centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 681

IMPLEMENTACIÓN DEL ENS EN POSTFIX SOBRE CENTOS 7

OCTUBRE 2019

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-19-244-9
Fecha de Edición: octubre de 2019

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

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 (CNI), 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 (CCN) 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.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado 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 (STIC) 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.

julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE POSTFIX SOBRE CENTOS 7.

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE POSTFIX SOBRE CENTOS 7.

1. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN POSTFIX 2.10.1-7.EL17

Atendiendo a la necesidad de aplicar medidas de refuerzo de seguridad en aquellos escenarios de gestión de correo electrónico con Postfix y que, además, requieran la aplicación del Esquema Nacional de Seguridad (ENS). En la presente guía, se identifican y establecen las directrices y condiciones necesarias para realizar dicho refuerzo de seguridad.

Estas medidas de seguridad se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos de refuerzo, cuando así se demande. En este último caso, por ejemplo, para la segregación de roles, se detallarán los procedimientos y las condiciones que deberá aplicar un administrador de una organización para hacerlas efectivas.

Nota: Se debe tener en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada, se hará usó de la aplicación de medidas de seguridad descritas en el "ANEXO A.4 CATEGORÍA ALTA / DIFUSIÓN LIMITADA".

La aplicación de medidas de seguridad y recomendaciones generales de refuerzo se pueden resumir en los siguientes puntos:

a) Aplicar un modelo de seguridad en profundidad en donde se incluyan todos los elementos que intervienen en el servicio como serían componentes de red, sistemas operativos, servicios y aplicaciones.

b) Habilitar únicamente los servicios necesarios para el transporte de correo electrónico.

c) Cifrar comunicaciones internas y externas de cualquier naturaleza y protocolo.

d) Implementar protocolos y algoritmos de cifrado robustos, en todos los dominios y espacios de nombres SMTP cuya comunicación incluya contenido potencialmente sensible.

e) Implementar mecanismos de cifrado y control de la información adicionales como S/MIME o PGP, especialmente en entornos de categoría alta.

f) Autenticar siempre usuarios y equipos antes de hacer uso de los servicios de correo electrónico, especialmente en aquellas comunicaciones de tipo "retransmisión de mensajes".

g) Configurar mecanismos de defensa ante correo electrónico no deseado y código dañino.

h) Configurar directivas SPF y DKIM para proteger a la organización ante intentos de suplantación de identidad de usuarios o dominios.

i) Habilitar los registros de auditoría y acceso al servidor.

j) Implementar directivas de refuerzo de la seguridad en los servidores CentOS 7 donde esté instalado Postfix.

k) Implementar directivas de seguridad de Firewall.

l) Aplicar todas las actualizaciones disponibles por el fabricante, tanto para el propio Postfix como para todos sus componentes y el sistema operativo.

m) Aplicar un control estricto de roles de usuarios que tienen acceso a la administración de Postfix, los registros de auditoría, colas de mensajes y servicios en general.

n) Instalar y configurar una solución antivirus desarrollada especialmente para Postfix, que permita detectar código dañino en el transporte.

Nota: En esta guía, se ha seleccionado el sistema operativo Centos 7 por considerarse suficientemente seguro para realizar funciones de sistema de correo electrónico MTA. En cualquier caso, muchas, si no todas, las medidas y recomendaciones presentadas anteriormente son aplicables a otras distribuciones de Linux, en las cuales se pueda instalar Postfix como servidor de correo electrónico.

Las medidas aplicadas están sujetas al RD 3/2010 y se encuentran implementados sobre el sistema operativo CentOS 7 habiendo aplicado, así mismo, la guía CCN-STIC-619_ENS – Implementación del ENS en CentOS 7.

Para el análisis y desarrollo de las plantillas a aplicar, así como la ejecución de tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta CentOS 7, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, la asignación de permisos para la segregación de roles y funciones. Para un mejor entendimiento de las medidas a aplicar, a lo largo de esta guía, se van a explicar cada una de ellas y se van a definir los procedimientos y tareas necesarias para implementar los refuerzos de seguridad atendiendo a los criterios de categorización del ENS.

De esta forma, se irá delimitando cada una de las medidas y se irá estableciendo, según los niveles de clasificación de la información, qué configuraciones deben ser aplicadas para un adecuado cumplimiento de la categoría de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Mediante el cumplimiento de todas las medidas, se garantiza que nadie accederá a recursos sin la debida autorización. Adicionalmente se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la usabilidad y la protección del sistema, de tal forma que la seguridad se irá incrementando en base a la categoría exigida. Por lo tanto, se requiere una menor exigencia de seguridad para la categoría básica mientras que en las categorías media y alta se requiere una mayor exigencia.

1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN

Desde las categorías básicas, deben especificarse mecanismos para garantizar la autenticidad y trazabilidad de las diferentes entidades. Por tanto, se deberá emplear una identificación singular para cada entidad: usuario, proceso o servicio. De esta manera, siempre se podrá conocer quién recibe qué derechos y se podrá saber qué ha hecho.

Las limitaciones de acceso a los servicios se establecerán basándose en los métodos de identificación disponibles según el contenido al que se quiera acceder.

Debe tenerse en consideración que los requisitos para la identificación en un servidor Postfix serán gradualmente incrementados en cuanto a su robustez, según se eleve el nivel de seguridad, en función de la categoría establecida por el ENS.

La implementación de uno u otro mecanismo de identificación que aporta Postfix vendrá también demandada por el tipo de mensajes que transmite el sistema a securizar. Así, un servidor de correo electrónico de acceso público demandará un sistema de autenticación anónima, aun siendo la categoría alta categoría a implementar. No obstante, si esta misma plataforma contara con un espacio de acceso restringido para determinados usuarios, se implementará un mecanismo de autenticación asociado a la categoría requerida en el ENS.

Dentro de las guías de paso a paso se sugerirán los mecanismos de identificación más adecuados a cada una de las categorías de seguridad contempladas por el ENS.

La identificación de cada usuario se traduce en la necesidad de crear cuentas con un identificador único e inequívoco para cada usuario y servicio.

Nunca deberán existir dos cuentas iguales, de forma que éstas no puedan confundirse o bien imputarse acciones a usuarios diferentes al que haya realizado la acción a auditar.

1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS

Postfix, incluye un conjunto de permisos predefinidos para el acceso a diferentes apartados del servicio. Los permisos que se conceden a los administradores y a los usuarios se basan en roles de administración. Un rol o función define el conjunto de tareas que un administrador o un usuario pueden realizar.

En Postfix existen grupos de roles predeterminados las cuales establecen las diferentes funciones a realizar en la administración de Postfix.

1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Este proceso requiere consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada recurso se reducirán al mínimo estrictamente necesario para realizar las acciones requeridas para cumplir sus obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

Postfix se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso. Se deberán establecer, así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda visualizar contenido que no es requerido para las funciones que desempeña.

1.1.1.4. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Postfix utilizará siempre la autenticación basada en usuarios prevaleciendo la configuración de seguridad que se establece mediante las políticas de seguridad y según se establece en el Esquema Nacional de Seguridad.

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de usuario y contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información atendiendo lógicamente a diferentes criterios. Según establece el propio Esquema Nacional de Seguridad, a grandes rasgos, estos criterios serán los siguientes:

a) Para la categoría básica se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, dispositivos físicos (en inglés “Tokens”), sistemas de biometría o certificados digitales entre otros.

b) Para la categoría media se desaconseja el empleo de contraseñas o claves concertadas, siendo recomendable el uso de sistemas físicos (Tokens), biométricos o certificados digitales.

c) Para la categoría alta, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige, por tanto, el uso de dispositivos físicos o biometría. Para autenticarse deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-808 de criptología de empleo en el ENS.

1.1.1.5. OP. ACC. 7. ACCESO REMOTO

La organización deberá mantener las consideraciones de seguridad, en cuanto al acceso remoto, cuando éstas se realicen fuera de las propias instalaciones de la organización y a través de redes de terceros.

Estas consideraciones deberán también garantizar la seguridad, tanto en el propio acceso en sí, como en el canal del acceso remoto.

Postfix, al igual que ya lo hacían sus predecesores, proporciona mecanismos avanzados de seguridad para proteger las conexiones procedentes de fuentes no confiables como es Internet.

Dichos mecanismos implementan diferentes modelos de autenticación por certificados, dependiendo de si los extremos forman parte del mismo dominio o forman parte de dominios diferentes.

La seguridad de nivel de transporte (TLS) es un protocolo estándar que se usa para proporcionar comunicaciones seguras en Internet o en intranets, permitiendo a los clientes autenticar servidores y, opcionalmente, a los servidores autenticar clientes. También proporciona un canal seguro, ya que cifra las comunicaciones. TLS 1.3 es la versión más reciente del protocolo Nivel de sockets seguros (SSL).

1.1.2. EXPLOTACIÓN

Se incluyen, en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define, a través de éstas, una serie de procesos tanto para el control como para la gestión. Estos procesos que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que en un servidor con la integración de un sistema de agente de transporte (MTA)de Postfix, deben configurarse previamente a su entrada en producción las distintas medidas de seguridad teniendo en cuenta las siguientes directrices:

a) Se retirarán las cuentas y contraseñas estándar.

b) Se aplicará la regla de mínima funcionalidad.

En el ENS, se considera indispensable que el sistema no proporcione funcionalidades cuyo uso no esté contemplado y, por tanto, deberá proporcionar únicamente las estrictamente necesarias para desempeñar la función asignada. Por tanto, se eliminarán o desactivarán, mediante el control de la instalación y configuración, todas aquellas funciones que no sean necesarias e incluso aquellas que sean inadecuadas a fin de preservar el principio de mínima funcionalidad establecido en el ENS.

Para el cumplimiento del ENS, se establecen las diferentes plantillas de seguridad, las cuales se dotarán de las funcionalidades necesarias para deshabilitar y configurar todos aquellos servicios que, no siendo necesarios para ningún entorno operativo, pudieran constituir un riesgo de seguridad.

Adicionalmente, se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

1.1.2.2. OP. EXP. 4 MANTENIMIENTO

Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches y nuevas versiones para Postfix publicadas por el fabricante.

Se tendrán en consideración las especificaciones del fabricante en lo relativo a instalación y mantenimiento de Postfix.

Para el cumplimiento del ENS, se instalarán las actualizaciones acumulativas de Postfix publicadas por el fabricante, las cuales solventan vulnerabilidades detectadas.

1.1.2.3. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS

Postfix implementa mecanismos para la auditoría de los sistemas e infraestructuras. De forma predeterminada, los datos son almacenados localmente mediante ficheros de registro (logs).

En las categorías media y alta del marco operacional del ENS, se deberán implementar mecanismos que garanticen la trazabilidad de las acciones de los usuarios.

En Postfix se registrará la actividad de los usuarios para indicar quien realiza la actividad, cuando la realiza y sobre qué información para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

También se contempla el registro de actividad de los usuarios y ,en especial, de los operadores y administradores en cuanto al acceso a la configuración y mantenimiento del servidor de Postfix.

Deben registrarse las actividades realizadas con éxito y los intentos de fracaso.

Por lo tanto, se establece que para una categoría básica de seguridad se activaran los registros de actividad en los servidores, para una categoría media se revisaran informalmente los registros de actividad buscando patrones anormales y para una categoría alta se dispondrá de un sistema automático de recolección de registros y correlación de datos, es decir, una consola de seguridad centralizada.

1.1.2.4. OP. EXP. 9. REGISTRO DE LA GESTION DE INCIDENTES

Únicamente para las categorías media y alta de seguridad, se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de tal forma que, se registrara el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

Se registrarán todas aquellas evidencias que posteriormente puedan sustentar una demanda judicial o hacer frente a ella, o cuando el incidente en cuestión pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

En Postfix, existe la posibilidad de retener, por juicio, un buzón. Este hecho permitirá auditar un buzón de forma transparente para el usuario previniendo, con ello, posibles pérdidas de información ya sean accidentales o forzosas.

1.1.2.5. OP. EXP. 10. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

De nuevo, en las categorías altas, se deberán implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:

a) Determinar el período de retención de los registros.

b) Asegurar fecha y hora del registro de la actividad

c) Permitir el mantenimiento de los registros sin que estos puedan ser alterados o eliminados por personal no autorizado, evitando la modificación accidental de dichos registros.

d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

En Postfix existen grupos de roles predeterminados orientados a la protección de la información de los registros de actividad por lo que únicamente los usuarios establecidos por la organización tendrán acceso a la información de los registros de actividad.

