GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 845C

LUCIA – Manual Instalación Organismo



octubre de 2020

SIN CLASIFICAR

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

© Centro Criptológico Nacional, 2017

NIPO: 785-17-0008-2

Fecha de Edición: octubre de 2020

El CCN y CSA han participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.



Febrero de 2016

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 1
2. INSTALACIÓN EN UN SERVIDOR DE VIRTUALIZACIÓN (VMWARE ESXI) 2
2.1. IMPORTACIÓN DE LA IMAGEN EN EL SERVIDOR 2
2.1.1. RENOMBRADO DE LOS DISCOS 3
2.1.2. CONFIGURACIÓN DE LOS PARÁMETROS DE LA BIOS 4
3. CONFIGURACIÓN INICIAL 6
3.1. ACCESO INICIAL 6
3.2. CONFIGURAR CONEXIÓN DE RED 6
3.3. ACTUALIZACIÓN Y MANTENIMIENTO 7
3.4. AUTOINSTALADOR DE LUCIA 8
3.4.1. COMPLETAR MANUALMENTE EL FICHERO DE CONFIGURACIÓN 9
3.4.2. COMPLETAR EL FICHERO DE CONFIGURACIÓN DE FORMA ASISTIDA 9
4. ACCESO A LA INTERFAZ WEB DE LUCIA 14
4.1. CONFIGURACIÓN DE ACCESO POR LDAP 14
F.A.Q. (PREGUNTAS Y RESPUESTAS FRECUENTES) 16
ANEXO A. GENERACIÓN DE UNA CA Y EMISIÓN DE CERTIFICADOS 18
ANEXO A.1. GENERAR LA CA 18
ANEXO A.2. GENERAR UN CERTIFICADO DE SERVIDOR 20
ANEXO A.3. GENERAR UN CERTIFICADO DE CLIENTE 21
ANEXO A.4. GENERAR LA LISTA DE REVOCACIÓN DE USUARIOS (CRL) 22
ANEXO A.5. CAMBIAR EL FORMATO DE LOS CERTIFICADOS 23
ANEXO B. AUMENTO DE LA PARTICIÓN DE DATOS 24
ANEXO C. AÑADIR VIRTUALHOST 25
ANEXO D. FORMULARIO DE RECOGIDA DE DATOS DE INSTALACIÓN 27
ANEXO E. INSTALACIÓN MANUAL DE LUCIA 29
ANEXO E.1. CONFIGURACIÓN INICIAL 29
ANEXO E.1.1. ESTABLECER EL NOMBRE DE LA MÁQUINA 29
ANEXO E.1.2. CONFIGURACIÓN DE FECHA Y HORA 29
ANEXO E.1.3. CERTIFICADOS DIGITALES DEL SERVIDOR WEB 29
ANEXO E.1.4. CONFIGURACIÓN DE APACHE HTTP SERVER 31
ANEXO E.1.5. CONFIGURACIÓN DEL SERVICIO DE GESTIÓN DE TICKETS 32
ANEXO E.2. CONFIGURACIÓN DEL CORREO ELECTRÓNICO 33
ANEXO E.2.1. RECEPCIÓN DE CORREOS 33
ANEXO E.2.2. ENVÍO DE CORREOS 35
ANEXO E.2.3. NOTIFICACIONES INTERNAS 37
ANEXO E.3. COMUNICACIÓN CON LUCIA CENTRAL 38
ANEXO E.3.1. CONFIGURACIÓN DEL CERTIFICADO DE CLIENTE PROPORCIONADO POR EL CCN-CERT 39
ANEXO E.3.2. CONFIGURACIÓN DE SINCRONIZACIÓN DE INCIDENTES 39
ANEXO E.4. CAMBIO DE CONTRASEÑAS 40
ANEXO E.5. AUTENTICACIÓN SMTP 41

1. INTRODUCCIÓN

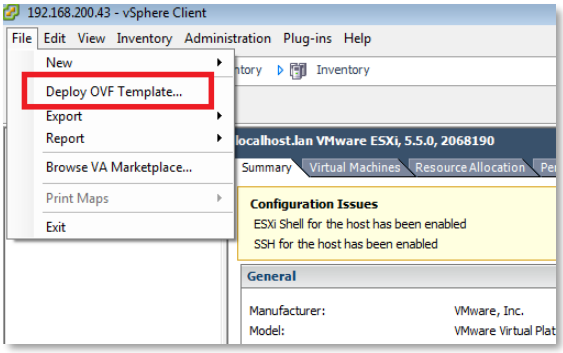
1. LUCIA se distribuye como máquina virtual en formato OVF lista para ser configurada y ejecutada, cuyo despliegue puede realizarse en cualquier servidor de virtualización que acepte este formato como por ejemplo VMWare ESXi o KVM. La distribución consta de un primer disco que contiene el sistema operativo (`lucia-so.vmdk` - 55GB) y de un segundo disco donde se encuentra toda la configuración y la instalación del software de gestión de tickets (`lucia-data.vmdk` - 50GB).
2. En caso de querer ampliar el espacio de almacenamiento asignado inicialmente o si se llenaran los discos, es posible aumentar el espacio del disco de datos siguiendo el procedimiento descrito en el Anexo B de este manual.
3. Para realizar la instalación de LUCIA se necesitará:
    - La máquina virtual de LUCIA en formato OVF que incluye los dos discos proporcionados con la distribución oficial del software.
    - Configuración de red para la máquina.
    - Un nombre de dominio para la máquina, es decir, la URL del servicio LUCIA.
    - Una o varias cuentas de correo (dependiendo de si el organismo se encuentra adscrito a los *Sistemas de Alerta Temprana* SAT-INET/SAT-SARA/SAT-ICS) en un servidor IMAP (también disponible para POP3) para la recepción de correos.
    - Un servidor SMTP para el envío de correos.
    - Un certificado digital válido perteneciente a una CA junto a su cadena de certificación para el servidor. De no estar en posesión del mismo o querer crear uno nuevo, se adjunta un procedimiento de creación de una nueva CA.
    - Un navegador con el certificado de cliente instalado que se genera durante la instalación.
4. En cuanto a los elementos de red de protección de perímetro hay que tener en cuenta los siguientes puertos:
    - Puerto `443` [entrada/salida]: para permitir *comunicación bidireccional* con el FQDN `lucia-rest.ccn-cert.cni.es`
    - Puerto `443` [entrada]: (opcional) restringido o no al rango que se requiera, para el acceso desde internet a la interfaz de LUCIA del organismo.
    - Salida a internet: (opcional dependiendo de la política de seguridad y actualizaciones del organismo) para la actualización del sistema operativo de la máquina virtual.
    - En caso de que los sistemas de correo al que LUCIA vaya a acceder estuviesen fuera de la red y se requiera usarlos, tener en cuenta gestionar los puertos SMTP (`25`, a veces `587`), IMAP (`143`)/IMAPs (`993`) o en su defecto POP3 (`110`)/POP3s (`995`).

2. INSTALACIÓN EN UN SERVIDOR DE VIRTUALIZACIÓN (VMWARE ESXI)

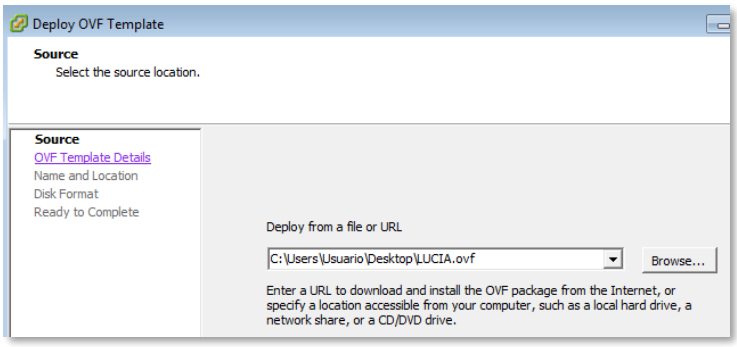
2.1. IMPORTACIÓN DE LA IMAGEN EN EL SERVIDOR

5. El formato OVF permite importar LUCIA en cualquier sistema de virtualización que soporte el formato OVF tales como VMware Workstation, VirtualBox o KVM. En este apartado se explica el procedimiento de importación en VMware ESXi.

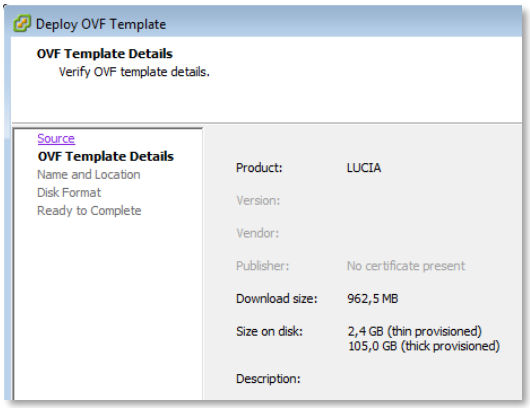
6. Una vez conectado al servidor VMware ESXi mediante la consola de gestión vSphere Client se inicia el asistente de importación mediante la opción *Deploy OVF Template*:



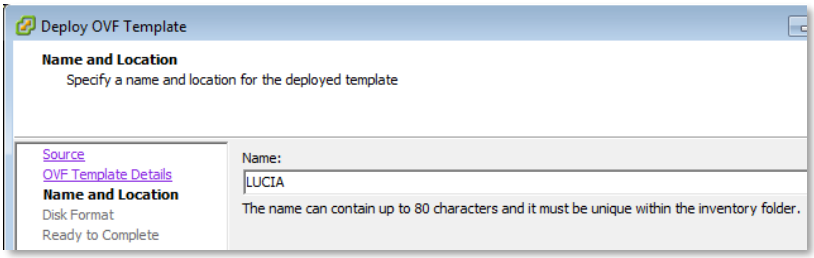
7. Se selecciona el fichero “LUCIA.ovf”:



8. Aparecerá el resumen de la máquina virtual a importar (los datos de la imagen mostrada pueden variar):

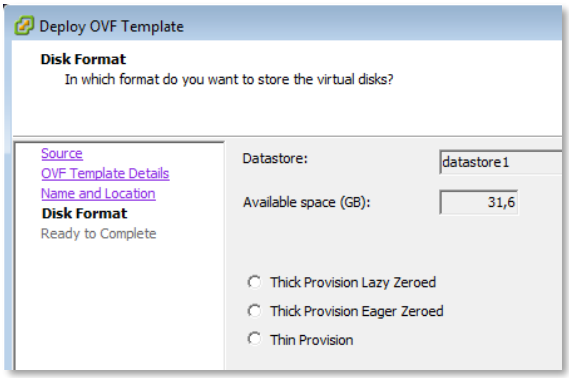


9. Se selecciona el nombre que se quiera asignar dentro de la infraestructura virtual de la organización:



10. Se selecciona el volumen de datos donde se almacenará LUCIA (datastore) y el modo en que se creará el disco (seleccionar lo que corresponda según la política del organismo):

    - *Thick Provision Lazy Zeroed*: Se crearán en el datastore los dos discos duros virtuales de LUCIA reservando todo el espacio asignado (50GB+55GB).
    - *Thick Provision Eager Zeroed*: Se crearán en el datastore los dos discos duros virtuales de LUCIA reservando todo el espacio asignado (50GB+55GB). La diferencia con el anterior es que el espacio en disco no ocupado por las imágenes de disco de LUCIA se inicializará con ceros.
    - *Thin Provision*: Se crearán en el datastore los dos discos duros virtuales con el tamaño exacto de las imágenes creciendo dinámicamente según se vaya necesitando hasta el tamaño definido por LUCIA.



11. Una vez finalizado el asistente, comenzará a importar LUCIA en la infraestructura de virtualización.
12. En cuanto a los parámetros del hardware, LUCIA se configura por defecto con 2GB de RAM y un procesador. Estos valores pueden modificarse dependiendo de las necesidades, siendo recomendables 4GB de RAM y dos procesadores.

2.1.1. RENOMBRADO DE LOS DISCOS

13. **NOTA**: Se ha detectado que los discos virtuales una vez importados en el servidor de virtualización se nombran como `LUCIA.vmdk` y `LUCIA_1.vmdk` (dependerá del nombre asignado la máquina virtual) debido a que las plantillas OVF no permiten definir el nombre de los discos en el destino.

