214. Paso 3 – Consulta de certificados cliente Figura 215. Paso 1 – Revocar certificados cliente Figura 216. Paso 2 – Revocar certificados cliente Figura 216. Paso 2 – Revocar certificados cliente Figura 217. Paso 3 – Revocar certificados cliente Figura 216. Paso 2 – Revocar certificados cliente	65 65 65 66 66 66 66 67 67 68 68 68 68 68 69 69
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 Figura 210. Paso 12 – Re carga de CRL de Sub-CA Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente Figura 214. Paso 3 – Consulta de certificados cliente Figura 215. Paso 1 – Revocar certificados cliente Figura 216. Paso 2 – Revocar certificados cliente Figura 217. Paso 3 – Revocar certificados cliente Figura 217. Paso 3 – Revocar certificados cliente Figura 217. Paso 3 – Revocar certificados cliente Figura 217. Paso 4 – Revocar certificados cliente Figura 218. Paso 4 – Revocar certificados cliente	65 65 65 66 66 66 66 67 68 68 68 68 69 69 69 69
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 Figura 211. Gestión de Certificados cliente Figura 212. Paso 1 – Consulta de certificados cliente Figura 213. Paso 2 – Consulta de certificados cliente Figura 214. Paso 3 – Consulta de certificados cliente Figura 215. Paso 1 – Revocar certificados cliente Figura 216. Paso 2 – Revocar certificados cliente Figura 217. Paso 3 – Revocar certificados cliente Figura 217. Paso 3 – Revocar certificados cliente Figura 217. Paso 4 – Revocar certificados cliente Figura 218. Paso 4 – Revocar certificados cliente Figura 218. Paso 4 – Revocar certificados cliente Figura 219. Nuevo certificados cliente Figura 219. Nuevo certificados cliente	65 65 65 66 66 66 66 67 68 68 68 68 69 69 69 69 69

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	
rigara ozri riaco z rigrogar vonomiono oktorio internetionali internetionali	98
Figura 328. Paso 3 - Agregar Vencimiento externo	98 98
Figura 328. Paso 3 - Agregar Vencimiento externo Figura 329. Alertas y Notificaciones – Edición de Configuración	98 98 99
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	98 98 99 100