1.2. MEDIDAS DE PROTECCIÓN

1.2.1. PROTECCIÓN DE LAS COMUNICACIONES

Para alcanzar un nivel de seguridad en las comunicaciones adecuado en el entorno será necesario involucrar, en diferentes medidas, tanto a administradores como a desarrolladores e incluso a los propios usuarios de la red.

La formación de seguridad debe centrarse en proporcionar un conocimiento adecuado a administradores, desarrolladores y usuarios respecto a las vulnerabilidades y amenazas de seguridad, los diferentes tipos de ataques existentes y los mecanismos de defensa asociados, preferiblemente mediante ejemplos prácticos.

El Real Decreto 3/2010 de 8 de enero de desarrollo del Esquema Nacional de Seguridad 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.

1.2.1.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberán prevenirse ataques activos, garantizando que los mismos serán detectados, permitiendo activarse los procedimientos previstos en el tratamiento frente a incidentes usando los mecanismos de autenticación establecidos anteriormente expuestos en este documento en el punto “1.1.1.4 OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN”.

En aquellos sistemas en que sea de aplicación la categoría media de seguridad del ENS, además de los mecanismos anteriores aplicables a categoría básica, les será de aplicación la necesidad de implementar redes virtuales privadas cuando su comunicación se realice a través de redes fuera de la organización o del propio dominio de la seguridad. Para ello, se deberán tener en consideración los algoritmos acreditados por el Centro Criptológico Nacional.

Para aquellos entornos con sistemas o información catalogados como categoría alta de seguridad del ENS, es recomendable el empleo de dispositivos de hardware para el establecimiento de la comunicación y la utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberán tener en consideración únicamente los productos que se encuentran certificados y acreditados para tal efecto.

Se establecerá una prevención activa de ataques garantizando, como mínimo, que estos sean detectados y se procederá a activar los procedimientos previstos en el tratamiento de incidentes de los cuales se consideran ataques activos los siguientes supuestos:

a) La alteración de la información en el tránsito de la comunicación.

b) La inyección de información ilegitima en la comunicación con un fin fraudulento.

c) El secuestro de una sesión por una tercera parte.

Se deberán aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma de Postfix: software de los dispositivos de red y firewalls, sistema operativo de los servidores (Web, aplicación, y base de datos).

1.2.1.2. MP. COM. 9. MEDIOS ALTERNATIVOS

En la categoría alta de seguridad del ENS, se establece que se deberá garantizar la existencia y disponibilidad de medios alternativos en caso de que fallen los medios habituales . Por ello, Postfix utiliza, tanto para la alta disponibilidad como para la resistencia de sitio, un concepto conocido como implementación incremental. Se debe disponer, por tanto, de dos o más servidores de transporte de correo de Postfix y, en un siguiente paso, configurarlos de manera incremental junto con las bases de datos de buzones de correo para que haya una alta disponibilidad y resistencia de sitios según sea necesario.

Postfix implementa la alta disponibilidad del transporte de la información, la cual es responsable de mantener copias redundantes de los mensajes antes y después de la entrega correcta de éstos.

1.2.1.3. MP. SI. 5. BORRADO Y DESTRUCCION

Las medidas de borrado y destrucción de información se aplicarán a todo tipo de equipos susceptibles de almacenar información.

El borrado seguro de datos en Postfix viene proporcionado por el sistema operativo CentOS7.4, con la aplicación de borrado seguro “shrek”, que permite un borrado con varias “pasadas” de borrado, incluso el rellenado de bloques de datos con ceros “0” con el fin de imposibilitar la recuperación de información.

Postfix, con la ayuda de CentOS 7, permite el borrado seguro de datos pero se debe tener en cuenta que el usuario que realiza la acción debe tener los permisos adecuados y, una vez desvinculada, se deberá eliminar físicamente la carpeta contenedora de la información. Si se desea eliminar el soporte de dicha información, se deberá actuar siguiendo el procedimiento marcado en el borrado y destrucción de soportes físicos que establece el ENS.

Así mismo, el ENS establece que las organizaciones cuya información esté categorizada como categoría alta debe estar cifrada para evitar, con ello, que sea sustraída en caso de intercepción de la información emitida en un correo electrónico.

Cada organización debe analizar la conveniencia de implantar controles y herramientas para el cifrado y firma del correo electrónico, que empleen una robustez y algoritmos acreditados por el Centro Criptológico Nacional y, preferentemente, productos certificados en el caso de entornos de categoría alta.

Postfix permite implementar mecanismos de cifrado y control de la información adicionales como S/MIME y derechos de información (IRM). Postfix proporciona agentes IRM que permiten aplicar plantillas de seguridad en los mensajes en tránsito de forma automática, antes de salir de la organización.

S/MIME permite cifrar mensajes de correo electrónico y firmarlos digitalmente. Cuando se usa S/MIME con un mensaje de correo electrónico, los destinatarios pueden comprobar que lo que ven en sus bandejas de entrada es el mensaje exacto que envió el remitente, además, proporciona servicios de seguridad criptográfica como cifrado, autenticación, integridad de mensajes y no rechazo de origen (haciendo uso de firmas digitales).

1.2.1.4. MP. INFO. 4. FIRMA ELECTRONICA

Postfix permite firmar digitalmente un mensaje de correo, el cual aplica una marca digital única al mensaje. La firma digital incluye la clave pública del certificado, que procede del Id. digital. Un mensaje firmado digitalmente garantiza al destinatario que el usuario, y no un impostor, ha firmado el contenido del mensaje y que el contenido no se ha modificado durante la transmisión.

Las firmas digitales son el servicio más utilizado de S/MIME. Como su nombre indica, las firmas digitales son la contrapartida digital a la tradicional firma legal en un documento impreso. Al igual que ocurre con una firma legal, las firmas digitales ofrecen las diferentes capacidades de seguridad:

a) Autenticación. Una firma sirve para validar una identidad. Comprueba la respuesta a "quién es usted" al ofrecer una forma de diferenciar esa entidad de todas las demás y demostrar su unicidad. Como no existe autenticación en el correo electrónico SMTP, no hay ninguna forma de saber quién envió realmente un mensaje. La autenticación en una firma digital resuelve este problema al permitir que un destinatario sepa que un mensaje fue enviado por la persona o la organización que dice haber enviado el mensaje.

b) No rechazo. La unicidad de una firma impide que el propietario de la misma no pueda rechazar la legitimidad su firma. Esta capacidad se llama no rechazo. Así, la autenticación proporcionada por una firma aporta el medio de exigir el no rechazo. El concepto de no rechazo resulta más familiar en el contexto de los contratos en papel: un contrato firmado es un documento legalmente vinculante y es imposible no reconocer una firma autenticada. Las firmas digitales ofrecen la misma función y, cada vez en más áreas, se reconocen como legalmente vinculantes, de manera similar a una firma en un papel. Como el correo electrónico SMTP no ofrece ningún medio de autenticación, no puede proporcionar la función de no rechazo.

c) Integridad de los datos. Un servicio de seguridad adicional que ofrecen las firmas digitales es la integridad de los datos. La integridad de los datos es uno de los resultados de las operaciones que hacen posibles las firmas digitales. Con los servicios de integridad de datos, cuando el destinatario de un mensaje de correo electrónico firmado digitalmente valida la firma digital, tiene la seguridad de que el mensaje recibido es el mismo mensaje que se firmó y se envió, y que no se ha manipulado mientras estaba en tránsito. Cualquier alteración del mensaje mientras estaba en tránsito una vez firmado invalida la firma. De esta forma, las firmas digitales son capaces de ofrecer una garantía que no permiten tener las firmas en papel, ya que es posible alterar un documento en papel una vez que ha sido firmado.

1.2.1.5. MP. S. 1. PROTECCIÓN DEL CORREO ELECTRONICO

En Postfix.x86_64 2.10.1-7.el17, se han habilitado protecciones para los mensajes de la organización, permitiendo crear reglas de protección de transporte y reglas de integridad y legitimidad de los mensajes durante el transporte de los correos electrónicos entre servidores.

1.2.1.6. MP. S. 2. PROTECCIÓN DE SERVICIOS

Postfix.x86_64 2.10.1-7.el17 utiliza una serie de mecanismos de protección sobre los servicios de transporte de correo electrónico y acceso al servidor de correo asociado. Todos los sistemas dedicados al transporte de información, vía mensaje electrónico deberán ser protegidos frente a las amenazas que le competen como:

a) Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno.

b) Ataques indirectos, dónde cualquiera de los elementos es empleado como herramienta en el ataque. Por ejemplo, un ataque sobre los servidores de DNS podría permitir redireccionar el tráfico de los clientes hacia un entorno malicioso que suplante la aplicación real.

c) Ataques de denegación de servicio (DoS). Las arquitecturas de red están basadas en tecnologías TCP/IP y, por tanto, son vulnerables a los ataques de DoS comunes en TCP/IP. Es necesario disponer de contramedidas técnicas y procedimientos de actuación frente a este tipo de ataques.

Se deberán aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma de correo electrónico: software de los dispositivos de red y firewalls, sistema operativo de los servidores (aplicación, y base de datos) y software de la plataforma de desarrollo empleada (PHP, ASP, Java, etc).

1.2.1.7. MP. S. 9. MEDIOS ALTERNATIVOS

En la categoría alta de seguridad del ENS, se establece que se deberá garantizar la existencia y disponibilidad de medios alternativos en caso de que fallen los medios habituales .Por ello, Postfix utiliza, tanto para la alta disponibilidad como para la resistencia de sitio, un concepto conocido como implementación incremental. Para ello, se debe disponer de dos o más servidores de buzones de correo y, luego, configurarlos de manera incremental junto con las bases de datos de buzones de correo para que haya una alta disponibilidad y resistencia de sitios según sea necesario.

Postfix.x86_64 2.10.1-7.el17, implementa la alta disponibilidad del transporte de la información la cual es responsable de mantener copias redundantes de los mensajes antes y después de la entrega correcta de estos.

2. RESUMEN Y APLICACIÓN DE MEDIDAS DE POSTFIX 2.10.1-7.EL17 SOBRE CENTOS 7.4

A continuación, se establece un cuadro resumen con las diferentes medidas a aplicar, así como los mecanismos que se implementarán para su aplicación. Dichas implementaciones podrán provenir de la revisión de otras guías de seguridad de la serie CCN-STIC-600, de la serie CCN-STIC-800 o bien la aplicación de medidas de seguridad a nivel local.

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
OP. ACC. 3	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
OP. ACC. 5	Mecanismos de autenticación	Revisión e implementación de guía CCN-STIC-681 y CCN-STIC-619, adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
OP. EXP. 4	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad, el registro de actividad es requerido desde la categoría básica.
OP. EXP. 9	Registro de la gestión de incidentes	Revisión e implementación de guía CCN-STIC-681 y CCN-STIC 619, adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación y de la integridad	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. COM. 9	Medios alternativos	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. SI. 5	Borrado y destrucción de la información	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. INFO. 3	Cifrado de la información	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. INFO. 4	Firma electrónica de la información	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. S. 1	Protección del correo electrónico	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. S. 2	Protección de servicios	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.
MP. S. 9	Medios alternativos	Revisión e implementación de guía CCN-STIC-681, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 2.10.1-7.EL17 SOBRE CENTOS 7 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar Postfix.x86_64 2.10.1-7.el17 sobre un servidor CentOS 7, con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación del presente Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad, según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

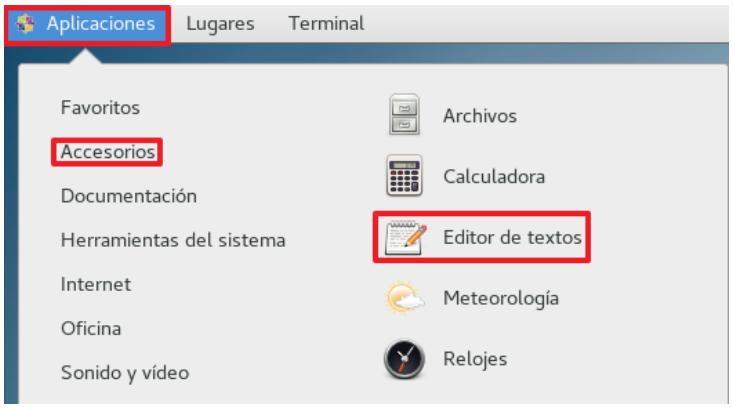
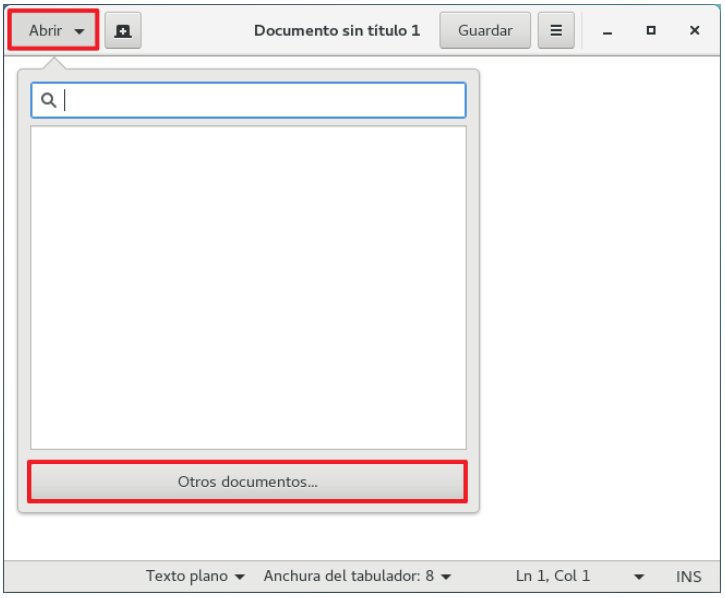
Postfix.x86_64 2.10.1-7.el17 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Postfix, en caso de necesitar información sobre los requisitos previos de instalación de Postfix visite el siguiente enlace.