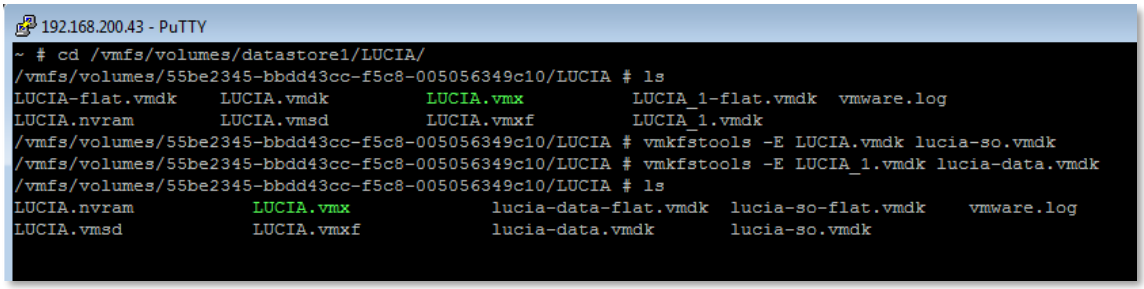
14. Aunque no es necesario, es posible mantener los nombres originales de los discos duros virtuales de LUCIA renombrándolos en el *datastore*.

15. Con la máquina virtual de LUCIA apagada, hay que conectarse por consola al servidor VMware ESXi (por SSH si está habilitado) y situándose en el directorio donde se almacena LUCIA se utiliza el comando `vmkfstools`.

16. Para ello se ejecuta:

```
bash (VMWare ESXi)

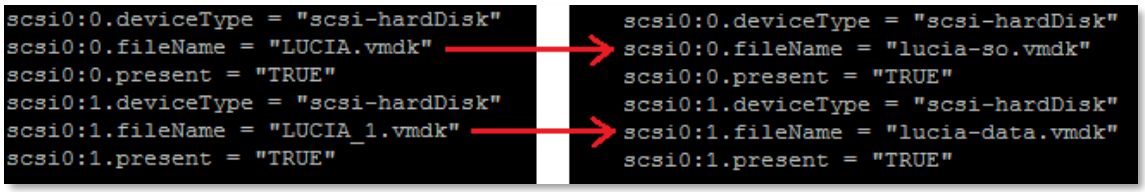
vmkfstools -E LUCIA.vmdk lucia-so.vmdk
vmkfstools -E LUCIA_1.vmdk lucia-data.vmdk
```



17. Se debe modificar en el fichero de configuración `LUCIA.vmx` (dependerá del nombre asignado la máquina virtual) los parámetros relativos a los nombres de los ficheros que contienen los discos virtuales:

```
bash (VMWare ESXi)

vi LUCIA.vmx
```



18. Una vez se inicie la máquina virtual los nuevos parámetros se actualizarán automáticamente en la interfaz. En caso de algún tipo de error, bastaría con eliminar la máquina virtual del inventario y volver a añadirla.

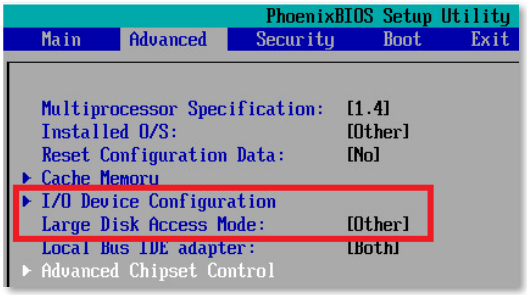
2.1.2. CONFIGURACIÓN DE LOS PARÁMETROS DE LA BIOS

19. Se pueden afinar los parámetros de la BIOS de la máquina virtual de LUCIA pulsando la tecla *F2* en el arranque y configurándolos como se detalla a continuación.

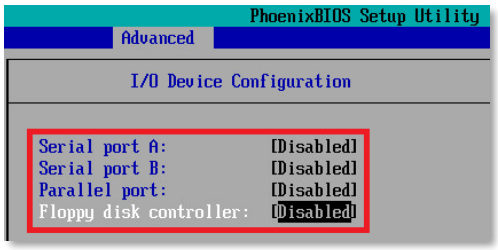
20. En la pestaña *Main* establecer *Legacy Diskette A* al valor *Disabled*:



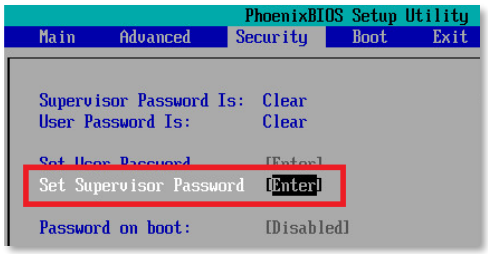
21. En la pestaña *Advanced* establecer *Large Disk Access Mode* al valor *Other*:



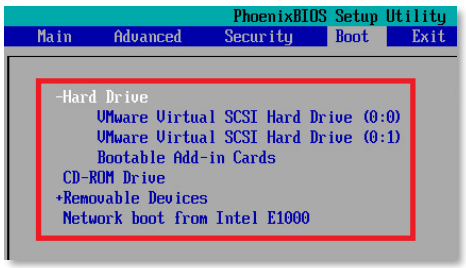
22. En la pestaña *Advanced* submenú *I/O Device Configuration* deshabilitar *Serial port A*, *Serial port B*, *Parallel port* y *Floppy disk controller*:



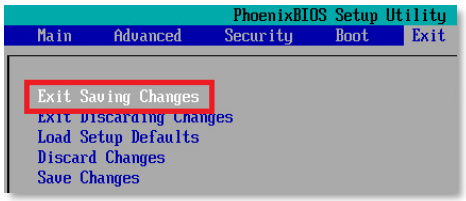
23. Dependiendo de la política de seguridad del organismo, en la pestaña *Security* establecer la contraseña de BIOS:



24. En la pestaña *Boot* establecer el orden de los dispositivos de arranque



25. Por último, en la pestaña *Exit* salir de la BIOS guardando los cambios



3. CONFIGURACIÓN INICIAL

3.1. ACCESO INICIAL

26. Una vez importada e iniciada la máquina virtual de LUCIA se debe acceder y ejecutar las instrucciones de este manual con las credenciales de administrador para realizar las configuraciones correspondientes directamente sobre la consola de la máquina.
27. Las credenciales de los usuarios son las siguientes:

Usuario	Contraseña	Rol
root	C3nTo5uS3rR00T	Usuario privilegiado del sistema
nopriv	C3nTo5uS3rN0pR1v	Usuario no privilegiado del sistema
root	LuC14MySQLR00T	Usuario privilegiado de MariaDB
root	3rtuo47	Usuario privilegiado web LUCIA
operador	operador11	Usuario operador web LUCIA

28. La configuración de seguridad aplicada exige que en caso de que el acceso se haga por SSH, se deba utilizar el usuario no privilegiado `nopriv` y una vez autenticado, elevar privilegios y convertirnos en `root` mediante el comando:

```
bash
su
```

29. Una vez autenticado, para poner la distribución del teclado en español, ejecutar el comando:

```
bash
loadkeys es
```

30. Tras la finalización de la configuración es importante realizar el cambio de todas las contraseñas proporcionadas por defecto tal y como se indica en Anexo E.4.

3.2. CONFIGURAR CONEXIÓN DE RED

31. La configuración de la conexión de red se realiza modificando el fichero de configuración `/etc/sysconfig/network-scripts/ifcfg-eth0`
32. En la configuración inicial de la máquina distribuida el servicio de red se encuentra configurado como DHCP:

```
INI: /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
DEVICE=ens33
```

```
ONBOOT=yes
PEERDNS=yes
```

33. Es posible que el identificador del adaptador (parámetro `DEVICE`) del fichero de configuración incluido no se corresponda con el detectado. Para identificar el parámetro correcto a utilizar basta con consultar la salida del comando:

```
bash
```

```
ifconfig –a
```

34. A continuación, se describe un ejemplo de configuración completo para una interfaz de red estática:

```
INI: /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
DEVICE=ens32
ONBOOT=yes
PEERDNS=yes
IPADDR0=192.168.1.1
PREFIX0=24
GATEWAY=192.168.1.254
DNS1=192.168.1.101
DNS2=192.168.1.102
```

35. Una vez finalizada la configuración, se debe reiniciar el servicio de red:

```
bash
```

```
systemctl restart network.service
```

36. Dadas todas las posibilidades de configuración de red, se recomienda remitirse a la configuración de RedHat Enterprise Linux 7[1] y determinar la configuración correcta del adaptador.
37. Puede ocurrir que si se ponen en funcionamiento varias máquinas de LUCIA en la misma red, colisionen sus direcciones MAC. Para solucionar esto, se debe asignar una dirección MAC diferente en el adaptador de red virtual en el servidor de virtualización y automáticamente quedará asignada al arrancar en la máquina virtual.
38. Una vez que la configuración de red esté funcionando se puede acceder a la máquina a través de SSH recordando que se debe utilizar el usuario `nopriv` y elevar privilegios.

3.3. ACTUALIZACIÓN Y MANTENIMIENTO

39. Tras iniciar el servicio de red y una vez comprobado que LUCIA tiene salida a Internet, se puede actualizar el sistema operativo ejecutando:

[1] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/

```
bash
yum update
```

40. Una vez finalizado el proceso de actualización y reiniciado el sistema, se pueden eliminar los kernel antiguos y los instaladores de los paquetes descargados ejecutando los siguientes comandos:

```
bash
package-cleanup --oldkernels –count=1
yum clean all
```

41. La actualización del sistema operativo no implica la actualización de LUCIA. Para ello se liberarán parches específicos que serán aplicados de forma independiente.
42. Es responsabilidad del administrador mantener actualizado el sistema, así como aplicar las políticas y medidas de protección vigentes en su organización.
43. A partir de este momento, existen dos posibilidades para la instalación, automática o manual. **Se recomienda utilizar la instalación automática.**

3.4. AUTOINSTALADOR DE LUCIA

44. A partir de la versión 2.0.2 de LUCIA, se incluye en la imagen un ejecutable para facilitar la instalación de la herramienta. Los pasos que automatiza son exactamente los mismos que se describen en el Anexo E del presente manual.
45. Para continuar con el autoinstalador hay que completar el fichero de configuración. Existen dos maneras de poder completarlo, manual y asistida, descritas en los apartados 3.4.1 y 3.4.2.
46. Una vez completado el fichero de configuración, se procede con los siguientes pasos para terminar la instalación.
47. Una vez cumplimentados todos los parámetros necesarios, se ejecuta el siguiente comando con el usuario privilegiado `root` y se siguen los pasos mostrados en pantalla:

```
bash
sh /media/lucia-data/usr/bin/lucia_installer.sh
```

48. El propio instalador ejecutará una serie de validaciones sobre los datos introducidos, abortando la instalación en el caso de encontrar alguna discordancia.
49. Tras una ejecución correcta, se dispondrá de una instancia de LUCIA funcional sobre la que se deberán **aplicar todas las actualizaciones publicadas de manera ordenada y secuencial**.
50. Se recuerda que, por motivos de seguridad, se deberá extraer la CA generada, si procede, a una máquina aislada y eliminarla de la instancia de LUCIA.

51. Si se ha autogenerado la CA, el certificado de cliente para importar en el navegador se encuentra en la ruta `/var/local/ca/certs/[nombre].p12`.

3.4.1. COMPLETAR MANUALMENTE EL FICHERO DE CONFIGURACIÓN

52. Para utilizarlo, es necesario rellenar antes el fichero de configuración (`lucia_installer.ini`) con los datos a configurar en la instancia (similar al indicado en el Anexo D "Formulario de recogida de datos de instalación") el cual se encuentra en la ruta `/media/lucia-data/usr/bin/lucia_installer.ini`.
53. En el propio fichero se indican la explicación de cada parámetro y su sintaxis.
54. A continuación, se resumen algunas notas de interés:
55. Los parámetros `AVAILABLE_SATINET`, `AVAILABLE_SATSARA` y `AVAILABLE_SATICS` se deberán rellenar a `S` en caso de disponer del servicio y querer sincronizar la instancia con LUCIA Central.
56. El parámetro `AVAILABLE_CERTS` se deberá rellenar con `S` en el caso de que el organismo disponga de una CA y un certificado de servidor, debiendo en tal caso copiar dichos archivos a la máquina de LUCIA (por ejemplo al directorio `/home/nopriv`) e indicar en los parámetros de la sección correspondiente las rutas completas a los ficheros que se hayan copiado:

```
INI: lucia_installer.ini
```

```
# -- Rutas de los certificados disponibles (si AVAILABLE_CERTS=S)
```

57. **NOTA:** una vez completada la instalación, los certificados copiados se eliminarán automáticamente de forma segura.
58. Por último, en el fichero se incluye el apartado para cambiar las contraseñas por seguridad y que no sean las que aparecen por defecto para MariaDB, usuario RT y para la sincronización además de los usuarios de sistema, tanto el `nopriv` como `root`.