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
	107
Figura 359. Paso 8 – Edición de Subjets CSR pre cargados	. 107
Figura 359. Paso 8 – Edición de Subjets CSR pre cargados Figura 360. Paso 9 – Ejemplo de edición de Subjets CSR pre cargados	. 107
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	. 107 . 107 . 108
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	. 107 . 107 . 108 . 108
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	. 107 . 107 . 108 . 108 . 108
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	. 107 . 107 . 108 . 108 . 108 . 108
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	. 107 . 107 . 108 . 108 . 108 . 108 . 108
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	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108
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	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109
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	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109
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	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109
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 Figura 370. Paso 1 – Recepción y composición de certificado final.	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 110
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 Figura 370. Paso 1 – Recepción y composición de certificado final. Figura 371. Paso 2 – Recepción y composición de certificado final.	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 110 . 111
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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 372. Paso 3 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 110 . 110 . 111 . 111
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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 110 . 110 . 111 . 111
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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 4B – Recepción y composición de certificado final Figura 374. Paso 4B – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 111 . 111 . 111
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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 4B – Recepción y composición de certificado final Figura 375. Paso 5 – Recepción y composición de certificado final Figura 375. Paso 5 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 111 . 111 . 111 . 111
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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – 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 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 6 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 111 . 111 . 111 . 111 . 112
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 Figura 369. Paso 18 - Pedido de certificado Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – 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 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 111 . 111 . 111 . 111 . 112 . 112
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 Figura 369. Paso 18 - Pedido de certificado Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – Recepción y composición de certificado final Figura 375. Paso 5 – Recepción y composición de certificado final Figura 376. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – 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 377. Paso 7 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 111 . 111 . 111 . 111 . 111 . 112 . 112 . 112
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 Figura 369. Paso 18 - Pedido de certificado Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – 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 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 7 – 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 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 109 . 109 . 110 . 110 . 110 . 109 . 109 . 110 . 110 . 109 . 110 . 111 . 111 . 111 . 111 . 111 . 111 . 111 . 111 . 112 . 112
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 Figura 369. Paso 18 - Pedido de certificado Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – 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 377. Paso 7 – 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 379. Paso 9 – 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 Figura 380. Paso 10 – Recepción y composición de certificado final Figura 380. Paso 10 – Recepción y composición de certificado final Figura 380. Paso 10 – Recepción y composición de certificado final Figura 380. Paso 10 – Recepción y composición de certificado final Figura 380. Paso 10 – Recepción y composición de certificado final	. 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 110 . 111 . 111 . 111 . 111 . 111 . 112 . 112 . 112 . 113
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 . Figura 370. Paso 18 - Pedido de certificado . Figura 370. Paso 1 – Recepción y composición de certificado final . Figura 371. Paso 2 – Recepción y composición de certificado final . Figura 373. Paso 4A – Recepción y composición de certificado final . Figura 374. Paso 5 – Recepción y composición de certificado final . Figura 375. Paso 5 – Recepción y composición de certificado final . Figura 376. Paso 5 – 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 379. Paso 9 – Recepción y composición de certificado final . Figura 379. Paso 9 – Recepción y composición de certificado final . Figura 379. Paso 9 – Recepción y composición de certificado final . Figura 379. Paso 9 – 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 . Figura 381. Validaciones varias – Text box campo vacío .	. 107 . 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 111 . 111 . 111 . 111 . 112 . 112 . 112 . 113 . 113
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 370. Paso 16 - Pedido de certificado Figura 370. Paso 1 - Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – Recepción y composición de certificado final Figura 375. Paso 6 – Recepción y composición de certificado final Figura 376. Paso 5 – Recepción y composición de certificado final Figura 377. Paso 5 – Recepción y composición de certificado final Figura 378. Paso 6 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 8 – 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 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – 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 Figura 381. Validaciones varias – Text box campo vacío Figura 382. Validaciones varias – Text box Mensaje	. 107 . 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 111 . 111 . 111 . 111 . 112 . 112 . 112 . 113 . 113 . 113
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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 373. Paso 4A – Recepción y composición de certificado final Figura 374. Paso 5 – Recepción y composición de certificado final Figura 375. Paso 5 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 377. Paso 8 – Recepción y composición de certificado final Figura 378. Paso 8 – Recepción y composición de certificado final Figura 377. Paso 7 – Recepción y composición de certificado final Figura 376. Paso 8 – 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 379. Paso 9 – Recepción y composición de certificado final Figura 379. Paso 9 – 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 Figura 381. Validaciones varias – Text box campo vacío Figura 383. Validaciones varias – Text box correo electrónico	. 107 . 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 111 . 111 . 111 . 111 . 112 . 112 . 112 . 112 . 112 . 113 . 113 . 114
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 Figura 369. Paso 18 - Pedido de certificado Figura 370. Paso 1 - Recepción y composición de certificado final Figura 371. Paso 2 - Recepción y composición de certificado final Figura 372. Paso 3 - Recepción y composición de certificado final Figura 373. Paso 4A - Recepción y composición de certificado final Figura 374. Paso 5 - 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 379. Paso 9 - 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 Figura 381. Validaciones varias - Text box Campo vacío Figura 383. Validaciones varias - Text box Mensaje Figura 384. Validaciones varias - Text box Mensaje	. 107 . 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 101 . 109 . 109 . 109 . 109 . 109 . 109 . 109 . 110 . 111 . 111
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 364. 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 Figura 370. Paso 1 – Recepción y composición de certificado final Figura 371. Paso 2 – Recepción y composición de certificado final Figura 372. Paso 3 – Recepción y composición de certificado final Figura 373. Paso 4 – Recepción y composición de certificado final Figura 374. Paso 4B – Recepción y composición de certificado final Figura 375. Paso 5 – Recepción y composición de certificado final Figura 376. Paso 8 – 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 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 Figura 381. Validaciones varias – Text box correo electrónico Figura 384. Validaciones varias – Text box Mensaje Figura 384. Validaciones varias – Text box Mensaje Figura 385. Validaciones varias – Text box Mensaje Figura 384. Validaciones varias – Text box Mensaje Figura 385. Validaciones varias – Text box Me	. 107 . 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 111 . 111 . 111 . 111 . 112 . 112 . 112 . 113 . 113 . 114 . 114 . 114
Figura 359. Paso 8 – Edición de Subjets CSR pre cargados. Figura 360. Paso 9 – Ejemplo de edición de Subjets CSR pre cargados	. 107 . 107 . 107 . 108 . 108 . 108 . 108 . 108 . 108 . 109 . 110 . 111 . 111 . 111 . 111 . 112 . 112 . 112 . 112 . 113 . 114 . 114 . 114 . 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, <u>https://tomcat.apache.org/tomcat-8.5-doc/config/http.html</u> (consultada el 09/11/2018)