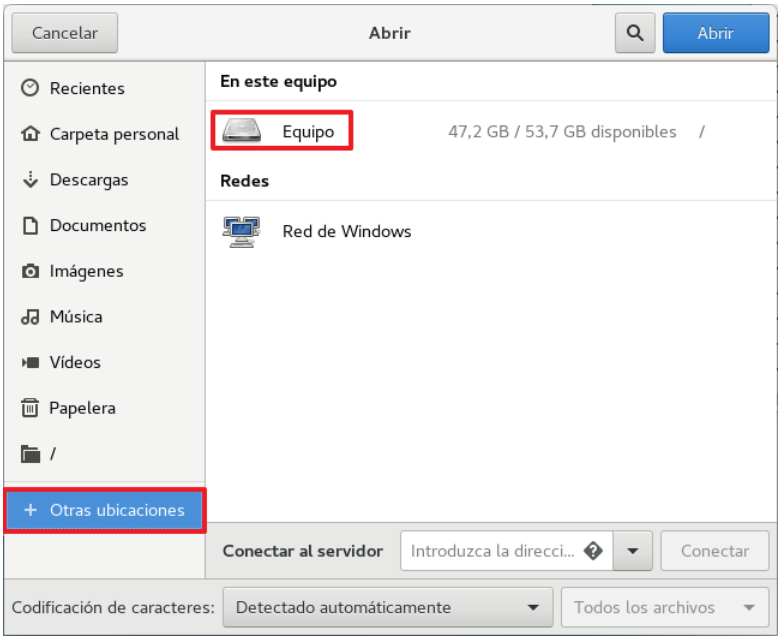
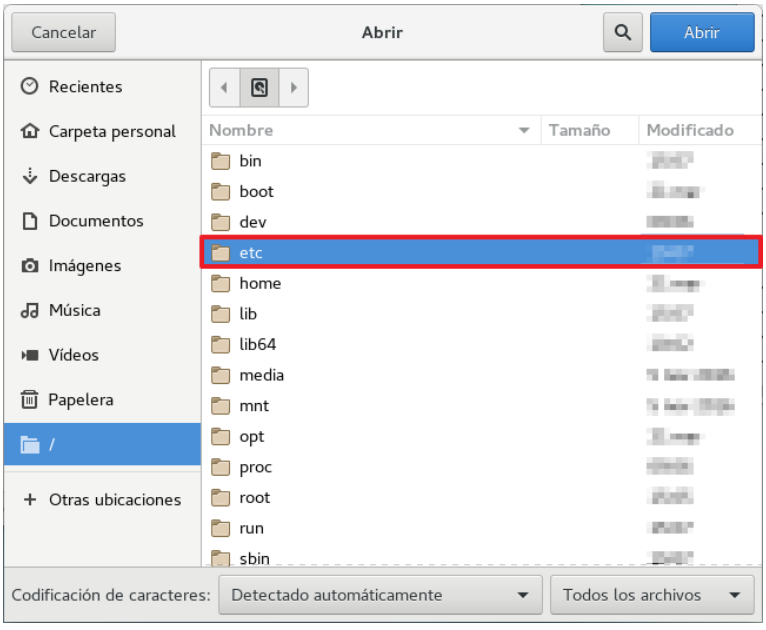
http://www.postfix.org/features.html#fs-requirements

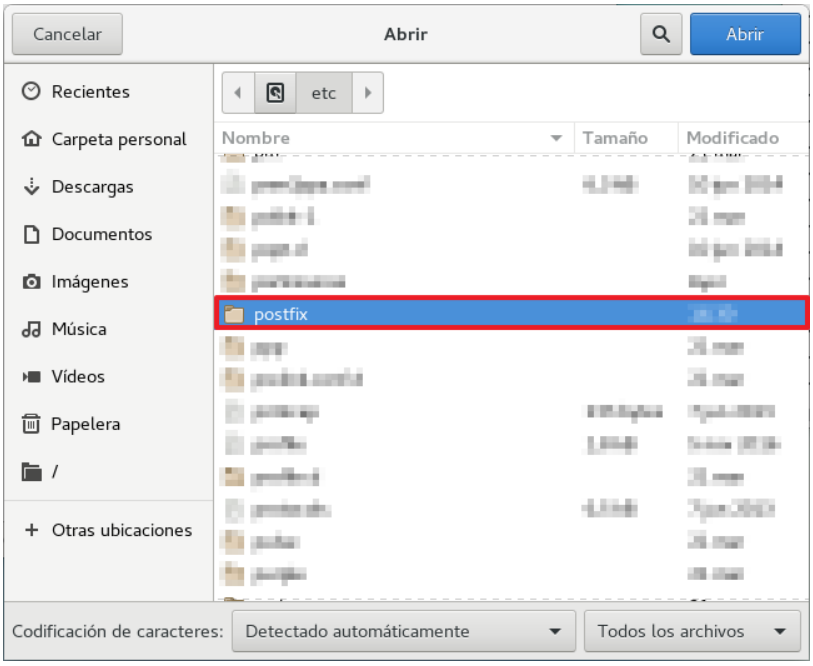
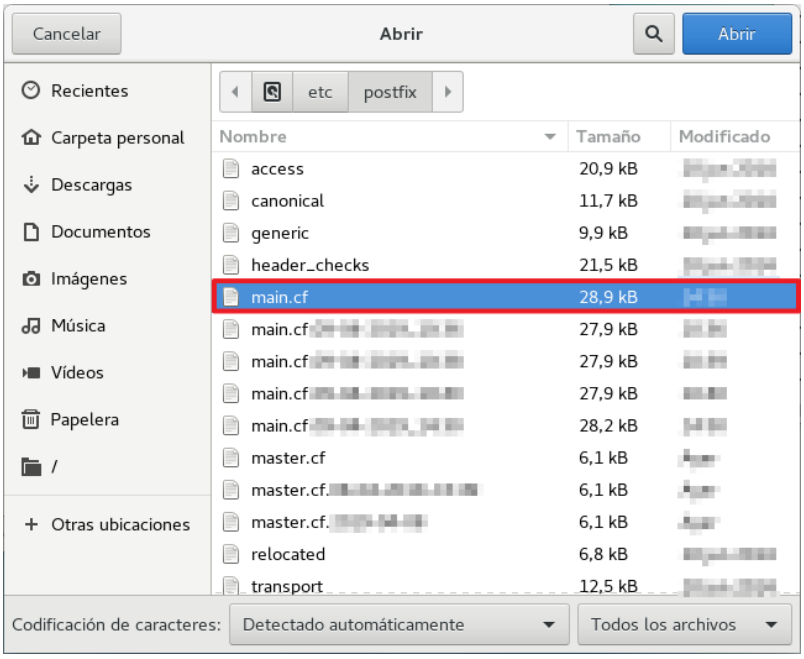
Nota: La instalación de Postfix se debe realizar en un volumen que debe haber sido formateado previamente con el formato XFS, formato que permite la aplicación de ACL's. Así mismo, antes de proceder a instalar las diferentes funcionalidades y complementos de Postfix, se debe haber reiniciado el servidor que se ha preparado hasta este momento, para garantizar que los servicios necesarios para Postfix están aplicados y en ejecución. La preparación del servidor debe haberse realizado de acuerdo con la implantación de la guía codificada como "CCN-STIC-619".
Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando.

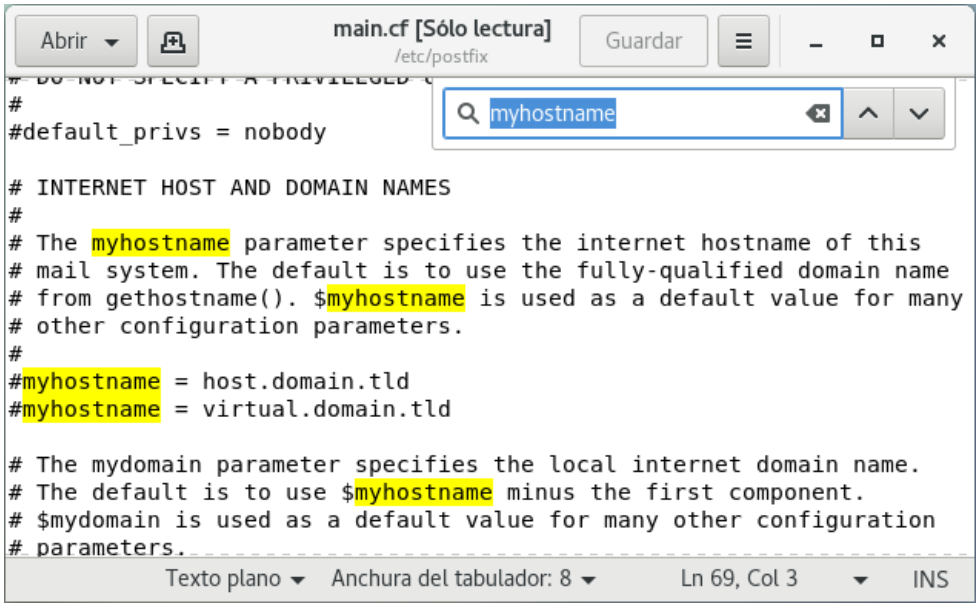
- **$ sudo setenforce 0**

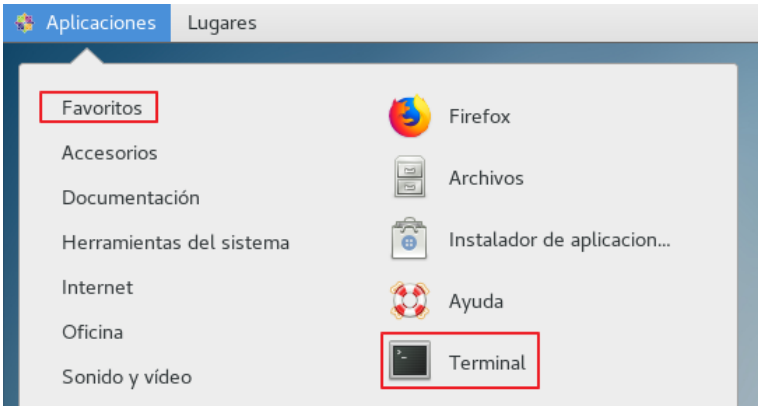
Deberá adaptar los parámetros de configuración de firewalld acorde a su organización. Tenga en cuenta que en esta guía se utilizan, a modo de ejemplo, varios puertos, que es necesario que estén abiertos para el correcto funcionamiento de los productos descritos.