3.4.2. COMPLETAR EL FICHERO DE CONFIGURACIÓN DE FORMA ASISTIDA

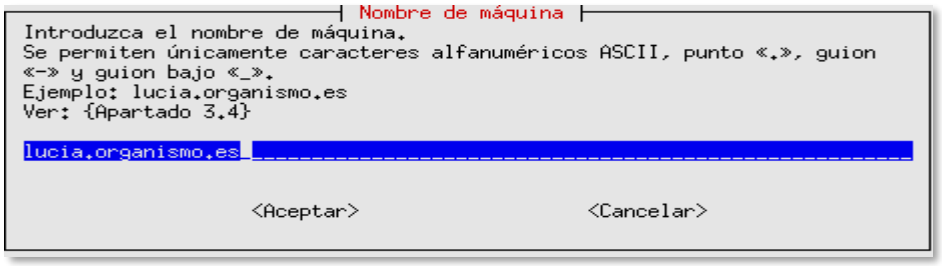
59. Se ejecuta el siguiente comando con el usuario privilegiado `root`:

```
bash
```

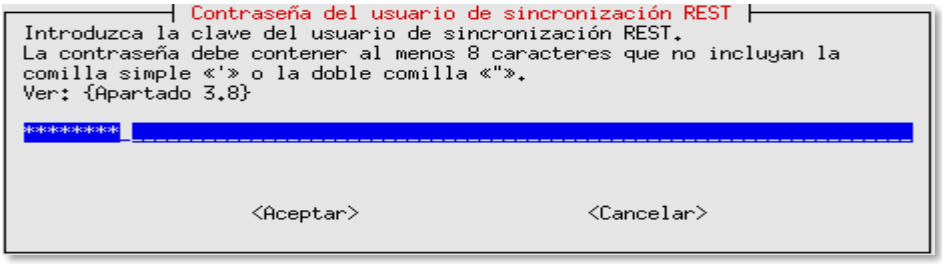
```
sh /media/lucia-data/usr/bin/lucia_installer_wizard.sh
```

60. Las primeras pantallas son para configurar el servicio de gestión de tickets y se solicitará introducir el nombre de la máquina (ejemplo: `lucia.organismo.es`), nombre de instancia (en mayúsculas; e.g., `ORGANISMO`) y también la URL del

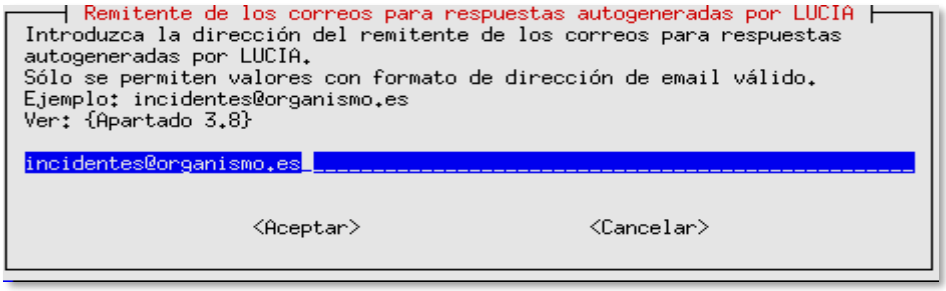
organismo (ejemplo: `https://www.organismo.es`). A continuación, la FQDN de LUCIA que suele coincidir con el nombre de la máquina.



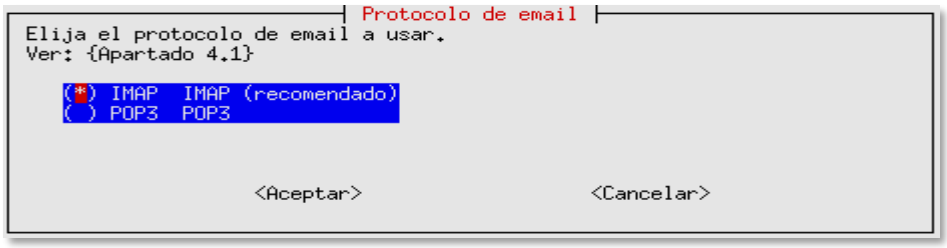
61. Introducir la contraseña del usuario de REST con las restricciones que se indican en la pantalla, también se solicitará poner el nombre del DNS visible en internet (ejemplo: `lucia.organismo.es`).



62. A continuación, solicitará introducir la dirección de correo del remitente para respuestas autogeneradas, el remitente por defecto de los correos para comentarios autogenerados y al que se enviarán informes de error en la sincronización para LUCIA. Ejemplo: `incidentes@organismo.es` y `errores_sync_lucia@organismo.es`.

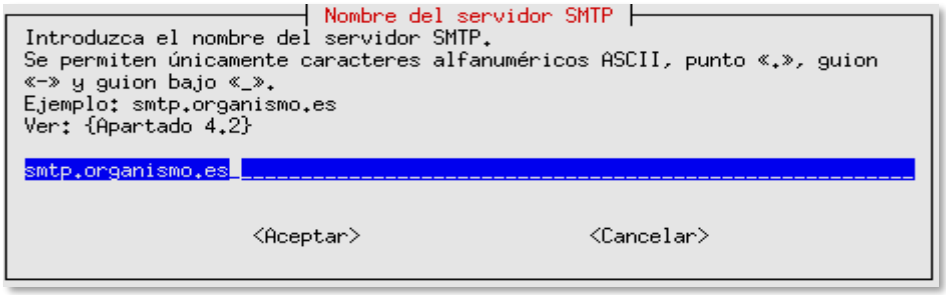


63. Ahora se debe configurar el correo electrónico. Para ello se debe elegir el protocolo a utilizar (IMAP/POP3). (Nota: Mover con el cursor y seleccionar con barra espaciadora).

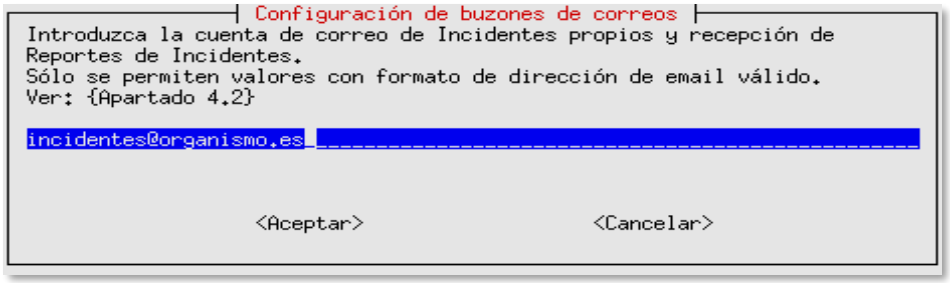


64. Nos va a pedir el nombre del servidor IMAP/POP3 (ejemplo: `email.organismo.es`), también la dirección IP del servidor en formato IPv4 y los puertos, los cuales por defecto son el `143` para IMAP y el `110` para POP3.

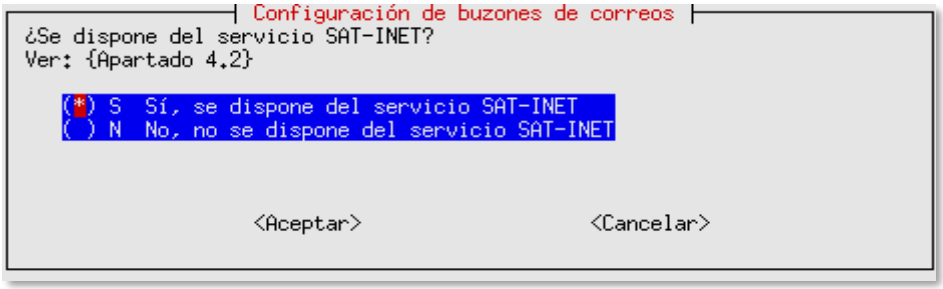
65. De igual modo, introducir el nombre del servidor SMTP (ejemplo: `smtp.organismo.es`), dirección IP en formato IPv4 válidos y el puerto, que por defecto que es el `25`.



66. Ahora continuamos con la configuración de buzones de correos. Se debe introducir la cuenta de correo de incidentes propios y recepción de reporte de incidentes (ejemplo: `incidentes@organismo.es`), también el nombre de usuario de conexión, la contraseña y el alias generado para dicha cuenta (ejemplo: `alias_incidentes@organismo.es`).

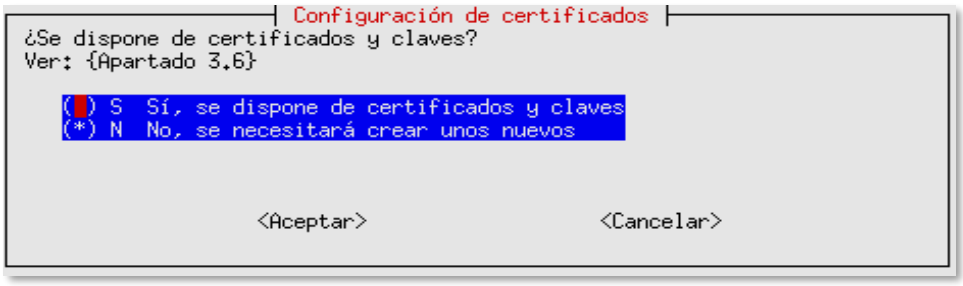


67. Si se dispone de alguna sonda *SAT-INET*, *SAT-SARA* o *SAT-ICS*, se deben configurar las cuentas de correo de incidentes, indicando la cuenta de correo, usuario, contraseña y el alias generado para dicha cuenta. Ejemplo para *SAT-INET*: `satinet@organismo.es` (cuenta de correo y usuario) y `alias_satinet@organismo.es`



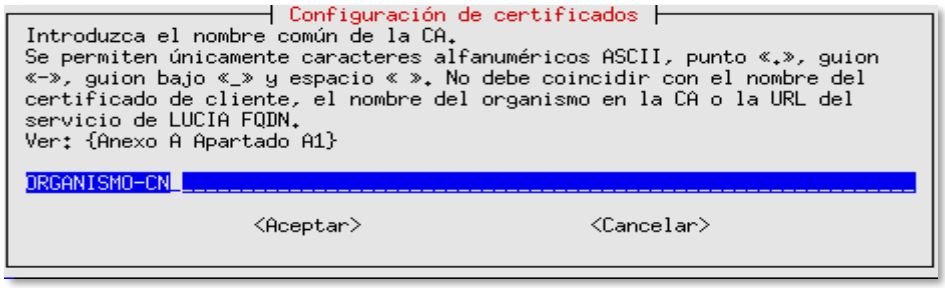
68. Si se dispone de certificados propios y claves se deben indicar las rutas de los mismos. En caso negativo se generará una CA y se emitirán los certificados.

69. **NOTA:** El propio autoinstalador se encargará de validar los certificados proporcionados.

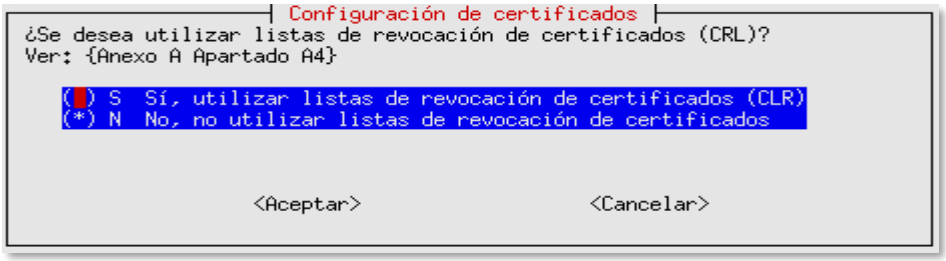


70. En caso de no disponer de certificados, se deberán introducir todos los campos necesarios para la generación de los mismos: nombre común de la CA (ejemplo: `ORGANISMO-CN`), caducidad de la CA en días, nombre del organismo (ejemplo: `ORGANISMO-CA`), ciudad y provincia (ejemplo: `Madrid`), así como una cuenta de correo, contraseña de la CA de al menos 8 caracteres y que no incluyan la comilla simple o la comilla doble.