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

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

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

Buenas prácticas TLS / SSL, <u>https://ciberseguridad.blog/buenas-practicas-tls-ssl/</u> (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-

<u>17_Recomendaciones_implementacion_HTTPS.pdf</u> (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/wpcontent/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%2 0COLEGIO%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 riesgos buenas prácticas autenticación sobre en online, Inteco. У 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?, <u>https://askubuntu.com/questions/239631/how-can-i-watch-the-current-connections-on-my-</u> apache-webserver (consultada el 21/07/2019) How to read the SSL certificate info from the CLI, <u>https://ma.ttias.be/how-to-read-ssl-certificate-info-from-the-cli/</u> (consultada el 11/02/2019)

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

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

Internet X.509 Public Key Infrastructure Qualified Certificates Profile, <u>https://tools.ietf.org/html/rfc3039</u> (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, <u>https://www.openssl.org/docs/man1.1.1/man1/ca.html</u> (consultada el 19/02/2019)

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

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

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

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

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

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

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

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

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

Recommendation X.509, <u>https://www.itu.int/rec/T-REC-X.509/en</u> (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), <u>https://tools.ietf.org/html/rfc6125.html</u> (consultada el 22/08/2019)

SSL / TLS Best Pactices, Deploy SSL with Confidence, <u>https://www.entrust.com/lp/wp-</u> 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, <u>https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices</u> (consultada el 17/06/2019)

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

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

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

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

Trabajo con los certificados en Java keystore, <u>https://www.sslmarket.es/ssl/help-trabajar-con-los-certificados-en-java-keystore/</u> (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-ssI-de-cliente-como-sistema-de-

autenticacion-web/ (consultada el 22/06/2019)

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

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

7. Bibliografía específica

Wikipedia, [1] Infraestructura de pública, clave https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica (Consultada el 12/10/2019) Wikipedia, https://es.wikipedia.org/wiki/C%C3%B3digo abierto [2] Código Abierto, (Consultada el 03/11/2019) [3] Open Source Iniciative, https://opensource.org/ (Consultada el 03/11/2019) Añadir certificados CA almacén JRE. IBM [4] al de claves 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 autenticación https://northsecure.es/wpprácticas en online. 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/wpcontent/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://pkitutorial.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/fundamentossobre-certificados-digitales-iv-mecanismos-de-validacion-de-certificados/ (Consultada el 05/01/2019) PFX IIS [14] Tutorial de Exportar Importar Certificados SSL en 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-deidentidad-digital (Consultada el 29/11/2019) [20]Taxistas deben identificación, usar nueva http://www.defensoriaturista.org.ar/oldweb/index.php/noticias/34-taxistas-deben-usar-nuevaidentificacion (Consultada el 16/10/2019) Advanced PKI, OpenSSL PKI Tutorial, https://pki-[21] tutorial.readthedocs.io/en/latest/advanced/index.html (Consultada el 11/06/2019) [22] TLS Client Certificate Request Configuration File, OpenSSL PKI Tutorial, https://pkitutorial.readthedocs.io/en/latest/expert/client.conf.html (Consultada el 11/06/2019) [23] TLS Server Certificate Request Configuration File, OpenSSL PKI Tutorial, https://pkitutorial.readthedocs.io/en/latest/expert/server.conf.html (Consultada el 11/06/2019) CA Configuration [24] Software File, OpenSSL PKI Tutorial, https://pkitutorial.readthedocs.io/en/latest/advanced/software-ca.conf.html (Consultada el 13/06/2019) [25] Root CA Configuration File, OpenSSL PKI Tutorial, https://pkitutorial.readthedocs.io/en/latest/advanced/root-ca.conf.html (Consultada el 18/06/2019)