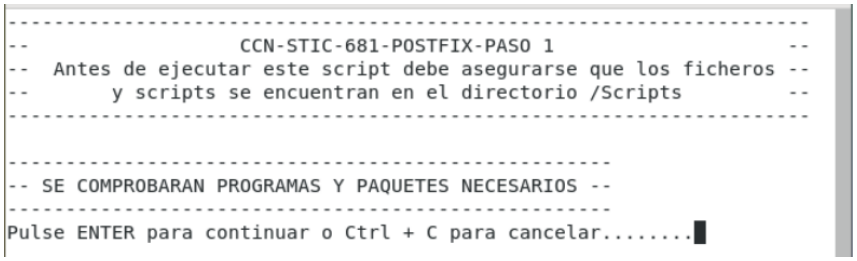
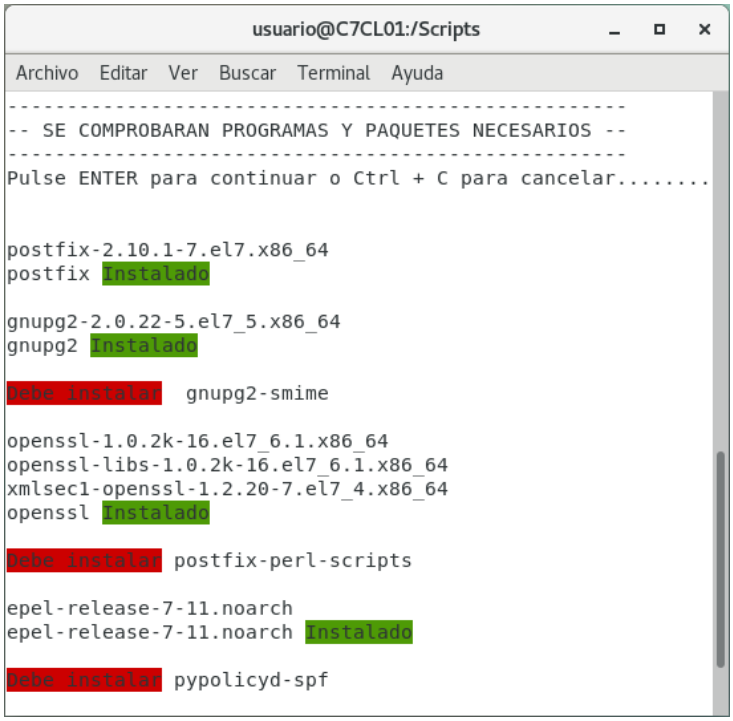
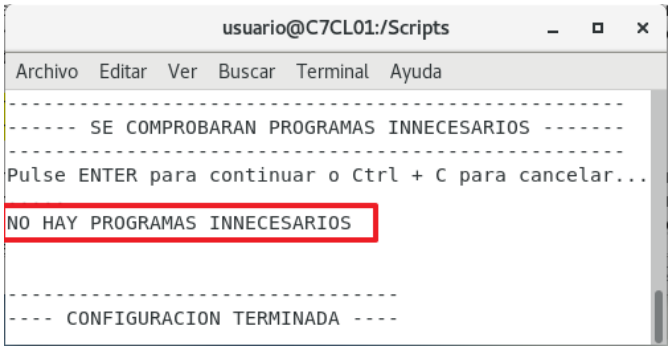
Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".
2.	Diríjase a la barra de tareas superior, pulse sobre "Aplicaciones" y en el apartado "Accesorios" seleccione "Editor de textos". 
3.	Diríjase a la esquina superior izquierda del editor de textos y pulse sobre "Abrir" y en "Otros documentos…". 

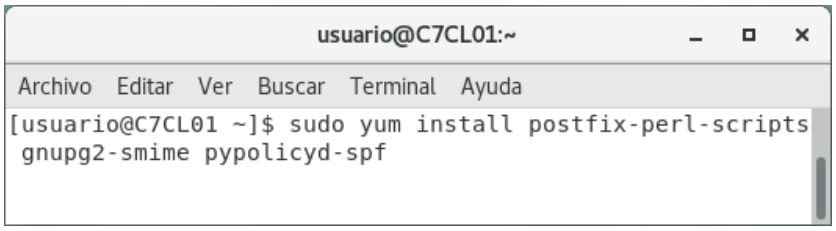
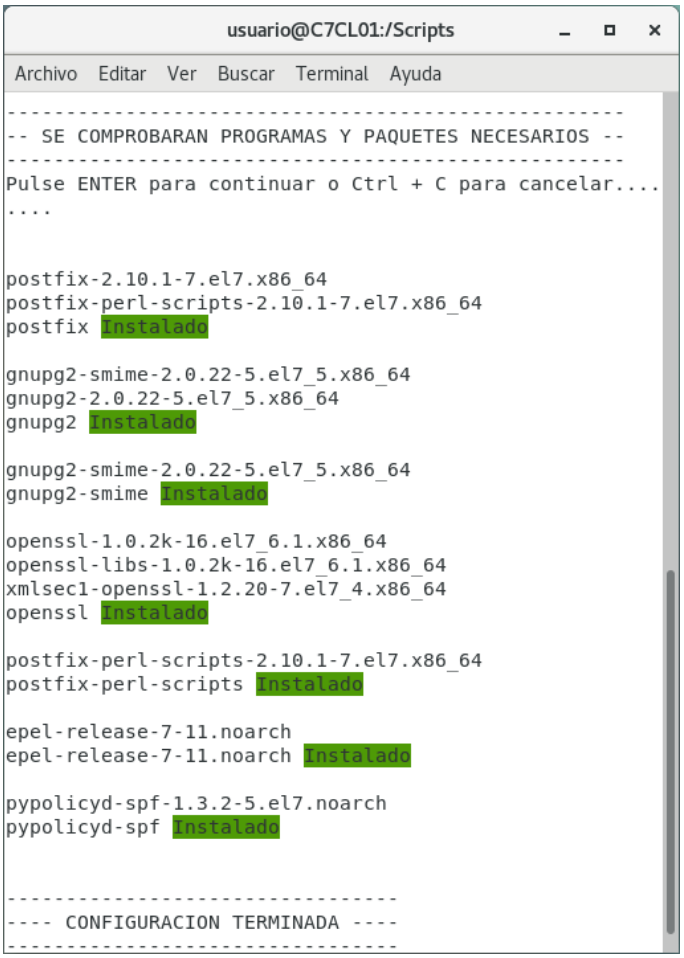
Paso	Descripción
4.	Deberá pulsar sobre “+ Otras Ubicaciones” y posteriormente sobre “Equipo”. 
5.	Ingrese a la carpeta “etc”. 

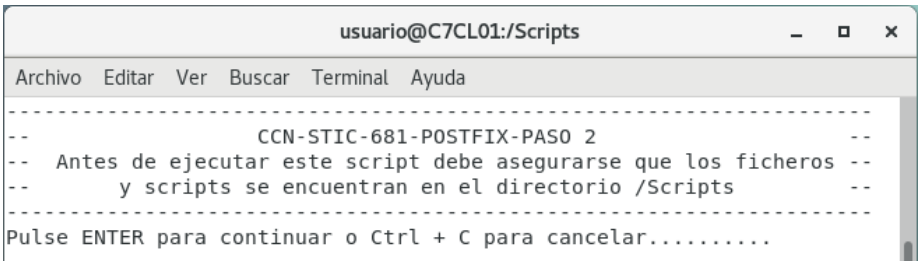
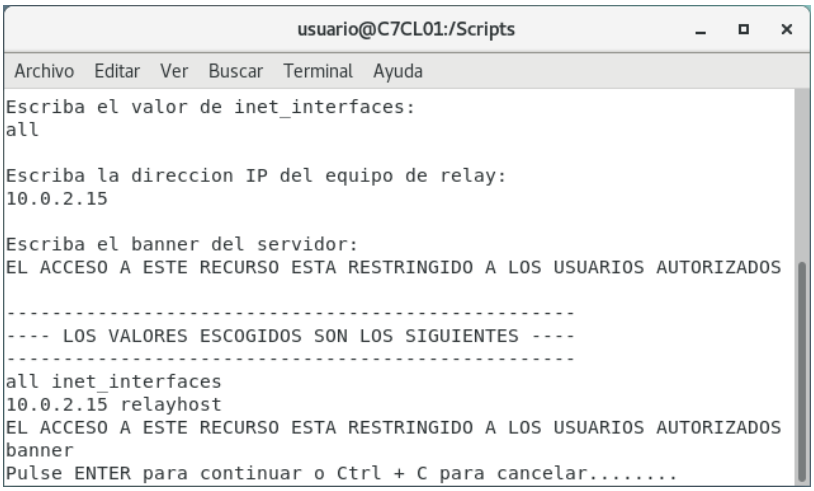
Paso	Descripción
6.	Ingrese en la carpeta “postfix”. 
7.	Ejecute el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón. 

Paso	Descripción
8.	A continuación, se muestran los parámetros a modificar. Estos parámetros responden a una configuración de tipo “parámetro=valor”, utilizando el símbolo “dólar” ($) para exportarlo globalmente en todo el fichero. – **Myhostname** = Nombre del servidor MTA Postfix. – **Mydomain** = Nombre del dominio de la organización. – **Inet_interfaces** = Interfaz de red por donde Postfix debe recibir mensajes. – **Smtpd_banner** = Mensaje deseado. – **Relayhost** = Servidor de correo al que se redireccionan los mensajes electrónicos procesados por Postfix. **Nota:** Estos parámetros se modificarán según las necesidades de cada organización.
9.	Por ser un archivo de configuración muy extenso, se recomienda pulsar “CTRL + f” y buscar el término deseado. 
10.	Una vez definidos los parámetros indicados, pulse “**Guardar**” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 

Paso	Descripción
11.	Diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Favoritos” seleccione “Terminal”. 
12.	Cree la carpeta “**Scripts**”. Para ello, en el terminal, ejecute el comando siguiente. **$ cd /** Para crear la carpeta en la ubicación ejecute el siguiente comando. **$ sudo mkdir Scripts** **Nota:** Puede comprobar que la carpeta ha sido creada ejecutando **ls /**.
13.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía CCN-STIC-681- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE CENTOS 7 LINUX. Introduzca las credenciales si se lo solicita.
14.	Copie el contenido de la carpeta con la categoría de seguridad “CATEGORIA_BASICA” correspondiente al directorio “Scripts/ENS_BASICA” asociado a esta guía en la ruta “**/Scripts**”. Pare ello, ejecute el comando siguiente. **$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_BASICA/* /Scripts/** **Nota:** Se considera que los scripts están disponibles en un disco óptico que es sistema reconoce como ISO Label, en caso contrario adapte la ruta al medio de almacenamiento escogido. Los scripts asumen que su ubicación en el sistema será bajo “/Scripts”. Si se desea modificar la ubicación deberá editar los scripts para reflejar la nueva ubicación.
15.	Expulse el CD/DVD de la unidad y diríjase a la carpeta “Scripts”. Para ello ejecute el comando siguiente. **$ cd /Scripts**
16.	Ejecute el siguiente comando. Introduzca la contraseña del usuario para continuar. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso1_comprobacion_paquetes_necesarios.sh** **Nota:** Los scripts están confeccionados para las versiones correspondientes de los paquetes que se describen en esta guía. Si se dispone de versiones más actualizadas, se deberán modificar los scripts con las nuevas versiones.

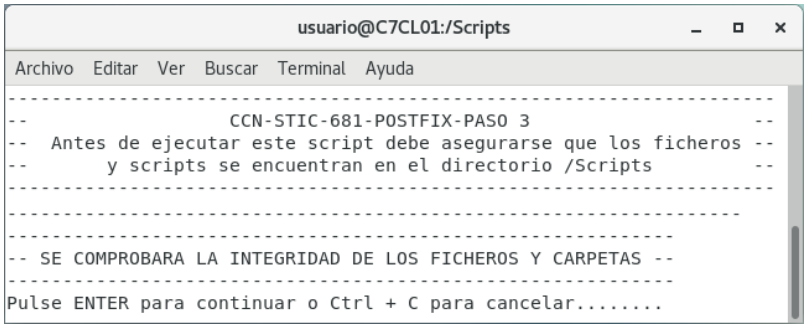
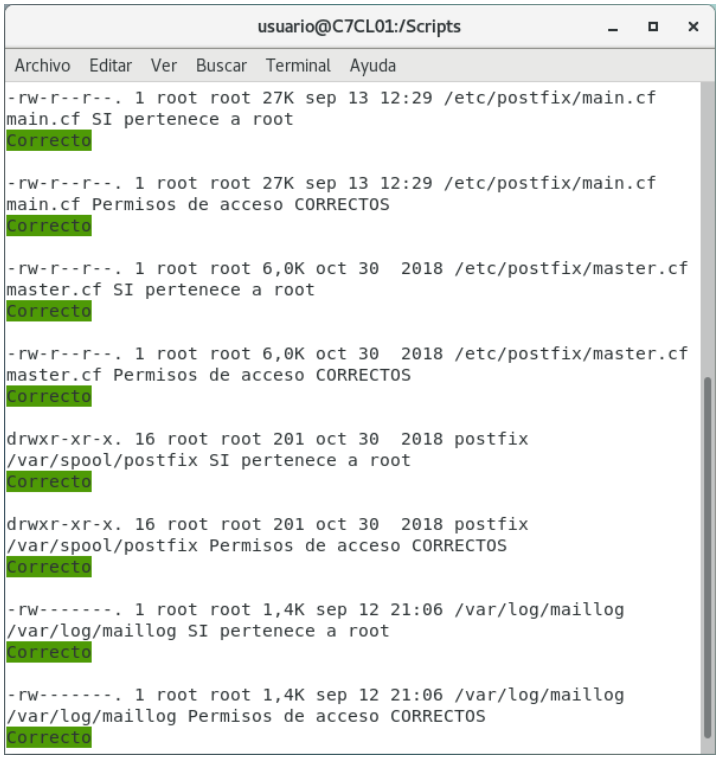
Paso	Descripción
17.	Pulse “ENTER” para continuar. 
18.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar.  **Nota:** Los resultados mostrados en pantalla pueden variar dependiendo de las configuraciones específicas de su organización.
19.	Como último paso comprobará si hay algún programa incompatible con la ejecución de postfix. Deberá mostrar el mensaje “NO HAY PROGRAMAS INNECESARIOS”. El script finalizará con el mensaje “CONFIGURACIÓN TERMINADA”. 