71. **NOTA:** Los parámetros Nombre Común de la CA, Nombre del organismo para la CA, Nombre del Certificado de Cliente y la URL de la instancia no deben coincidir.

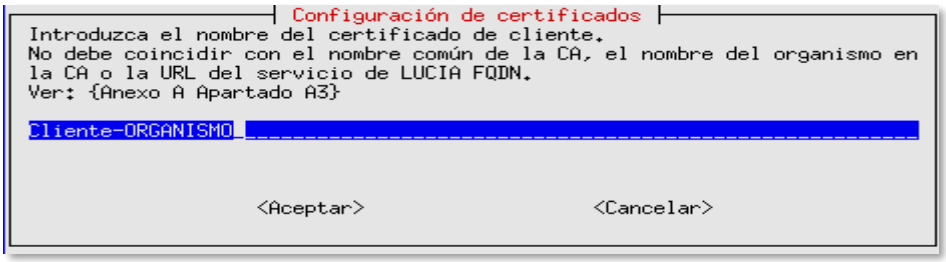


72. Se debe indicar si se desean usar listas de revocación de certificados (CRL). En caso afirmativo indicar la caducidad en días.



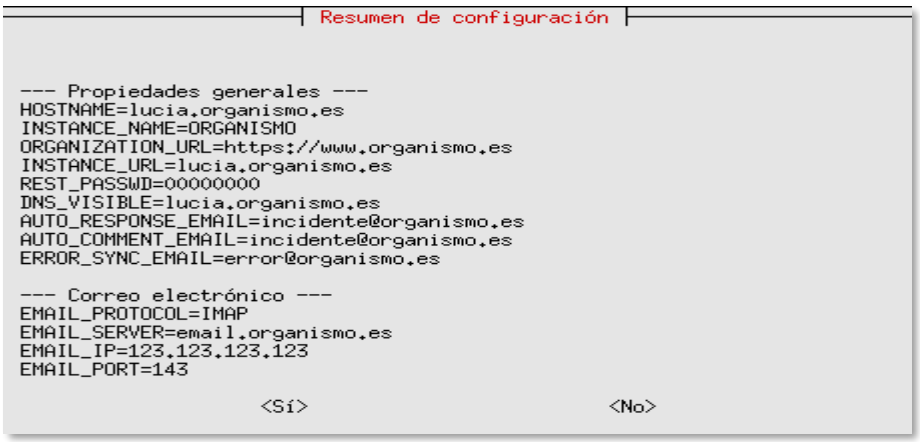
73. A continuación, se generará el certificado cliente, para lo cual se solicitará el Nombre del Certificado de Cliente (ejemplo: `Cliente_Organismo`) y la contraseña.

74. **NOTA:** La contraseña es la que solicitará el navegador cuando se importe el certificado.



75. Por último, es necesario cambiar las contraseñas por defecto para MariaDB[2], usuario RT[2] y para la sincronización[2] además de los usuarios de sistema[3], tanto el `nopriv` como `root`.

76. Para finalizar, nos saldrá el resumen de la configuración que vamos a usar en nuestra instalación.



[2] La contraseña debe de contener al menos 4 caracteres, que no incluyan la comilla simple o la doble.
[3] La contraseña debe contener al menos 8 caracteres, que no incluyan la comilla simple o la doble.

4. ACCESO A LA INTERFAZ WEB DE LUCIA

78. Si la configuración anterior ha sido correcta y con el certificado de cliente cargado en el navegador que vaya a utilizarse, se puede acceder al servidor web donde se encuentre instalado a través de la dirección del servicio `https://<URL_servicio_LUCIA>`.

79. Los usuarios por defecto definidos en LUCIA son los siguientes:

Usuario	Contraseña	Rol
root	3rtuo47	Usuario privilegiado web LUCIA
operador	operador11	Usuario operador web LUCIA

80. El usuario `root` es el administrador con el que se puede configurar el entorno (usuarios, grupos, campos personalizados, colas, etc.) Tiene visibilidad completa de todos los tickets.

81. El usuario `operador` se crea en la instalación y en principio no tiene visibilidad sobre ninguna cola. Consulte la guía CCN-STIC 845D, Manual de Administrador de LUCIA.

4.1. CONFIGURACIÓN DE ACCESO POR LDAP

82. Es posible configurar el acceso por LDAP al portal de LUCIA.

83. Es necesario habilitar el plugin `RT::Authen::ExternalAuth` tal y como se muestra a continuación en un fichero de configuración (por ejemplo `/opt/rt4/etc/RT_SiteConfig.d/ExternalAuth_Plugin_Config.pm`):

Perl: /opt/rt4/etc/RT_SiteConfig.d/ExternalAuth_Plugin_Config.pm

```
# ...
Plugin("RT::Authen::ExternalAuth");
# ...
```

84. Y configurar los datos de conexión al LDAP:

Perl: /opt/rt4/etc/RT_SiteConfig.d/ExternalSettings_Config.pm

```
# Minimal LDAP configuration; see RT::Authen::ExternalAuth::LDAP for
# further details and examples
Set($ExternalSettings, {
    'My_LDAP'       =>  {
        'type'              =>  'ldap',
        'server'            =>  'ad.localhost.localdomain',
        # By not passing 'user' and 'pass' we are using an anonymous
        # bind, which some servers to not allow
        'user'              => 'ad_user',
        'pass'              => 'ad_password',
        'base'              =>  'dc=ad,dc=localhost,dc=localdomain',
        'filter'            =>  '(objectClass=user)',
        # Users are allowed to log in via email address or account
        # name
        'attr_match_list'   => [
            'Name',
            'EmailAddress',
        ],
        # Import the following properties of the user from LDAP upon
        # login
        'attr_map' => {
```

```
            'Name'         => 'sAMAccountName',
            'EmailAddress' => 'mail',
            'RealName'     => 'cn',
            'WorkPhone'    => 'telephoneNumber',
            'Address1'     => 'streetAddress',
            'City'         => 'l',
            'State'        => 'st',
            'Zip'          => 'postalCode',
            'Country'      => 'co',
        },
    },
} );
```

85. Destacar que el parámetro `filter` es el que restringe a qué usuarios se les permite el acceso a LUCIA, por lo que es importante configurarlo adecuadamente.

86. La primera vez que un usuario del LDAP accede a LUCIA, se le crea un nuevo usuario privilegiado en LUCIA. Este usuario, al igual que uno nuevo recién creado a través de la interfaz web, no pertenece a ningún grupo, por lo que sus permisos están limitados. Será necesario añadir a este usuario a los grupos pertinentes.

87. Por último, se debe reiniciar el servicio de Apache:

```
bash
```

```
systemctl restart httpd.service
```

F.A.Q. (PREGUNTAS Y RESPUESTAS FRECUENTES)

¿Qué debe intercambiar con el CCN-CERT para que la instancia sincronice con LUCIA Central?

88. El Organismo debe enviar los siguientes datos en un correo cifrado:
    - Clave PGP/GPG para el intercambio de correos.
    - Teléfono de contacto.
    - URL pública del servicio LUCIA.
    - Fichero `.crt` correspondiente a la parte pública de su CA.
    - Contraseña REST definida en el parámetro `$lucia_sync_client_rest_password` en el fichero `/opt/rt4/local/etc/lucia_sync_client_rest_password_Config.pm` o el fichero de configuración pertinente (consultar guía CCN-STIC 845D)
    - Nombre de la instancia en el parámetro `$lucia_rtbase_instance_name` en `/opt/rt4/local/etc/00_lucia_rtbase_instance_name_Config.pm` o el fichero de configuración pertinente (consultar guía CCN-STIC 845D)
    - Lista de colas de incidentes que van a gestionar desde su instancia de LUCIA y se desea que sincronicen con LUCIA Central. Esto incluye el caso de disponer de sonda *SAT-INET* y/o *SAT-SARA* y/o *SAT-ICS*.
    - Fichero `/media/lucia-data/etc/pki/tls/certs/ca-bundle.crt`.
89. En respuesta al correo anterior el CCN-CERT enviará de forma cifrada:
    - GUID de instancia (ver Anexo E.3)
    - Certificado de cliente y clave de cliente (ver Anexo E.3.1)

Al acceder a LUCIA obtengo un CSRF (Falsificación de petición en sitios cruzados)

90. Esto se debe a que se está intentando acceder a través de una URL no configurada en RT.
91. Salvo que se haya añadido algún otro VirtualHost, no se han debido de configurar los ficheros `/media/lucia-data/etc/httpd/conf.d/rt.conf` y `/opt/rt4/etc/RT_SiteConfig.pm` tal y como se especifica en el manual.
92. El dominio incluido en los VirtualHost del fichero `rt.conf` ha de ser el mismo que el incluido en el parámetro `$WebDomain` del fichero `RT_SiteConfig.pm`.
93. En caso de haber añadido un nuevo VirtualHost, consulte el Anexo C del presente documento.

Apache no se inicia en un entorno de doble virtualización

94. Se ha detectado que Apache tiene problemas a la hora de iniciarse en un entorno de doble virtualización (sistema virtualizado contenido sobre otro entorno virtualizado, por ejemplo VMWare ESXi sobre VMWare WorkStation), por lo que

para que arranque, se deberá reemplazar el contenido del fichero `/usr/lib/systemd/system/httpd.service` por el siguiente:

INI: /usr/lib/systemd/system/httpd.service

```
[Unit]
Description=The Apache HTTP Server
After=network.target remote-fs.target nss-lookup.target

[Service]
Type=forking
EnvironmentFile=/etc/sysconfig/httpd
ExecStart=/usr/sbin/httpd $OPTIONS -k start
ExecReload=/usr/sbin/httpd $OPTIONS -k graceful
ExecStop=/usr/sbin/httpd $OPTIONS -k graceful-stop
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

Una vez modificado el fichero, se debe reiniciar el servidor Apache.

Anexo A. GENERACIÓN DE UNA CA Y EMISIÓN DE CERTIFICADOS

95. Si no se dispone de una Autoridad Certificadora (CA) propia y no es posible emitir certificados para LUCIA a través de terceros, puede utilizar este procedimiento para generar una CA propia y emitir sus propios certificados autofirmados.

96. Es necesario tener instalado `openssl` en el sistema para poder generar la CA y cualquier otro certificado. En el ejemplo, a fin de resumir el proceso, los certificados se generan en LUCIA, aunque lo ideal a efectos de seguridad es tener la CA en una máquina aislada generada a tal efecto.

ANEXO A.1. GENERAR LA CA

97. Crear los directorios donde se generarán la CA y los certificados:

```
bash
```

```
mkdir /var/local/ca/private -p
mkdir /var/local/ca/certs
mkdir /var/local/ca/conf
mkdir /var/local/ca/crl
touch /var/local/ca/index.txt
echo '01' > /var/local/ca/serial
echo '01' > /var/local/ca/crlnumber
```

98. Crear el fichero de configuración de la CA en la ruta `/var/local/ca/conf/ca.cnf` con el siguiente contenido sustituyendo los campos marcados en amarillo por su valor correspondiente.