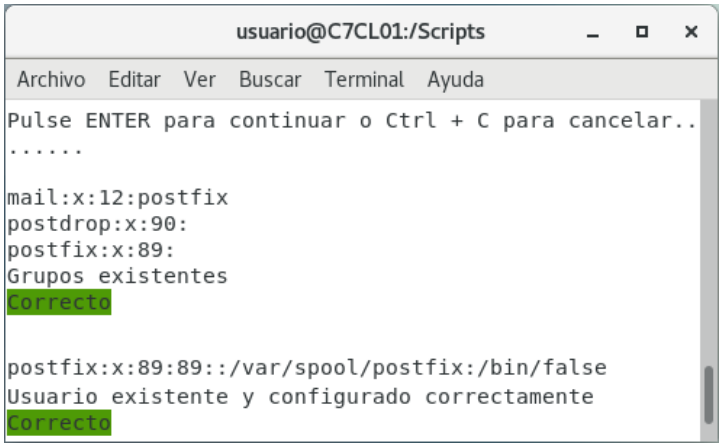
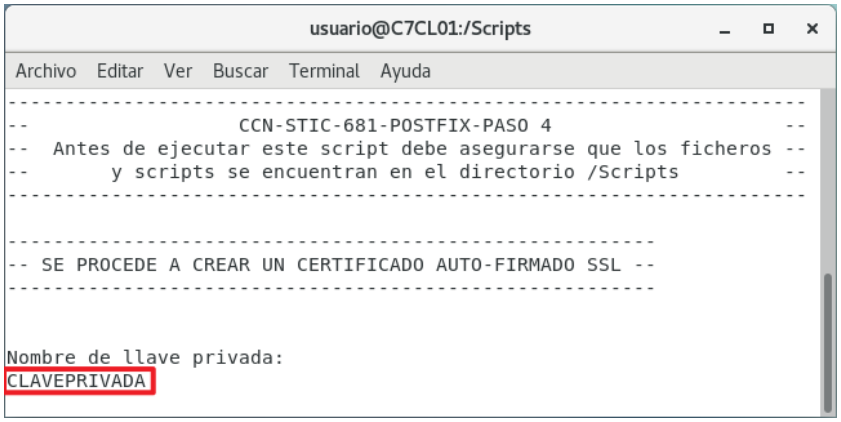
Paso	Descripción
20.	Instale, actualice o elimine los componentes que el script muestre en color rojo por medio de los siguientes comandos. **$ sudo yum install <Paquete1 Paquete2 Paquete 3 …>** **$ sudo yum update <Paquete1 Paquete2 Paquete 3 …>** **$ sudo yum remove <Paquete1 Paquete2 Paquete 3 …>** 
21.	Ejecute el script de nuevo para comprobar que la configuración es correcta. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso1_comprobacion_paquetes_necesarios.sh** 

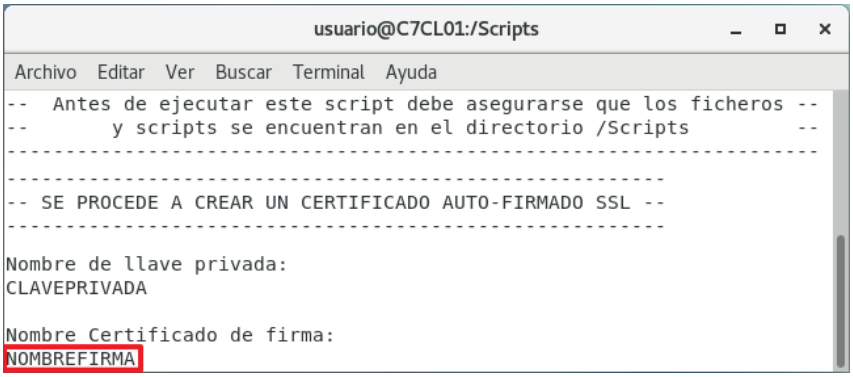
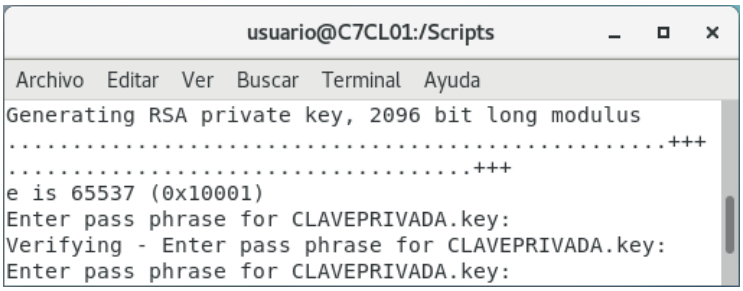
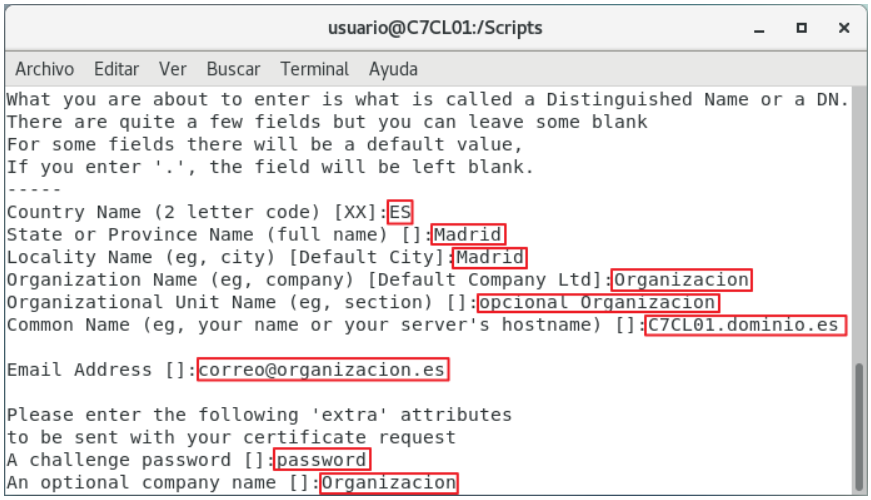
Paso	Descripción
22.	Por motivos de seguridad preservando los datos y configuraciones de su organización, se va a proceder a realizar una copia de seguridad de las configuraciones originales de todos los archivos de configuración susceptibles de ser cambiados por esta guía. Para dicho proceso, escriba los siguientes comandos. **$ sudo mkdir /home/usuario/BACKUP/** **$ sudo cp -f /etc/aliases /home/usuario/BACKUP/aliases_copia** **$ sudo cp -f /etc/postfix/main.cf /home/usuario/BACKUP/main.cf_copia** **$ sudo cp -f /etc/postfix/master.cf /home/usuario/BACKUP/master.cf_copia** **Nota:** Debe elegir una ruta o medio extraíble donde ubicar dichas configuraciones para una posible restauración a un punto anterior. La ubicación "/home/BACKUP/" es la ubicación elegida por esta guía a modo de ejemplo. Adapte la configuración según requisitos específicos de su organización.
23.	Se procede a configurar el fichero "main.cf" para ello, ejecute el siguiente comando. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso2_configuracion_main.cf.sh**
24.	Para continuar con la ejecución del script, pulse "ENTER". 
25.	Para configurar el fichero "main.cf" pulse "Enter". Introduzca los parámetros relativos a las interfaces de red y pulse "Enter" cuando finalice de configurar cada uno de los parámetros.  **Nota:** Tras introducir cada parámetro, deberá pulsar "ENTER" de nuevo para que quede registrado en el fichero. Tenga en cuenta que un parámetro en blanco también puede ser una configuración correcta. Deberá adaptar la configuración a los parámetros de su organización.

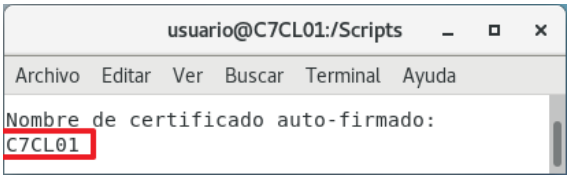
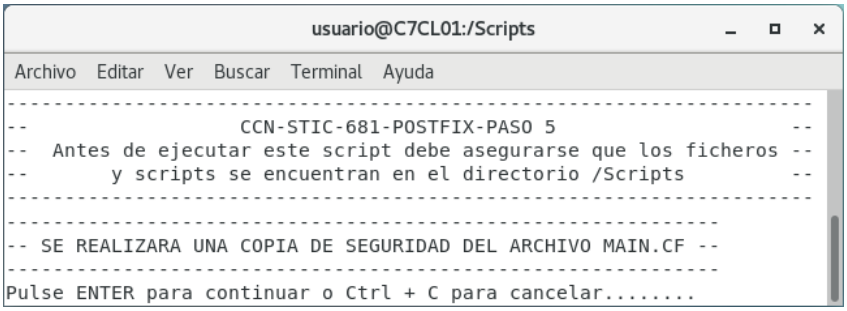
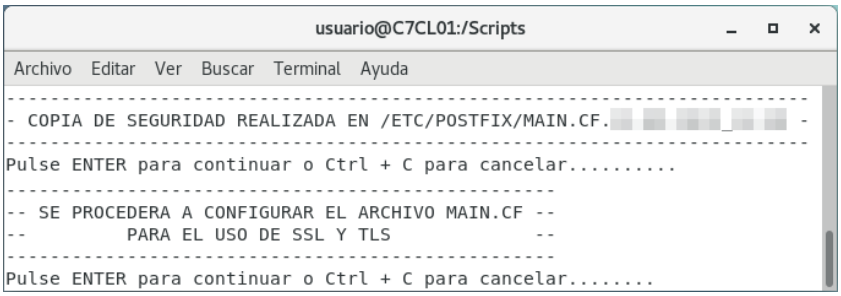
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>26.</td><td>Seguidamente se visualizan los parámetros seleccionados. Si por error se inserta un parámetro no deseado, pulse la combinación de teclas “Ctrl + c” y vuelva a ejecutar el script. Si la inserción ha sido correcta, pulse “ENTER” para continuar.
<pre>

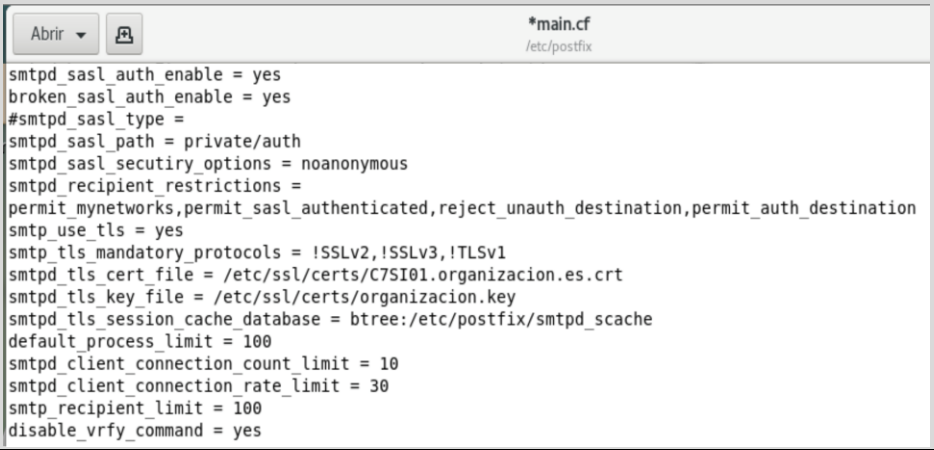
---- LOS VALORES ESCOGIDOS SON LOS SIGUIENTES ----
----
all inet_interfaces
10.0.2.15 relayhost
EL ACCESO A ESTE RECURSO ESTA RESTRINGIDO A LOS USUARIOS AUTORIZADOS
banner
Pulse ENTER para continuar o Ctrl + C para cancelar........
</pre></td></tr>
<tr><td>27.</td><td>El script editará el fichero de configuración, deberá insertar en el archivo los valores correspondientes al tamaño de mensajes, el mínimo de memoria para la correcta función de Postfix, el tamaño de cabecera de los correos electrónicos y el tamaño del cuerpo de los mensajes.
A continuación, se muestran los valores recomendados para cada opción.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>body_checks_size_limit =</td><td>65536</td></tr>
<tr><td>queue_minfree =</td><td>20971520</td></tr>
<tr><td>header_size_limit =</td><td>1024</td></tr>
<tr><td>message_size_limit =</td><td>65536</td></tr>
</table>
Nota: Deberá adaptar los valores a los requeridos por su organización.
<pre>
Abrir main.cf /etc/postfix Guardar
readme_directory: The location of the Postfix README files.
#
readme_directory = /usr/share/doc/postfix-2.10.1/README_FILES
relayhost = 10.0.2.15
body_checks_size_limit =
queue_minfree =
header_size_limit =
message_size_limit =
smtpd_banner = EL ACCESO A ESTE RECURSO ESTA RESTRINGIDO A LOS
USUARIOS AUTORIZADOS
Texto plano Anchura del tabulador: 8 Ln 679, Col 62 INS
</pre>
Además, deberá añadir la siguiente información en el fichero.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>Mydomain =</td><td><Su dominio></td></tr>
<tr><td>Myhostname =</td><td><El nombre del servidor></td></tr>
<tr><td>Myorigin =</td><td><Su dominio></td></tr>
</table></td></tr>
<tr><td>28.</td><td>Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.
<pre>
Abrir main.cf /etc/postfix Guardar
</pre></td></tr>
</table>

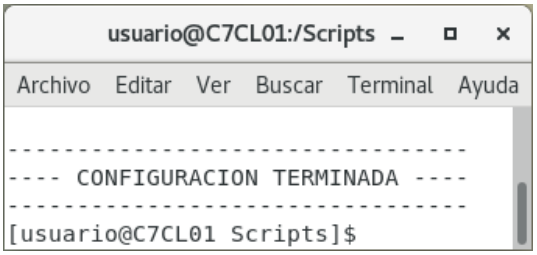
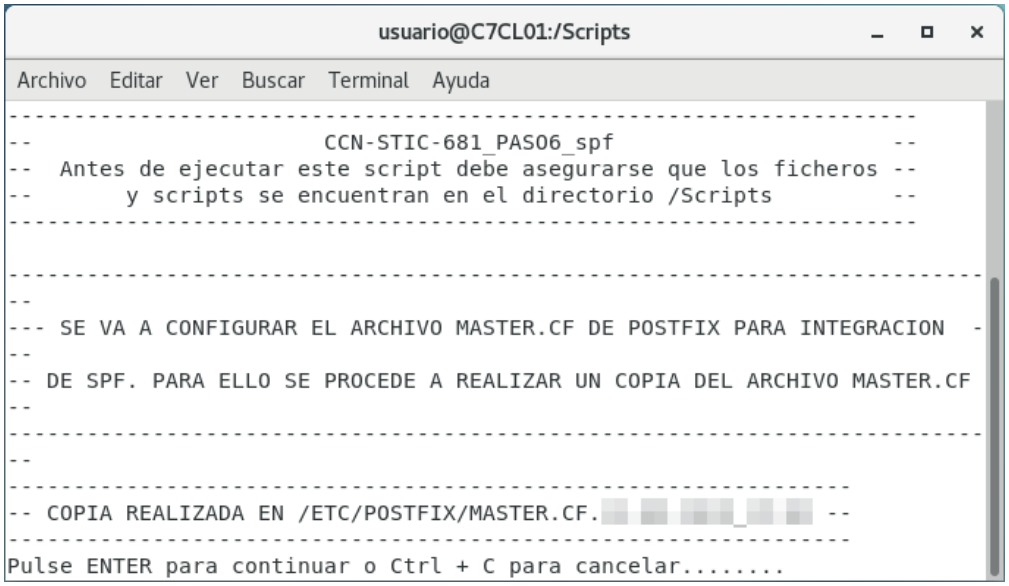
Paso	Descripción
29.	La configuración termina con la salida del proceso de configuración y el mensaje de finalización del mismo.
30.	Se procede a comprobar la configuración de Postfix. Para ello ejecute el siguiente comando. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso3_comprobacion_configuracion.sh**
31.	El script iniciará el proceso de verificación de acceso y pertenencia de los archivos y carpetas necesarias para el correcto funcionamiento seguro de Postfix. Pulse "ENTER" para continuar.  **Nota:** No pulse ningún botón ni cierre la ventana hasta que finalice el script.
32.	En la salida del script, mostrará los archivos y carpetas necesarios para el correcto funcionamiento de Postfix y las recomendaciones pertinentes.  **Nota:** En el caso de que los archivos no pertenezcan a root o no tengan los permisos adecuados deberá cambiarlos con los comandos **chmod** y **chown,** y siempre adecuándose a los parámetros de su organización.

Paso	Descripción
33.	El Script continua con la comprobación de los usuarios y grupos necesarios para el correcto funcionamiento de Postfix de forma segura. Deberá pulsar "ENTER" para continuar.  **Nota:** Si no existieran los grupos postdrop y Postfix o el usuario postfix, indicaría un fallo en la instalación del mismo. Deberá desinstalar el paquete, crear los usuarios y grupos e instalar el paquete de Postfix nuevamente.
34.	La implementación de certificados puede realizarse empleando certificados emitidos por una entidad certificadora perteneciente a la organización o bien por un certificado adquirido a una entidad certificadora oficial de terceros. Para realizar las modificaciones relativas al uso de certificados ejecute el siguiente comando para generar un certificado SSL autofirmado. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso4_certificados_openSSL.sh** **Nota:** En este paso a paso, se va a realizar una configuración con certificados auto firmados, puesto que no todas las organizaciones poseen acceso a una entidad certificadora (CA) oficial.
35.	Se procederá a crear la clave privada RSA. Deberá dar un nombre al fichero ".key" y pulsar "ENTER" para continuar. 

Paso	Descripción
36.	Posteriormente introduzca un nombre para el fichero CSR (solicitud de firma de certificado) que se generará posteriormente. Pulse “Enter” para continuar. 
37.	Se generará la clave privada RSA con una longitud de 2096 bits y seguidamente solicitará la contraseña, una verificación de la misma y una tercera solicitud. Introduzca la contraseña y pulse “Enter” repitiendo el proceso en las tres ocasiones. 
38.	Durante la generación del CSR, se solicitará diversa información sobre su organización relativa a los atributos X.509 del certificado. Uno de los puntos más relevantes es el dato “Common Name” que corresponde al nombre del equipo junto al dominio completo con el que se va a realizar la conexión SSL. Rellene cada campo con los requerimientos específicos de su organización y pulse “Enter” para continuar.  **Nota:** Deberá pulsar “ENTER” para que los datos queden introducidos en la información del certificado.

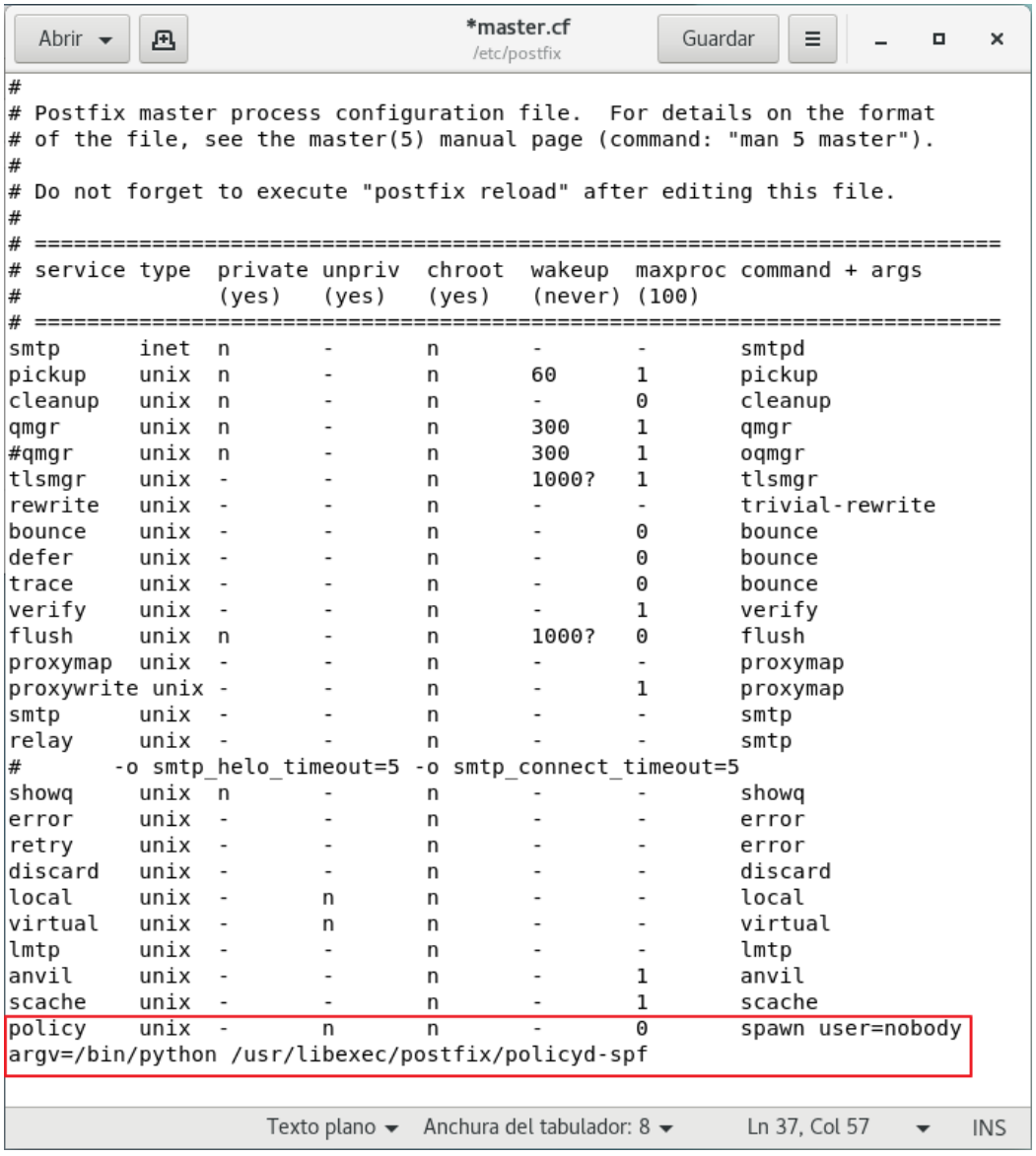
Paso	Descripción
39.	Continúe con el proceso nombrando el certificado. Cuando finalice pulse “ENTER”. 
40.	El proceso finaliza con el mensaje “Signature ok” y mostrando las configuraciones elegidas. Para finalizar el proceso de generación de firma “auto-firmada”, se solicita que ingrese la contraseña de su clave privada. 
41.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso5_Seguridad.sh**
42.	La primera acción que se realizará a través el script es la copia de seguridad del archivo /etc/postfix/main.cf. Para continuar con la ejecución del script pulse “ENTER”. 
43.	Se confirma la realización de la copia de seguridad. Una vez realizada la copia, pulse “ENTER”. Se procederá a configurar el archivo main.cf. Pulse “ENTER” para continuar. Esto abrirá el fichero main.cf en el editor de texto. 