```
INI: /var/local/ca/conf/ca.cnf
```

```
[ ca ]
default_ca = ORGANISMO-CA
[ ORGANISMO-CA ]
dir = /var/local/ca
serial = $dir/serial
database = $dir/index.txt
new_certs_dir = $dir/certs
certificate = $dir/certs/ca.crt
private_key = $dir/private/ca.key
crl_dir = $dir/crl
crlnumber = $dir/crlnumber
# Definir caducidad default_days y default_crl_days (valor en días)
default_days = 1825
default_crl_days = 1825
default_md = sha256
preserve = no
email_in_dn = no
nameopt = default_ca
certopt = default_ca
policy = policy_match
[ policy_match ]
countryName = optional
stateOrProvinceName = optional
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[ req ]
default_bits = 4096 # Size of keys
default_keyfile = key.pem # name of generated keys
```

```
default_md = sha256 # message digest algorithm
string_mask = nombstr # permitted characters
distinguished_name = req_distinguished_name
req_extensions = v3_req
[ req_distinguished_name ]
# Variable name Prompt string
#---------------------- ---------------------------------
0.organizationName = Organization Name (company)
organizationalUnitName = Organizational Unit Name (department, division)
emailAddress = Email Address
emailAddress_max = 40
localityName = Locality Name (city, district)
stateOrProvinceName = State or Province Name (full name)
countryName = Country Name (2 letter code)
countryName_min = 2
countryName_max = 2
commonName = Common Name (hostname, IP, or your name)
commonName_max = 64
# Default values for the above, for consistency and less typing.
# Variable name Value
#---------------------- ----------------------------
0.organizationName_default = ORGANISMO
localityName_default = CIUDAD
stateOrProvinceName_default = PROVINCIA
countryName_default = ES
emailAddress_default = email@organismo.es

[ v3_ca ]
basicConstraints = CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
[ v3_req ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
```

99. Dar los permisos correctos:

```bash
chmod 700 /var/local/ca/private
chmod 700 /var/local/ca/certs
chmod 700 /var/local/ca/conf
chmod 700 /var/local/ca/crl
chmod 600 /var/local/ca/index.txt
chmod 600 /var/local/ca/crlnumber
chmod 600 /var/local/ca/serial
chmod 600 /var/local/ca/conf/ca.cnf
```

100. Generar el certificado de la CA:

```bash
openssl req -new -x509 -extensions v3_ca \
  -keyout /var/local/ca/private/ca.key \
  -out /var/local/ca/certs/ca.crt \
  -days 14610 -config /var/local/ca/conf/ca.cnf
```

101. Cuando se solicite, se debe introducir el *PEM pass phrase* y en el *Common Name* un valor como el sustituido en `ORGANISMO-CA`.

102. Copiar el certificado de la CA y darle permisos necesarios:

```
bash
```

```
cp /var/local/ca/certs/ca.crt \
  /media/lucia-data/etc/pki/tls/assets/ca_nombre.organismo.crt
chmod 644 /media/lucia-data/etc/pki/tls/assets/ca_nombre.organismo.crt
```

103. El fichero `ca_nombre.organismo.crt` es el que hay que proporcionar al CCN-CERT para la correcta sincronización de incidentes.

104. Opcionalmente también puede incluirse como autoridad de certificación raíz de confianza en el navegador para evitar el mensaje de "posible sitio fraudulento".

105. Añadir al fichero `ca-bundle.crt` el certificado de la CA recién creada:

```
bash
```

```
cat /media/lucia-data/etc/pki/tls/assets/ca_nombre.organismo.crt >> \
  /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
```

106. Garantizaremos el acceso correcto al fichero asignándole los permisos necesarios:

```
bash
```

```
chmod 644 /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
```

107. Como medida de seguridad adicional, se establecerá en la configuración de Apache que sólo se admitan certificados generador por la CA de LUCIA Central y por la nuestra. Para ello, se sustituirá en el fichero `/etc/httpd/conf.d/rt.conf` la ocurrencia `ORGANISMO-CA` por el *Common Name* introducido en la generación de la CA:

```
Apache: /etc/httpd/conf.d/rt.conf
```

```
# Lucia default access
<VirtualHost *:443>
# [...]
<Directory /opt/rt4/>
    Order allow,deny
    Allow from all
    Require all granted

    SSLRequire(%{SSL_CLIENT_I_DN_CN}=="LUCIA CCN-CERT"||%{SSL_CLIENT_I_DN_CN}=="ORGANISMO-
CA")
</Directory>
# [...]
</VirtualHost>
```

ANEXO A.2. GENERAR UN CERTIFICADO DE SERVIDOR

108. **IMPORTANTE:** El valor del campo *Common Name* debe coincidir con el FQDN (p.ej. `lucia.organismo.es`) utilizado en la URL de servicio de LUCIA (p.ej. `https://lucia.organismo.es`).

109. Ejecutar los siguientes comandos:

```
bash
```

```
# Introducir como “Common Name” el dominio FQDN de LUCIA: nombre.organismo
openssl req -new -nodes \
  -out /var/local/ca/certs/nombre.organismo.csr \
  -keyout /var/local/ca/private/nombre.organismo.key \
  -config /var/local/ca/conf/ca.cnf
openssl ca \
  -out /var/local/ca/certs/nombre.organismo.crt \
  -config /var/local/ca/conf/ca.cnf \
  -infiles /var/local/ca/certs/nombre.organismo.csr
```

110. Copiar el certificado y establecer los permisos correctos:

```
bash
```

```
cp /var/local/ca/certs/nombre.organismo.crt \
  /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
cp /var/local/ca/private/nombre.organismo.key \
  /media/lucia-data/etc/pki/tls/private/server_lucia.key
chmod 644 /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
chmod 600 /media/lucia-data/etc/pki/tls/private/server_lucia.key
chcon unconfined_u:object_r:cert_t:s0 \
  /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
chcon unconfined_u:object_r:cert_t:s0 \
  /media/lucia-data/etc/pki/tls/private/server_lucia.key
chmod 600 /var/local/ca/certs/*
chmod 600 /var/local/ca/private/*
```

ANEXO A.3. GENERAR UN CERTIFICADO DE CLIENTE

111. Ejecutar los siguientes comandos:

```
bash
```

```
# Introducir como “Common Name” el cliente: nombre.cliente
openssl req -new -nodes \
  -out /var/local/ca/certs/nombre.cliente_nombre.organismo.csr \
  -keyout /var/local/ca/private/nombre.cliente_nombre.organismo.key \
  -config /var/local/ca/conf/ca.cnf
openssl ca \
  -out /var/local/ca/certs/nombre.cliente_nombre.organismo.crt \
  -config /var/local/ca/conf/ca.cnf \
  -infiles /var/local/ca/certs/nombre.cliente_nombre.organismo.csr
```

112. En las siguientes rutas se tendrán generados el certificado de cliente y su clave:

```
/var/local/ca/certs/nombre.cliente_nombre.organismo.crt
/var/local/ca/private/nombre.cliente_nombre.organismo.key
```

113. Por último, se genera un certificado protegido por contraseña en formato p12 para importarlo en el navegador del usuario que vaya a conectarse a LUCIA:

```
bash
```

```
openssl pkcs12 -export \
  -in /var/local/ca/certs/nombre.cliente_nombre.organismo.crt \
  -inkey /var/local/ca/private/nombre.cliente_nombre.organismo.key \
  -certfile /media/lucia-data/etc/pki/tls/assets/ca_nombre.organismo.crt \
  -out /var/local/ca/certs/nombre.cliente_nombre.organismo.p12
```

ANEXO A.4. GENERAR LA LISTA DE REVOCACIÓN DE USUARIOS (CRL)

114. La CRL (Certificate Revocation List) debe ser regenerada cada X días, acorde al parámetro `default_crl_days` establecido en el fichero de configuración `/var/local/ca/conf/ca.cnf`.

```bash
openssl ca \
  -config /var/local/ca/conf/ca.cnf \
  -gencrl -out /var/local/ca/crl/crl_nombre.organismo.pem
```

115. Copiar al directorio indicado:

```bash
cp /var/local/ca/crl/crl_nombre.organismo.pem /media/lucia-data/etc/pki/tls/crl/crl.pem
```

116. Volcar la CRL recién generada en el fichero `ca-bundle.crl`:

```bash
cat /media/lucia-data/etc/pki/tls/crl/crl.pem >> \
  /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
chmod 644 /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
```

117. Y, en el fichero `/etc/httpd/conf.d/rt.conf`, activar (eliminando los `#`) las directivas `SSLCARevocationFile` y `SSLCARevocationCheck` (resaltado):

```bash
# Lucia default access
<VirtualHost *:443>
# [...]

SSLVerifyClient require
SSLVerifyDepth 2
SSLCACertificateFile /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt

SSLCARevocationFile /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
SSLCARevocationCheck leaf
```

118. Una vez hecho esto, se debe reiniciar el servicio Apache:

```bash
systemctl restart httpd.service
```

119. En caso de necesitar revocar un certificado se debe ejecutar el siguiente comando:

```bash
openssl ca \
  -config /var/local/ca/conf/ca.cnf \
  -revoke /var/local/ca/certs/nombre.cliente_nombre.organismo.crt
```

120. Volver a regenerar la CRL y copiar al directorio indicado:

```bash
openssl ca \
  -config /var/local/ca/conf/ca.cnf \
  -gencrl -out /var/local/ca/crl/crl_nombre.organismo.pem
cp /var/local/ca/crl/crl_nombre.organismo.pem /media/lucia-data/etc/pki/tls/crl/crl.pem
```

121. Volcar todas las CRL existentes en el fichero `ca-bundle.crl`. Primero la de LUCIA y, a continuación, la regenerada. Si hubiese alguna CRL más, se debería volcar también:

```bash
cat /media/lucia-data/etc/pki/tls/crl/subca_lucia.crl > \
  /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
cat /media/lucia-data/etc/pki/tls/crl/crl.pem >> \
  /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
chmod 644 /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
```

122. Una vez hecho esto, reiniciar el servicio de Apache:

```bash
systemctl restart httpd.service
```

123. Se pueden comprobar los certificados revocados con el comando:

```bash
openssl crl -in /var/local/ca/crl/crl_nombre.organismo.pem -noout -text
```

ANEXO A.5. CAMBIAR EL FORMATO DE LOS CERTIFICADOS

124. Los certificados pueden almacenarse en varios formatos. LUCIA utiliza archivos CRT para la información del certificado y archivos KEY para las claves.

125. Para convertir un certificado en formato CER a formato CRT, se debe ejecutar:

```bash
openssl pkcs7 -text -in certfile.cer -print_certs -outform PEM -out certfile.pem
```

126. Para convertir de un certificado en formato PFX a formatos CRT y KEY, se debe ejecutar:

```bash
openssl pkcs12 -in certfile.pfx -clcerts -nokeys -out certfile.cer
openssl pkcs12 -in certfile.pfx -nocerts -nodes  -out certfile.key
```

Anexo B. AUMENTO DE LA PARTICIÓN DE DATOS

127. **ATENCIÓN**: Este proceso puede causar pérdida de datos y por tanto se recomienda realizar una copia de seguridad de la máquina completa.

128. LUCIA dispone de un primer disco que contiene el sistema operativo (`lucia-so.vmdk` 55GB) y de un segundo disco donde se encuentra toda la configuración y la instalación del software de gestión de tickets (`lucia-data.vmdk` 50GB).

129. Si fuese necesario ampliar la capacidad del segundo disco inicialmente o si el sistema se queda sin espacio de almacenamiento, será necesario previamente redimensionar en la infraestructura virtual el segundo disco que está etiquetado como `lucia-data.vmdk` y tiene una sola partición en `/dev/sdb1`.

130. Con la máquina virtual de LUCIA apagada, hay que conectarse por consola al servidor VMware ESXi (por SSH si está habilitado) y utilizar el comando `vmkfstools` pasando como parámetros el nuevo tamaño del disco (en el ejemplo 120GB) y la ubicación del fichero del disco virtual `lucia-data.vmdk`:

```
bash (VMWare ESXi)
vmkfstools -X 120g /vmfs/volumes/datastore1/LUCIA/lucia-data.vmdk
```

131. Se debe añadir un dispositivo virtual CD-ROM a la infraestructura virtual y cargar la imagen ISO de la aplicación GPARTED (descargable de http://gparted.org).

132. Arrancaremos LUCIA desde el CD y una vez que termine de cargar GPARTED, podremos extender la partición al tamaño que previamente le asignamos desde la infraestructura virtual.

133. Una vez finalizada la operación y apagada la máquina, se puede eliminar el dispositivo virtual CD-ROM y arrancar LUCIA para comprobar el resultado mediante el comando:

```
bash (VMWare ESXi)
df –h /dev/sdb1
```

Anexo C. AÑADIR VIRTUALHOST

134. Si se desea añadir un segundo VirtualHost para, por ejemplo, la recepción de peticiones REST, se añadirá lo siguiente en el fichero `/etc/httpd/conf.d/rt.conf`:

Apache: /etc/httpd/conf.d/rt.conf