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>44.</td><td>A continuación, se muestra una tabla con los valores recomendados que se deberán aplicar en el archivo de configuración main.cf de Postfix.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>smtpd_sasl_auth_enable =</td><td>yes</td></tr>
<tr><td>broken_sasl_auth_clients =</td><td>yes</td></tr>
<tr><td>#smtpd_sasl_type =</td><td></td></tr>
<tr><td>smtpd_sasl_path =</td><td>private/auth</td></tr>
<tr><td>smtpd_sasl_security_options =</td><td>noanonymous</td></tr>
<tr><td>smtpd_recipient_restrictions =</td><td>permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_destination,
reject_unauth_destination,
permit_auth_destination</td></tr>
<tr><td>smtp_use_tls =</td><td>yes</td></tr>
<tr><td>smtp_tls_mandatory_protocols =</td><td>!SSLv2,!SSLv3, !TLSv1</td></tr>
<tr><td>smtpd_tls_cert_file =</td><td>/etc/ssl/certs/<certificado></td></tr>
<tr><td>smtpd_tls_key_file =</td><td>/etc/ssl/certs/<certificado></td></tr>
<tr><td>smtpd_tls_session_cache_database =</td><td>btree:/etc/postfix/smtpd_scache</td></tr>
<tr><td>default_process_limit =</td><td>100</td></tr>
<tr><td>smtpd_client_connection_count_limit =</td><td>10</td></tr>
<tr><td>smtpd_client_connection_rate_limit =</td><td>30</td></tr>
<tr><td>smtpd_recipient_limit =</td><td>100</td></tr>
<tr><td>disable_vrfy_command =</td><td>yes</td></tr>
</table>
Nota: Si detectara que alguno de estos parámetros ya existe en el documento , se deberá modificar el valor en lugar de generar una línea nueva.
Debe tener en cuenta que en Postfix, un parámetro sin ningún valor se considera como un parámetro válido de configuración. Así mismo deberá tener en consideración los valores establecidos en la tabla anterior y adaptarlos a los valores que más se ajusten a las necesidades de su organización.

</td></tr>
</table>

Paso	Descripción
45.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
46.	El script finalizará mostrando el mensaje “**CONFIGURACION TERMINADA**”. 
47.	Se procede a realizar una la integración de SPF sobre Postfix. Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_ENS_BASICA_Paso6_spf.sh** **Nota:** Para la integración en el servidor de la funcionalidad SPF, deberá de poseer anteriormente ciertas configuraciones específicas en un servidor DNS para que el complemento surta efecto. No es objetivo de esta guía la configuración de un servidor DNS para tal efecto.
48.	Para ello, primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar “ENTER” para continuar. 

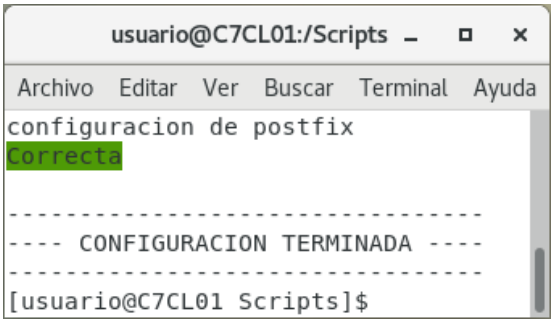
Paso	Descripción
49.	El script editará el fichero master.cf. Inserte la siguiente línea en "master.cf" para configurar SPF.

policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf




```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
pickup    unix  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr     unix  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       n       -       -       smtp
relay     unix  -       -       n       -       -       smtp
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache    unix  -       -       n       -       1       scache
policy    unix  -       n       n       -       0       spawn user=nobody
argv=/bin/python /usr/libexec/postfix/policyd-spf
```

Nota: Tenga en cuenta que el fichero de configuración de la imagen se ha modificado del original para clarificar los parámetros que se deben modificar. Es posible que en su caso pueda tener varias líneas comentadas (#) intermedias.

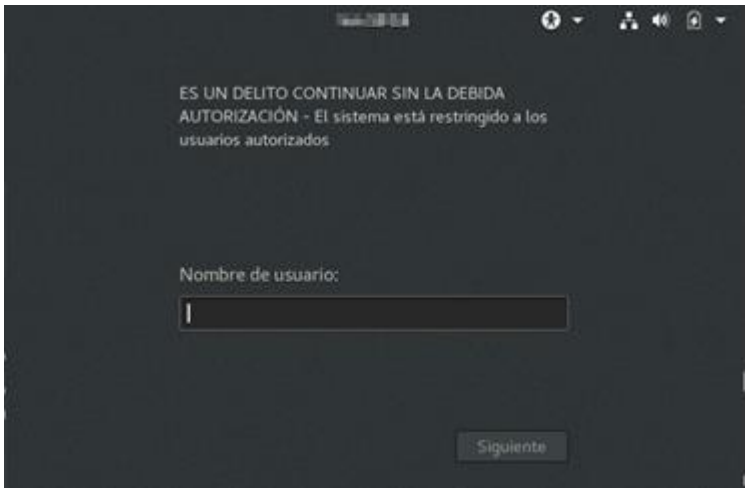
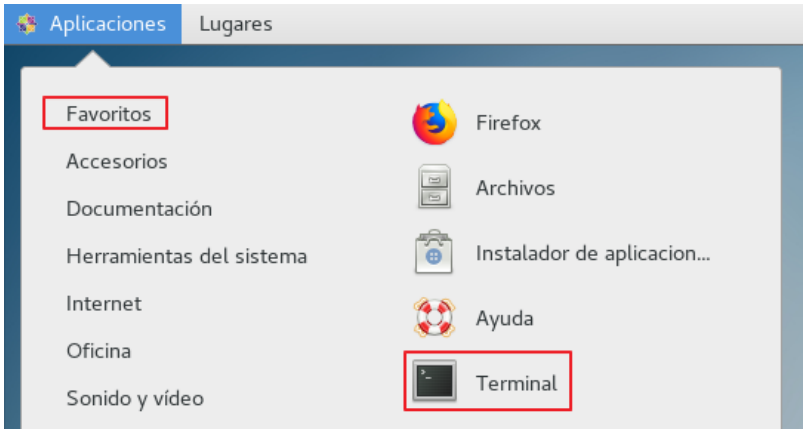
Paso	Descripción
50.	Pulse “Guardar” y cierre el Editor de textos pulsando la “**x**” situada en la zona superior derecha de la ventana. 
51.	El proceso finaliza con el siguiente mensaje, realizándose una comprobación de sintaxis de Postfix. 
52.	El último paso consiste en habilitar los servicios necesarios para el correcto funcionamiento del sistema. Ejecute los siguientes comandos e introduzca la contraseña si se le solicita. **$ sudo systemctl unmask postfix.service** **$ sudo systemctl start postfix.service** **$ sudo systemctl enable postfix.service**
53.	Elimine la carpeta **“/Scripts”** y todo su contenido.
54.	Guarde las aplicaciones que se encuentren abiertas y reinicie el servidor. **$ sudo shutdown -r**

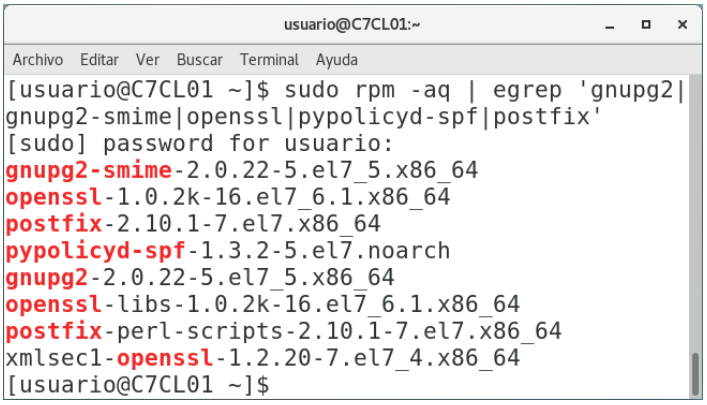
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR CENTOS7 ENS CATEGORÍA BÁSICA

Para realizar las comprobaciones pertinentes en el equipo se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán son las siguientes.

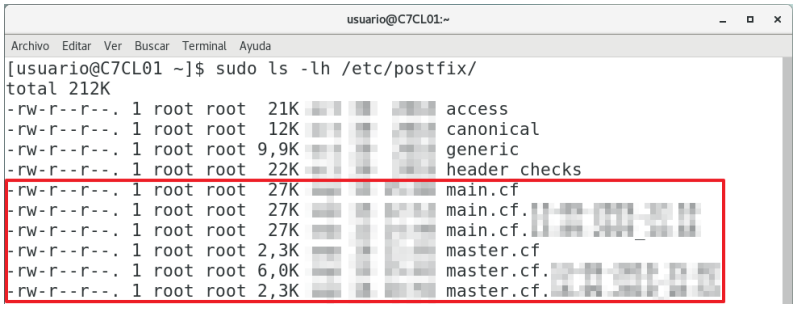
a) Terminal Linux.

b) Editor de textos.

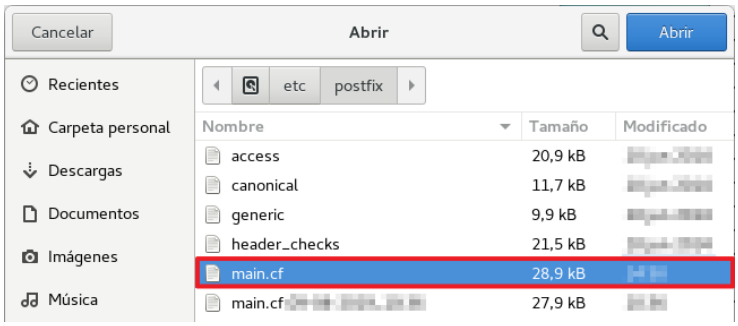
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En uno de los servidores CentOS 7, inicie sesión con una cuenta que tenga privilegios de administración. 
2. Inicie la Terminal de Linux.		Ejecute la “Terminal”. Para ello, diríjase a la barra de tareas superior, pulse en “Aplicaciones” y en el apartado “Favoritos” seleccione “Terminal”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>3. Verifique que se encuentren instalados los paquetes necesarios.</td><td></td><td>En la “terminal” ejecute el siguiente comando.
$ sudo rpm -aq | egrep 'gnupg2|gnupg2-smime|openssl|pypolicyd-spf|postfix'
 

Nota: Deberá comprobar que las versiones de los paquetes que aquí se comprueban, se encuentran en sus últimas versiones.</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Parámetros</th><th>OK/NOK</th></tr>
<tr><td>gnupg2-smime-[versión actualizada]</td><td></td></tr>
<tr><td>openssl-[versión actualizada]</td><td></td></tr>
<tr><td>postfix-[versión actualizada]</td><td></td></tr>
<tr><td>pypolicyd-spf-[versión actualizada]</td><td></td></tr>
<tr><td>gnupg2-[versión actualizada]</td><td></td></tr>
<tr><td>openssl-libs-[versión actualizada]</td><td></td></tr>
<tr><td>postfix-perl-scripts-[versión actualizada]</td><td></td></tr>
<tr><td>xmlsec1-openssl-[versión actualizada]</td><td></td></tr>
</table></td></tr>
<tr><td>4. Copias de seguridad de la organización</td><td></td><td>Compruebe que se realizó exitosamente una copia de seguridad de los siguientes archivos antes de aplicar configuraciones de esta guía. Para ello, ejecute los siguientes comandos y compruebe que existen dichos archivos.
Nota: Ajuste las rutas a las específicas de su organización.</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>OK/NOK</th></tr>
<tr><td>ls /home/usuario/BACKUP/ | egrep "main.cf"</td><td></td></tr>
<tr><td>ls /home/usuario/BACKUP/ | egrep "master.cf"</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
5. Copias de seguridad de la organización		En un terminal ejecute el siguiente comando. **$ ls -lh /etc/postfix** Revise que se han realizado las correspondientes copias de seguridad de los archivos según la ejecución de los scripts correspondientes.  **Nota:** Tenga en consideración que poseerá tantas copias como veces haya ejecutado los scripts.

Configuración	OK/NOK
master.cf.[FECHA]	
main.cf.[FECHA]	

6. Configuración del archivo main.cf		Edite el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón.  Compruebe los siguientes parámetros y cierre el editor de texto al finalizar la comprobación mediante la **“x”** de la esquina superior derecha de la ventana.