```
[...]
<VirtualHost *:443>
   ServerName lucia-rest.organismo.es:443
   AddDefaultCharset UTF-8
   DocumentRoot /opt/rt4/share/html
   Alias /NoAuth/images/ /opt/rt4/share/html/NoAuth/images/
   ScriptAlias / /opt/rt4/sbin/rt-server.fcgi/
   <Location />
      Require all granted
   </Location>
   <Directory /opt/rt4/>
      Order allow,deny
      Allow from all
      Require all granted
     SSLRequire(%{SSL_CLIENT_I_DN_CN}=="LUCIA CCN-
CERT"||%{SSL_CLIENT_I_DN_CN}=="<ORGANISMO-CA>")
   </Directory>

   SSLEngine on

   SSLCertificateFile    /media/lucia-data/etc/pki/tls/certs/server_lucia-rest.crt
   SSLCertificateKeyFile /media/lucia-data/etc/pki/tls/private/server_lucia-rest.key

   SSLVerifyClient require
   SSLVerifyDepth 2
   SSLCACertificateFile /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt

   ErrorLog /opt/rt4/var/log/httpd.lucia-rest.error.log
   LogLevel warn
   CustomLog /opt/rt4/var/log/httpd.lucia-rest.access.log combined

   ServerSignature Off

</VirtualHost>
[...]
```

135. Teniendo en cuenta que el certificado y la clave para este VirtualHost deben existir en las rutas especificadas:

```
/media/lucia-data/etc/pki/tls/certs/server_lucia-rest.crt
/media/lucia-data/etc/pki/tls/private/server_lucia-rest.key
```

136. Además, por cada VirtualHost adicional apuntando a RT que añadamos, deberemos configurar el parámetro `@ReferrerWhitelist` para evitar un error CSRF en el fichero `/opt/rt4/etc/RT_SiteConfig.pm`:

Perl

```
# ...
Set(@ReferrerWhitelist, qw(lucia.localhost.localdomain:80
lucia-rest.organismo.es:443));
# ...
```

137.Por último, reiniciar el servidor web:

```bash
systemctl restart httpd.service
```

Anexo D. FORMULARIO DE RECOGIDA DE DATOS DE INSTALACIÓN

138. El siguiente texto se encuentra disponible como documento de texto plano para su descarga y uso como anexo independiente.

```
==================================
== LUCIA - DATOS DE INSTALACIÓN ==
==================================
- El siguiente formulario recopila los datos necesarios para una correcta instalación de
una instancia de LUCIA cuyo proceso queda recogido en el documento "CCN-STIC 845C – LUCIA.
MANUAL DE INSTALACIÓN". Cualquier aclaración sobre los parámetros indicados puede
encontrarla en dicho manual.
- Toda contraseña no solicitada a continuación, será la definida por defecto en el manual
de instalación en el cual se indica como modificarlas.
- Recuerde que dada la sensibilidad de la información contenida en este formulario, debe
ser cifrado si es remitido por correo.
==================================

____________
HARDWARE

* ¿Se dispone de un servidor de virtualización donde se va a desplegar LUCIA (ESXi, HyperV,
...) con un mínimo de 2GB RAM y 120GB HDD? [SI | NO]:
* Tamaño deseado del disco de datos (lucia-data.vmdk – Por defecto 50GB):
_____________________________
CONFIGURACIÓN DE RED

* IP privada:
* Mascara de red:
* Puerta de enlace:
* Servidores DNS:
* Nombre de máquina completo (FQDN):
* Nombre DNS visible en Internet:
_____________________________
CONFIGURACIÓN DE SISTEMA

* Nueva contraseña para usuario nopriv del sistema:
* Nueva contraseña para usuario root del sistema:
* Nueva contraseña para usuario rt_user de base de datos:
* Nueva contraseña para usuario rt4_sync de base de datos:
* Nueva contraseña para usuario root de base de datos:
* Nueva contraseña para usuario root del portal web:


_____________________________________
CONFIGURACIÓN DE CERTIFICADOS (En caso de no disponer de una CA propia)

-- Generación de la CA --

* Nombre común de la CA (CN - Common Name):
* Caducidad de la CA (en días):
* Nombre del organismo:
* Ciudad:
* Provincia:
* Correo electrónico:
* Contraseña de la CA:
* ¿Se desea utilizar listas de revocación de certificados (CRL)? [SI | NO]:
  => Caducidad de la CRL (en días):


-- Generación del certificado de cliente --

* Nombre del certificado de cliente:
* Contraseña de importación del certificado PEM:
_____________________________________________________
CONFIGURACIÓN DEL SERVICIO DE GESTIÓN DE TICKETS

* Nombre de la instancia LUCIA (Ejemplo: CCN-CERT):
* URL del organismo (Ejemplo: https://www.ccn-cert.cni.es):
* URL de servicio de LUCIA (Ejemplo: lucia.ccn-cert.cni.es):
* Contraseña del usuario de sincronización REST:
```

```
_____________________________________________
CONFIGURACIÓN DEL CORREO ELECTRÓNICO

-- Configuración IMAP/POP3 --

* ¿Se usará protocolo IMAP (recomendado) o POP3?:
* Nombre del servidor IMAP/POP3:
* Puerto IMAP/POP3 (Por defecto 143/110):
* IP del servidor IMAP/POP3:

-- Configuración SMTP --

* Nombre del servidor SMTP:
* IP del servidor SMTP:
* Puerto SMTP (Por defecto 25):

-- Configuración de buzones de correos --

* Cuenta de correo de Incidentes propios y recepción de Reportes de Incidentes
  => Cuenta de correo:
  => Usuario:
  => Contraseña:
  => Alias de la cuenta:

* Cuenta de correo de Incidentes SAT-INET (Si se dispone del servicio)
  => Cuenta de correo:
  => Alias de la cuenta:

* Cuenta de correo de Incidentes SAT-SARA (Si se dispone del servicio)
  => Cuenta de correo:
  => Alias de la cuenta:

  * Cuenta de correo de Incidentes SAT-ICS (Si se dispone del servicio)
  => Cuenta de correo:
  => Alias de la cuenta:

* Remitente de los correos para respuestas autogeneradas por LUCIA (Ejemplo:
incidentes@ccn-cert.cni.es):

* Remitente por defecto de los correos para comentarios autogenerados por LUCIA (Ejemplo:
incidentes@ccn-cert.cni.es):

* Dirección a la que se enviarán informes de error en la sincronización (Ejemplo:
error_sync_lucia@ccn-cert.cni.es):
```

Anexo E. INSTALACIÓN MANUAL DE LUCIA

ANEXO E.1. CONFIGURACIÓN INICIAL

ANEXO E.1.1. ESTABLECER EL NOMBRE DE LA MÁQUINA

139. Se debe configurar LUCIA con un nombre de dominio. El nombre de dominio recomendado sería similar a `lucia.organismo.es`, coincidiendo con el nombre que tenga en el DNS visible a Internet, pero cualquier nombre de dominio válido funcionará. A efectos de este manual, el nombre de dominio será `<nombre.dominio>`.

140. Para establecer el nombre FQDN de la máquina se ejecutará:

```
bash
hostnamectl set-hostname <nombre.dominio>
```

141. Para comprobar que el nombre es correcto:

```
bash
hostname -f
```

ANEXO E.1.2. CONFIGURACIÓN DE FECHA Y HORA

142. La máquina viene instalada y configurada con el servicio de sincronización de tiempo `chrony` apuntando al servicio del *Real Observatorio de la Armada* (`hora.roa.es`), por lo que no es necesario instalar otros servicios como `ntp` con los que tendría conflicto.

143. Se puede comprobar que la hora es correcta y el servicio se está ejecutando mediante:

```
bash
date
systemctl status chronyd
```

144. Las fuentes de sincronización se muestran ejecutando:

```
bash
chronyc sources
```

ANEXO E.1.3. CERTIFICADOS DIGITALES DEL SERVIDOR WEB

145. La conexión a LUCIA se realizará siempre a través de SSL, por lo que es necesario disponer de un certificado digital válido para el servidor; no debe estar caducado y el nombre del dominio debe coincidir con su *Common Name* (`CN`).

146. A su vez, para la conexión de cualquier usuario a la interfaz de LUCIA será necesario un certificado de cliente emitido por la Autoridad Certificadora instalada en la instancia.

147. Se puede disponer de una Autoridad Certificadora propia para emitir certificados o utilizar aquellos emitidos por un tercero. En otro caso, puede generarse una Autoridad Certificadora dedicada para LUCIA siguiendo las instrucciones definidas en el Anexo A de este documento y continuando la configuración directamente en el siguiente punto "Configuración de Apache HTTP server".

148. Una vez se disponga de un certificado de servidor, el certificado de la CA (Autoridad de Certificación) principal y los certificados de las CAs intermedias si existieran, se puede proceder a configurar la conexión SSL del servidor.

149. Se deben crear los siguientes ficheros, respetando nombre y ruta, con el contenido en formato PEM de nuestro certificado y de nuestra clave privada respectivamente (consultar Anexo A.5 "Cambiar el formato de los certificados"):

```
/media/lucia-data/etc/pki/tls/certs/server_lucia.crt
/media/lucia-data/etc/pki/tls/private/server_lucia.key
```

150. Para garantizar el acceso restringido a los ficheros:

```bash
chmod 644 /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
chown root /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
chcon unconfined_u:object_r:cert_t:s0 /media/lucia-data/etc/pki/tls/certs/server_lucia.crt
chmod 600 /media/lucia-data/etc/pki/tls/private/server_lucia.key
chown root /media/lucia-data/etc/pki/tls/private/server_lucia.key
chcon unconfined_u:object_r:cert_t:s0 \
  /media/lucia-data/etc/pki/tls/private/server_lucia.key
```

151. Se deben incluir los ficheros de la CA y los de las CAs intermedias en el directorio `/media/lucia-data/etc/pki/tls/assets/`

152. Se deben incluir en un solo fichero `ca-bundle.crt` todos los certificados de la CA principal y de las CAs secundarias si existiesen:

```bash
cat /media/lucia-data/etc/pki/tls/assets/ca_<principal>.crt >> \
  /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
cat /media/lucia-data/etc/pki/tls/assets/ca_<secundaria>.crt >> \
  /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
# [...]
```

153. Y garantizar el acceso correcto al fichero asignándole los permisos necesarios:

```bash
chmod 644 /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt
```

154. Si se desea trabajar con CRL[4]s, se debe copiar la CRL del organismo (en formato `pem`) en la maqueta:

[4] CRL "Certificate Revocation List"

```
bash
cp <crl_organismo>.pem /media/lucia-data/etc/pki/tls/crl/crl.pem
```

155. Y volcar todas las CRL existentes en un fichero:

```
bash
cat /media/lucia-data/etc/pki/tls/crl/*.pem > \
  /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
chmod 644 /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
```

156. Y en el fichero `/etc/httpd/conf.d/rt.conf` activar las directivas `SSLCARevocationFile` y `SSLCARevocationCheck` (resaltado):

```
Apache: /etc/httpd/conf.d/rt.conf
# Lucia default access
<VirtualHost *:443>
[...]
SSLCACertificateFile /media/lucia-data/etc/pki/tls/certs/ca-bundle.crt

SSLCARevocationFile /media/lucia-data/etc/pki/tls/crl/ca-bundle.crl
SSLCARevocationCheck leaf
```

157. Por último, por motivos de seguridad se debe introducir el *Common Name* de la CA de nuestro organismo en el VirtualHost de Apache en `/etc/httpd/conf.d/rt.conf`:

```
Apache: /etc/httpd/conf.d/rt.conf
# Lucia default access
<VirtualHost *:443>
   ServerName <nombre.dominio>:443
   AddDefaultCharset UTF-8
   DocumentRoot /opt/rt4/share/html
   Alias /NoAuth/images/ /opt/rt4/share/html/NoAuth/images/
   ScriptAlias / /opt/rt4/sbin/rt-server.fcgi/
   <Location />
     Require all granted
   </Location>
   <Directory /opt/rt4/>
     Order allow,deny
     Allow from all
     Require all granted
     SSLRequire(%{SSL_CLIENT_I_DN_CN}=="LUCIA CCN-
CERT"||%{SSL_CLIENT_I_DN_CN}=="<ORGANISMO-CA>")
   </Directory>
```

ANEXO E.1.4. CONFIGURACIÓN DE APACHE HTTP SERVER

158. En el fichero `/media/lucia-data/etc/httpd/conf.d/rt.conf` se encuentra la configuración del servidor web y es necesario editarla para que LUCIA funcione correctamente.

159. En concreto se debe realizar una sustitución de la cadena `<nombre.dominio>` por el nombre de dominio definido, por ejemplo `lucia.organismo.es` (sin los símbolos "`<`" y "`>`"). Se debe editar el fichero y sustituir las cinco ocurrencias que se

encuentran. Es importante no modificar la línea `ServerName lucia.localhost.localdomain:80` de la directiva `<VirtualHost *:80>` manteniendo la referencia a `lucia.localhost.localdomain:80` tal y como aparece.

ANEXO E.1.5. CONFIGURACIÓN DEL SERVICIO DE GESTIÓN DE TICKETS

160. El siguiente paso es la configuración del servicio de gestión de tickets y consiste en la edición de varios parámetros de configuración. Se ha de cumplir la sintaxis del archivo de ejemplo mostrado, sustituyendo los parámetros con los valores correspondientes del organismo en los ficheros de configuración[5]:

Perl: /opt/rt4/etc/RT_SiteConfig.pm

```
# ...
# Nombre de la instancia LUCIA – Ejemplo: CCN-CERT
Set( $rtname, 'nombre_organismo' );
# URL del organismo – Ejemplo: https://www.ccn-cert.cni.es
Set( $Organization, 'url_organismo' );
# URL de servicio de LUCIA (¡¡No poner http/https!!) – Ejemplo: lucia.ccn-cert.cni.es
Set( $WebDomain, 'nombre_dominio' );
# Remitente por defecto de los correos para respuestas autogeneradas por LUCIA
# Ejemplo: incidentes@ccn-cert.cni.es
Set( $CorrespondAddress, 'incidentes@organismo.es' );
# Remitente por defecto de los correos para comentarios autogenerados por LUCIA
# Ejemplo: incidentes@ccn-cert.cni.es
Set( $CommentAddress, 'incidentes@organismo.es' );
# Dirección a la que se enviarán informes de error en la sincronización
# Ejemplo: error_sync_lucia@ccn-cert.cni.es
Set( $OwnerEmail, 'error_sync_lucia@organismo.es' );
# ...
```

Perl: /opt/rt4/local/etc/00_lucia_rtbase_instance_name_Config.pm

```
use utf8;

# Nombre de la instancia LUCIA (mismo valor que $rtname) - Ejemplo: CCN-CERT
Set( $lucia_rtbase_instance_name, 'nombre_organismo' );

1;
```

Perl: /opt/rt4/local/etc/lucia_sync_client_rest_credentials_Config.pm

```
use utf8;

# Contraseña del usuario de sincronización REST
Set( $lucia_sync_client_rest_user, 'rest' );
# Contraseña del usuario de sincronización REST
Set( $lucia_sync_client_rest_password, 'contraseña_usuario_rest' );

1;
```

161. Las direcciones de correo de notificación asociadas (y sus respectivos aliases) se especifican por cola[6]:

[5] En LUCIA REV3.1 y anteriores, `$lucia_rtbase_instance_name` se llamaba `$LuciaInstanceName`, `$lucia_sync_client_rest_user` no existía, `$lucia_sync_client_rest_password` se llamaba `$LuciaRestPassword`, y estaban en `/opt/rt4/etc/RT_SiteConfig.pm`.

[6] En LUCIA REV3.1 y anteriores, `%lucia_rtbase_email_address_for_queue` y `%lucia_rtbase_email_address_alias_for_queue` se llamaban respectivamente `%LuciaTicketCategoryEmailAddresses` y `%LuciaTicketCategoryEmailAddressesAliases`, ubicados en en `/opt/rt4/etc/RT_SiteConfig.pm`.

```
Perl: /opt/rt4/local/etc/lucia_rtbase_email_address_for_queue_Config.pm
```

```
use utf8;

# Cuentas de correo asociadas a las colas
Set( %lucia_rtbase_email_address_for_queue, (
    '' => 'dirección_notificacion_por_defecto@nombre_organismo',
    'nombre_cola' => 'dirección_notificacion_para_nombre_cola@nombre_organismo',
    # ...
));

1;
```

```
Perl: /opt/rt4/local/etc/lucia_rtbase_email_address_alias_for_queue_Config.pm
```

```
use utf8;

# Cuentas de correo asociadas a las colas
Set( %lucia_rtbase_email_address_aslias_for_queue, (
    '' => 'alias_dirección_notificacion_por_defecto@nombre_organismo',
    'nombre_cola' => 'alias_dirección_notificacion_para_nombre_cola@nombre_organismo',
    # ...
));

1;
```

162. Los valores que se deben incluir en estos parámetros (nombre de la instancia, urls, direcciones de correo y contraseña) han de ser propios del organismo; es decir, no serán valores facilitados por el CCN-CERT.

163. Una vez definida la configuración, se deben ejecutar los siguientes comandos para inicializar la instancia de LUCIA:

```
bash
```

```
rm -rf /opt/rt4/var/mason_data/obj
systemctl restart httpd.service
# initialize-lucia.in ya no es necesario desde LUCIA REV4.0
# perl /opt/rt4/local/plugins/RT-Extension-Lucia/bin/initialize-lucia.in
# systemctl restart httpd.service
```

164. Este comando solicitará la contraseña del usuario `root` de la base de datos. La contraseña por defecto para este usuario es `LuC14MySQLR00T`.

ANEXO E.2. CONFIGURACIÓN DEL CORREO ELECTRÓNICO

ANEXO E.2.1. RECEPCIÓN DE CORREOS

165. Para configurar la recepción de correo en LUCIA se recomienda utilizar un buzón IMAPS utilizando la herramienta preconfigurada `fetchmail`.

166. **NOTA**: Si no se dispone de un DNS interno para resolver correctamente el servidor de correo, es necesario añadir la siguiente entrada en el fichero `/etc/hosts`:

```
/etc/hosts
```

```
<dirección_IP_mail.server> <mail.server>
```

167. Es necesario crear el fichero `/media/lucia-data/usr/bin/fetchmailrc.sh` definiendo la cuenta de correo donde se recibirán los reportes de incidentes externos (no aplica a las cuentas de correo de SAT-INET, SAT-SARA y SAT-ICS), sustituyendo los valores `<mail.server>` (FQDN), `<usuario>` y `<contraseña>` (**Nota: no modificar la URL** `http://lucia.localhost.localdomain`).

```
/media/lucia-data/usr/bin/fetchmailrc.sh

# Global Settings
set logfile "/opt/rt4/var/log/fetchmail.log"
# set syslog
# User mail box setting – CUENTA DE INCIDENTES PROPIOS DEL ORGANISMO
poll <mail.server> protocol IMAP
   user "<usuario>" there with password "<contraseña>"
   nofetchall keep
   ssl
#  sslcertck sslcertpath /etc/pki/tls/certs/
   mda "/opt/rt4/bin/rt-mailgate --no-verify-ssl --url http://lucia.localhost.localdomain
--queue 'Incident Reports - <nombre_organismo>' --action correspond-linktoticket"
```

168. Si se utilizara POP3 (no recomendado), la configuración es similar cambiando únicamente la línea donde se menciona IMAP por POP3:

```
/media/lucia-data/usr/bin/fetchmailrc.sh

# ...
# User mail box setting
poll <mail.server> protocol POP3
# ...
```

169. En el caso de que no se utilizasen los puertos por defecto para el protocolo seleccionado, la configuración sería de la siguiente manera:

```
/media/lucia-data/usr/bin/fetchmailrc.sh

# ...
# User mail box setting
poll <mail.server> protocol IMAP:<puerto>
# ...
```

170. Si el nombre del servidor de correo es distinto al dominio de la dirección de correo, es necesario escribir la dirección completa en `<usuario>`:

```
/media/lucia-data/usr/bin/fetchmailrc.sh

# ...
# User mail box setting – CUENTA DE INCIDENTES PROPIOS DEL ORGANISMO
poll <mail.server> protocol IMAP
   user "<usuario@dominio.correo>" there with password "<contraseña>"
# ...
```

171. Es necesario dar permisos a los ficheros asociados a este proceso:

```
bash

touch /opt/rt4/var/log/fetchmail.log
chown rtcronuser:apache /opt/rt4/var/log/fetchmail.log
chmod 660 /opt/rt4/var/log/fetchmail.log
```

```
chown rtcronuser /media/lucia-data/usr/bin/fetchmailrc.sh
chmod 600 /media/lucia-data/usr/bin/fetchmailrc.sh
```

172. En versiones previas a LUCIA REV4.0, es necesario editar el `cron` de `root` mediante la instrucción (edición similar a `vi`) añadiendo una entrada para comprobar el correo entrante periódicamente:

```
bash
```

```
crontab -e
```

```
crontab
```

```
# Check incoming emails
* * * * * su rtcronuser -s "/bin/sh" -c "fetchmail --pidfile /tmp/.fetchmail.pid -f
/media/lucia-data/usr/bin/fetchmailrc.sh"
```

173. **NOTA**: El comportamiento de RT consiste en procesar todos aquellos correos en los buzones monitorizados que se encuentren como no leídos, y tras gestionarlos, marcarlos como leídos. Por otro lado, incorpora un control de bucles de correo bastante depurado dado que en la mayoría de las ocasiones se utiliza la misma cuenta para recibir el correo y las notificaciones generadas por el sistema. En caso de que se considere que genera notificaciones no deseadas en las colas de LUCIA, se puede optar por separar las cuentas de notificación o configurar `procmail` para procesar con antelación el correo no deseado marcándolo como leído (configuración fuera del alcance de este manual).

ANEXO E.2.2. ENVÍO DE CORREOS

174. Para el envío de correos es necesario un servidor STMP que permita hacer *relay* de los correos que envía LUCIA. `postfix` está preinstalado en la máquina virtual, pero se debe configurar adecuadamente.

175. Crear el fichero `/etc/postfix/sasl_passwd` con los datos de conexión de la cuenta de envío de correos que se vaya a utilizar en el servidor SMTP:

```
/etc/postfix/sasl_passwd
```

```
[<smtp.server>] <usuario_de_incidentes>:<contraseña>
```

176. Así mismo, si no se utilizase el puerto por defecto, la configuración de la cuenta para el envío de correos sería de la siguiente forma:

```
/etc/postfix/sasl_passwd
```

```
[<smtp.server>]:<puerto> <usuario_de_incidentes>:<contraseña>
```

177. Si el nombre del servidor de correo es distinto al dominio de la dirección de correo, es necesario escribir la dirección completa en `<usuario>`:

```
/etc/postfix/sasl_passwd
```

```
[<smtp.server>] <usuario_incidentes@dominio.correo>:<contraseña>
```

178. Solo el usuario `root` debe poder acceder a este fichero:

```
bash
```

```
chmod 600 /etc/postfix/sasl_passwd
```

179. Es necesario ejecutar el siguiente comando tanto en este momento como ante cualquier cambio realizado en el fichero anterior:

```
bash
```

```
postmap /etc/postfix/sasl_passwd
```

180. **Nota**: Si no se dispone de un DNS interno para resolver correctamente el servidor SMTP, es necesario añadir la siguiente entrada en el fichero `/etc/hosts`:

```
/etc/hosts
```

```
<dirección_IP_smtp.server> <smtp.server>
```

181. El siguiente paso será modificar la configuración de `postfix` en el fichero `/etc/postfix/main.cf` con nuestros parámetros añadiendo las siguientes líneas. Es importante que los corchetes en la opción `relayhost` se mantengan:

```
/etc/postfix/main.cf
```

```
# ...
# enable SASL authentication
smtp_sasl_auth_enable = yes
# tell Postfix where the credentials are stored
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
# use STARTTLS for encryption
smtp_use_tls = yes
relayhost = [<smtp.server>]
disable_dns_lookups = yes
```

182. De la misma manera, si no se utilizase el puerto por defecto, la configuración del parámetro `relayhost` sería de la siguiente forma:

```
/etc/postfix/main.cf
```

```
# ...
relayhost = [<smtp.server>]:<puerto>
```

183. Para aplicar estos cambios, es necesario recargar el servicio:

```
bash
```

```
postfix reload
```

184. Respecto a la configuración de RT, de cara a evitar posibles errores con ciertos servidores de correo, se debe establecer en el fichero de configuración `/opt/rt4/local/etc/OverrideOutgoingMailFrom_Config.pm` el mapeo de las direcciones de correo del remitente de cada cola, con las que se sobrescribirá la cabecera `Return-Path: apache@localhost` en los correos enviados desde LUCIA:

```
/opt/rt4/local/etc/OverrideOutgoingMailFrom_Config.pm
```

```
use utf8;

Set($OverrideOutgoingMailFrom, {
    'Default' => 'cuenta@dominio.correo',
    'Incidents - nombre_organismo' => 'cuenta@dominio.correo',
    'Incident Reports - nombre_organismo' => 'cuenta@dominio.correo',
    'Investigations - nombre_organismo' => 'cuenta@dominio.correo',
    # ...
});

1;
```

ANEXO E.2.3. NOTIFICACIONES INTERNAS

185. El último paso consiste en configurar las direcciones de notificación al propio organismo. Puede ocurrir que las direcciones de respuesta y comentario de LUCIA definidas en los parámetros `$CorrespondAddress` y `$CommentAddress` sean la misma que alguna de las definidas en `%lucia_rtbase_email_address_for_queue`[7], que se utilizan para las notificaciones al propio organismo:

186. **Si las cuentas de correo de respuesta y comentario NO COINCIDEN:** Definir en el parámetro `%lucia_rtbase_email_address_alias_for_queue`[8] las mismas cuentas de correo definidas en el parámetro `%lucia_rtbase_email_address_for_queue`:

```
Perl: /opt/rt4/local/etc/lucia_rtbase_email_address_for_queue_Config.pm
```

```
use utf8;

# Cuentas de correo asociadas a las colas
Set( %lucia_rtbase_email_address_for_queue, (
    '' => 'dirección_notificacion_por_defecto@nombre_organismo',
    'nombre_cola' => 'dirección_notificacion_para_nombre_cola@nombre_organismo',
    # ...
));

1;
```

```
Perl: /opt/rt4/local/etc/lucia_rtbase_email_address_alias_for_queue_Config.pm
```

```
use utf8;

# Cuentas de correo asociadas a las colas
Set( %lucia_rtbase_email_address_aslias_for_queue, (
    '' => 'dirección_notificacion_por_defecto@nombre_organismo',
    'nombre_cola' => 'dirección_notificacion_para_nombre_cola@nombre_organismo',
    # ...
));
```

[7] En LUCIA REV3.1 y anteriores, llamado `$LuciaTicketCategoryEmailAddresses`.
[8] En LUCIA REV3.1 y anteriores, llamado `$LuciaTicketCategoryEmailAddressesAliases`.

```
1;
```

```
bash
systemctl restart httpd.service
```

187. **Si las cuentas de correo de respuesta y comentario COINCIDEN:** Esta situación es detectada por RT como un bucle de correo por lo que las notificaciones de aviso no se enviarían. Para solucionarlo, se ha de crear en el servidor de correo (NO en LUCIA) un alias para cada una de las cuentas. Si el servidor de correo está basado en Linux, añadir las siguientes líneas en `/etc/aliases`:

```
/etc/aliases
<alias_correo_de_incidentes@organismo.es> : <correo_de_incidentes@organismo.es>
<alias_correo_de_sat-inet@organismo.es> : <correo_de_sat-inet@organismo.es>
<alias_correo_de_sat-sara@organismo.es> : <correo_de_sat-sara@organismo.es>
<alias_correo_de_sat-ics@organismo.es> : <correo_de_sat-ics@organismo.es>
```

```
bash (SMTP server)
newaliases
```

En caso de usar Microsoft Exchange Server, consultar la documentación al respecto.

De vuelta en LUCIA, definir los alias de las cuentas de correo en el parámetro `%lucia_rtbase_email_address_alias_for_queue`:

```
Perl: /opt/rt4/local/etc/lucia_rtbase_email_address_alias_for_queue_Config.pm
use utf8;

# Cuentas de correo asociadas a las colas
Set( %lucia_rtbase_email_address_aslias_for_queue, (
    '' => 'alias_dirección_notificacion_por_defecto@nombre_organismo',
    'nombre_cola' => 'alias_dirección_notificacion_para_nombre_cola@nombre_organismo',
    # ...
));

1;
```

```
bash
systemctl restart httpd.service
```

ANEXO E.3. COMUNICACIÓN CON LUCIA CENTRAL

188. Este apartado cubre la configuración de la instancia de organismo para configurar la sincronización de tickets con LUCIA Central en el CCN-CERT.

189. La comunicación con LUCIA Central se realiza a través de una conexión SSL en ambos sentidos, por tanto, es necesario disponer de un certificado de cliente emitido por el CCN-CERT. La CA que emite estos certificados ya está debidamente configurada en la máquina virtual proporcionada. Además, deberán proporcionarse al CCN-CERT

los certificados de la CA (y CAs secundarias del certificado si existen) del servidor configurado en la instancia del organismo para poder confiar en ellas como se comentó anteriormente al configurar el servidor web.

190. El CCN-CERT proporcionará un GUID de instancia, que debe configurarse en la instancia:

```
Perl: /opt/rt4/local/etc/lucia_sync_client_instance_guid_Config.pm
use utf8;

Set( $lucia_sync_client_instance_guid, 'guid_de_instancia' );

1;
```

ANEXO E.3.1. CONFIGURACIÓN DEL CERTIFICADO DE CLIENTE PROPORCIONADO POR EL CCN-CERT

191. Para poder sincronizar incidentes con LUCIA Central, se necesita un certificado de cliente y una clave para autenticarse, proporcionados por el CCN-CERT.

192. Se debe copiar en el directorio `/media/lucia-data/etc/pki/tls/certs` el certificado `client_lucia.crt` y asignarle los permisos correctos:

```
bash
chmod 644 /media/lucia-data/etc/pki/tls/certs/client_lucia.crt
chown rtcronuser /media/lucia-data/etc/pki/tls/certs/client_lucia.crt
```

193. Se debe copiar en el directorio `/media/lucia-data/etc/pki/tls/private` la clave `client_lucia.key` y asignarle los permisos correctos:

```
bash
chmod 600 /media/lucia-data/etc/pki/tls/private/client_lucia.key
chown rtcronuser /media/lucia-data/etc/pki/tls/private/client_lucia.key
```

ANEXO E.3.2. CONFIGURACIÓN DE SINCRONIZACIÓN DE INCIDENTES

194. Definir el usuario y *password* proporcionados para la sincronización de:

```
Perl: /opt/rt4/local/etc/lucia_sync_client_rest_credentials_Config.pm
use utf8;

# Contraseña del usuario de sincronización REST
Set( $lucia_sync_client_rest_user, 'rest' );
# Contraseña del usuario de sincronización REST
Set( $lucia_sync_client_rest_password, 'contraseña_usuario_rest' );

1;
```

195. A su vez, **se debe proporcionar al CCN-CERT las credenciales del usuario rest de la instancia propia** –definidas al inicializar la instancia de LUCIA en los parámetros

`$lucia_sync_client_rest_user` y `$lucia_sync_client_rest_password`– **y la CA propia para que confíe en ella**.

196. Se deberá configurar también la ruta y parámetros de conexión al servidor de sincronización:

```
Perl: /opt/rt4/etc/RT_SiteConfig.d/Lucia_Client_Main_Config.pm
```

```
# ...
Set( $lucia_sync_client_server_url, 'https://lucia-rest.ccn-cert.cni.es/sync/' );
Set( $lucia_sync_client_ssl_verify_hostname, 1 );
Set( $lucia_sync_client_ssl_cert_file, 'ruta_certificado_del_cliente' );
Set( $lucia_sync_client_ssl_key_file, 'ruta_clave_del_cliente' );
Set( $lucia_sync_client_ssl_ca_file, 'ruta_certificado_de_la_CA' );
# ...
```

197. Finalmente, se debe reiniciar el servicio web Apache:

```
bash
```

```
systemctl restart httpd.service
```

ANEXO E.4. CAMBIO DE CONTRASEÑAS

198. Para finalizar con la securización de la instalación de LUCIA, es necesario cambiar las contraseñas proporcionadas por defecto. Para ello se debe acceder a una consola con permisos de administración con el usuario `root`.

199. Primero, cambiar las contraseñas de los usuarios del sistema operativo:

```
bash
```

```
passwd nopriv # Para cambiar la contraseña del usuario nopriv
passwd # Para cambiar la contraseña del usuario root
```

200. Tras esto, se procede a cambiar las contraseñas del gestor de bases de datos MariaDB, para lo cual es necesario la contraseña de `root` por defecto (`LuC14MySQLR00T`):

```
bash
```

```
mysql -u root –p
```

```
MySQL
```

```
SET PASSWORD = PASSWORD('nueva_contraseña_root');
SET PASSWORD for rt_user@localhost = PASSWORD('nueva_contraseña_rt_user');
SET PASSWORD for rt4_sync@localhost = PASSWORD('nueva_contraseña_rt4_sync');
```

201. Una vez cambiadas las contraseñas de MariaDB es necesario sustituir en los ficheros de configuración su valor.

202. Si se cambia la contraseña de `rt_user`, modificar en `/opt/rt4/etc/RT_SiteConfig.pm`:

```
Perl: /opt/rt4/etc/RT_SiteConfig.pm

Set( $DatabasePassword, q{nueva_contraseña_rt_user} );
```

203. Si se cambia la contraseña de rt4_sync, modificar en */opt/rt4/etc/RT_SiteConfig.pm*:

```
Perl: /opt/rt4/etc/RT_SiteConfig.d/Lucia_Client_Main_Config.pm

Set( $lucia_rtbase_db_database, 'rt4_syncclient' );
Set( $lucia_rtbase_db_user, 'rt4_sync' );
Set( $lucia_rtbase_db_password, 'nueva_contraseña_rt4_sync' );
Set( $lucia_core_db_database, 'rt4_syncclient' );
Set( $lucia_core_db_user, 'rt4_sync' );
Set( $lucia_core_db_password, 'nueva_contraseña_rt4_sync' );
Set( $lucia_sync_client_db_database, 'rt4_syncclient' );
Set( $lucia_sync_client_db_user, 'rt4_sync' );
Set( $lucia_sync_client_db_password, 'nueva_contraseña_rt4_sync' );
```

204. Tras estos cambios se debe reiniciar Apache:

```
bash

systemctl restart httpd.service
```

205. Por último, es necesario cambiar la contraseña del usuario `root` administrador de LUCIA desde la propia interfaz web. Para ello, es necesario acceder con este usuario y la contraseña genérica proporcionada y realizar el cambio desde la gestión de perfil de usuario.

ANEXO E.5. AUTENTICACIÓN SMTP

206. Algunos servidores de correo no permiten el relay anónimo de correos, o por razones de seguridad, no se considera oportuno habilitar esta funcionalidad. En este caso, para poder enviar correos de manera segura, se puede habilitar la autenticación SMTP dependiendo del emisor. Para ello, se pueden seguir los pasos descritos a continuación.

207. Editar el fichero `/etc/postfix/sasl_paswd` y establecer las credenciales para cada buzón remitente de correos. Por último, se debe indicar las credenciales de una de ellas para usar como último recurso del `relayhost` por defecto:

```
/etc/postfix/sasl_passwd

cuenta1@dominio.correo usuario1:contraseña1
cuenta2@dominio.correo usuario2:contraseña2
cuenta3@dominio.correo usuario3:contraseña3

[<smtp.server>] usuario:contraseña
```

208. Si no existiese, crear el fichero `/etc/postfix/sender_relay` y en él, asociar cada buzón de correo con el servidor SMTP correspondiente:

```
/etc/postfix/sender_relay
```

```
cuenta1@dominio.correo [<smtp.server>]
cuenta2@dominio.correo [<smtp.server>]
cuenta3@dominio.correo [<smtp.server>]
```

209. Añadir los siguientes parámetros al final del fichero `/etc/postfix/main.cf`:

```
/etc/postfix/main.cf
```

```
# …
smtp_sender_dependent_authentication = yes
sender_dependent_relayhost_maps = hash:/etc/postfix/sender_relay
```

210. Ejecutar los siguientes comandos tras modificar los ficheros para recargar la configuración de `postfix`:

```
bash
```

```
postmap -r /etc/postfix/sasl_passwd /etc/postfix/sender_relay
postfix reload
```