Parámetros	Valor	OK/NOK
mydomain	[**DOMINIO**]	
myhostname	[**SERVIDOR POSTFIX**]	
myorigin	[**DOMINIO**]	
inet_protocols	Ipv4	
inet_interfaces	all	
mydestination	$myhostname, localhost.$mydomain, localhost	
relayhost	[**SERVIDOR DE CORREO PRINCIPAL**]	
smtpd_sasl_auth_enable	Yes	

Comprobación	OK/NOK	Cómo hacerlo

Parámetros	Valor	OK/NOK
smtpd_sasl_path	private/auth	
smtpd_sasl_security_options	noanonymous	
smtpd_recipient_restrictions	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, permit_auth_destination	
smtp_use_tls	yes	
smtp_tls_mandatory_protocols	!SSLv2,SSLv3, TLSv1	
smtpd_tls_cert_file	/etc/ssl/private/<certificado.extensión>	
smtpd_tls_key_file	/etc/ssl/private/<clave.extensión>	
smtpd_tls_session_cache_database	btree:/etc/postfix/smtd_scache	
smtpd_banner =	[**MENSAJE DISUASORIO**]	
smtpd_milters =	inet:127.0.0.1:8891	
message_size_limit	65536	
non_smtpd_milters =	$smtpd_milters	
milter_default_action =	accept	
milter_protocol =	2	
#smtpd_sasl_type		
default_process_limit	100	
smtpd_client_connection_count_limit	10	
smtpd_client_connection_rate_limit	30	
queue_minfree	20971520	
header_size_limit	512	
smtpd_recipient_limit	100	
body_checks_size_limit	65536	
disable_vrfy_command	yes	

7. Comprobación de posesión de archivos

Se va a proceder a la comprobación del propietario de los ficheros main.cf y master.cf y de los directorios /var/spool/postfix y /var/log/maillog. Todos ellos deben pertenecer al usuario “root”.
En la “terminal” ejecute los siguientes comandos.

```
$ ls -lh /etc/postfix/main.cf |grep root
$ ls -lh /etc/postfix/master.cf | grep root
$ ls -lh /var/spool/ | grep postfix | grep root
$ ls -lh /var/log/maillog |grep root
```

Ruta	Propietario	OK/NOK
/etc/postfix/main.cf	root	
/etc/postfix/master.cf	root	
/var/spool/	root	
/var/log/maillog	root	

Comprobación	OK/NOK	Cómo hacerlo
8. Comprobación de permisos de archivos		Se comprobará los permisos de archivos y carpetas del sistema. Para ello ejecute los siguientes comandos. **$ ls -lh /etc/postfix/main.cf |grep '\-rw-r--r\--'** **$ ls -lh /etc/postfix/master.cf |grep '\-rw-r--r\--'** **$ ls -lh /var/spool/ | grep postfix | grep rwxr-xr-x.** **$ ls -lh /var/log/maillog |grep '\-rw\-------'**

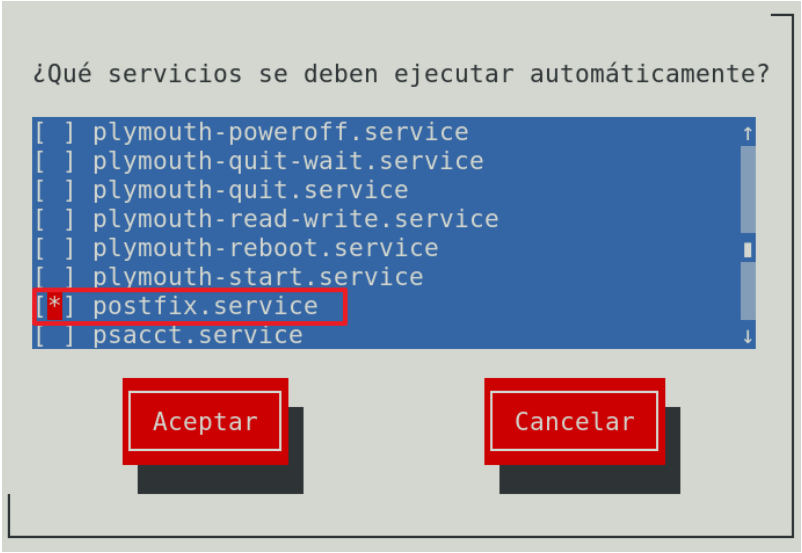
Fichero	Valor	OK/NOK
/etc/postfix/main.cf	-rw-r--r--	
/etc/postfix/master.cf	-rw-r--r--	
/var/spool/postfix	drwxr-xr-x	
/var/log/maillog	drw-------	

9. Comprobación de Usuarios y Grupos		Ejecute los siguientes comandos. **$ cat /etc/passwd |egrep "postfix|/bin/false"** **$ cat /etc/group |egrep "postfix|postdrop"**

Configuración	Valor	OK/NOK
Usuario: postfix	Existe	
Shell: postfix	/bin/false	
Grupo: postfix	Existe	
Grupo: postdrop	Existe	

10. Comprobación de los certificados OpenSSL.		En la "terminal" ejecute el siguiente comando para comprobar la creación de los certificados. **$ ls -lh /etc/ssl/certs** **Nota:** Los valores deben de ser coincidentes con los nombres y configuraciones específicos de su organización.

Configuración	Valor	OK/NOK
"NOMBREFIRMA"."extensión"	Existencia	
"CLAVEPRIVADA".key	Existencia	
Permisos "CLAVEPRIVADA".key	-r---------	
Permisos "NOMBREFIRMA"."extensión"	-rw-r--r--	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>11.Servicios necesarios por medio de herramienta ntsysv</td><td></td><td>Abra la Terminal y ejecute el siguiente comando.
$ sudo ntsysv
 

Compruebe la ejecución del siguiente servicio. Una vez realizada la comprobación utilice el tabulador para colocar el cursor y pulse “Aceptar” para cerrar “ntsysv”.
Nota: Los servicios activos están indicados con un asterisco (*).
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>postfix.service</td><td>Activo</td><td></td></tr>
</table></td></tr>
<tr><td>12.Configuración del archivo master.cf</td><td></td><td>Compruebe que se han modificado los siguientes parámetros del archivo master.cf.
Para ello, diríjase a la ruta /etc/postfix/ y edite el fichero “master.cf”.
 

<table>
<tr><th>Parámetros</th><th>OK/NOK</th></tr>
<tr><td>policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf</td><td></td></tr>
</table></td></tr>
</table>

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 2.10.1-7.EL17 SOBRE CENTOS 7 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar Postfix 2.10.1-7.el17 sobre CentOS 7, con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad, según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

Debe tener en consideración, que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

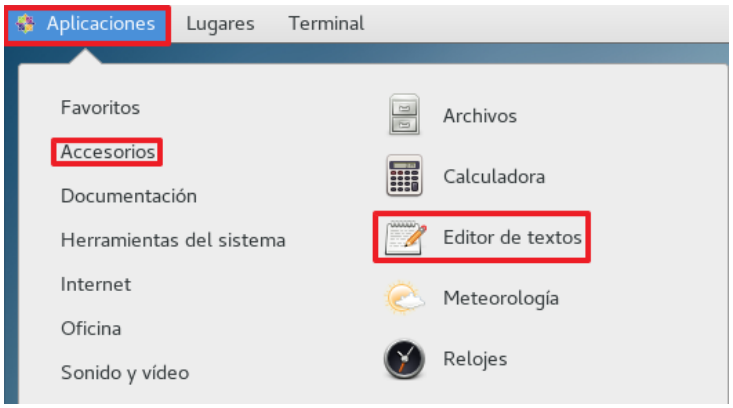
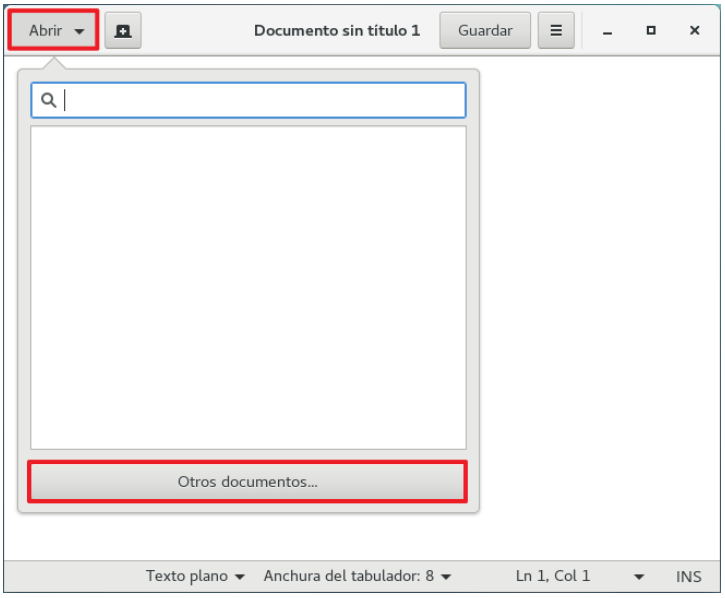
Postfix 2.10.1-7.el17 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Postfix, en caso de necesitar información sobre los requisitos previos de instalación de Postfix visite el siguiente enlace.

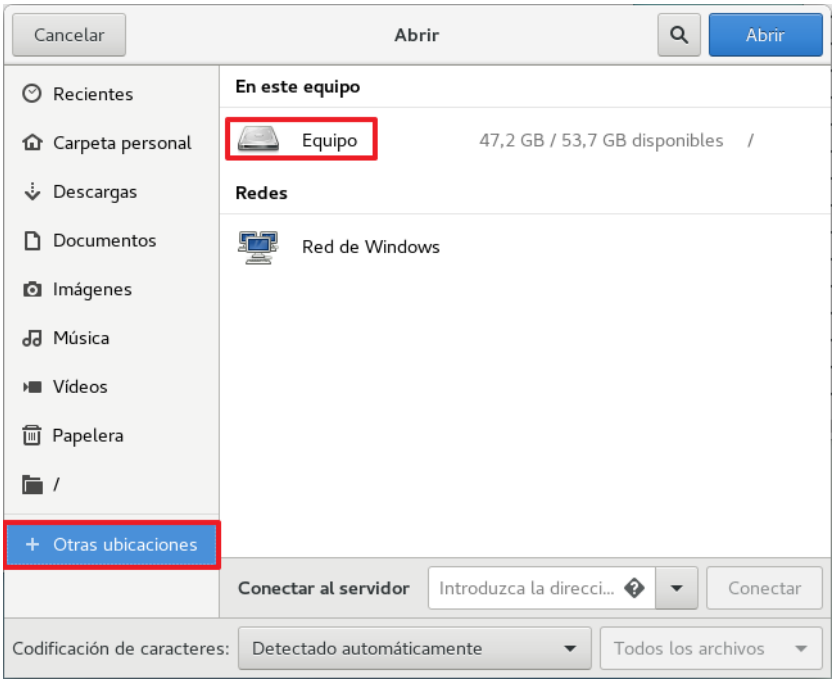
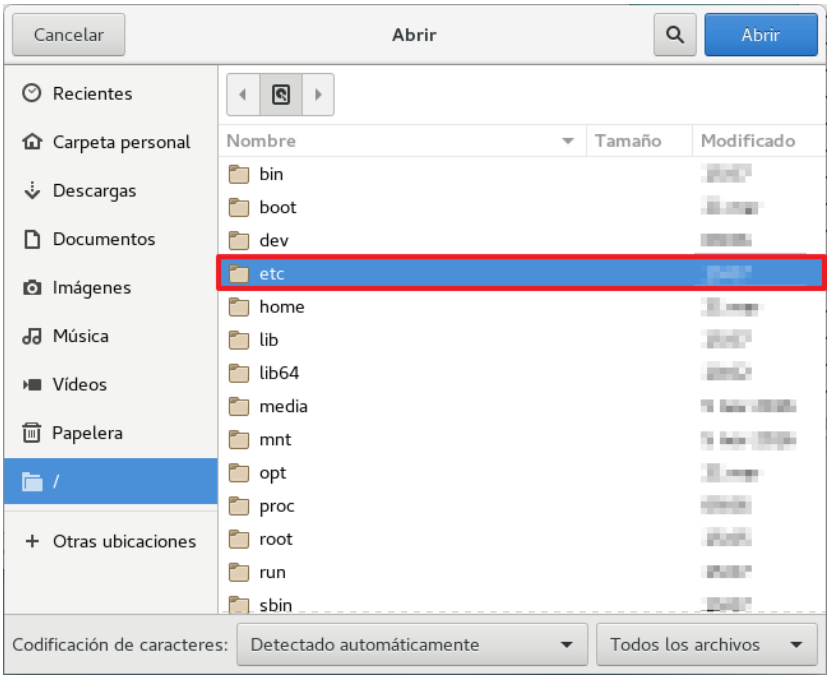
http://www.postfix.org/features.html#fs-requirements

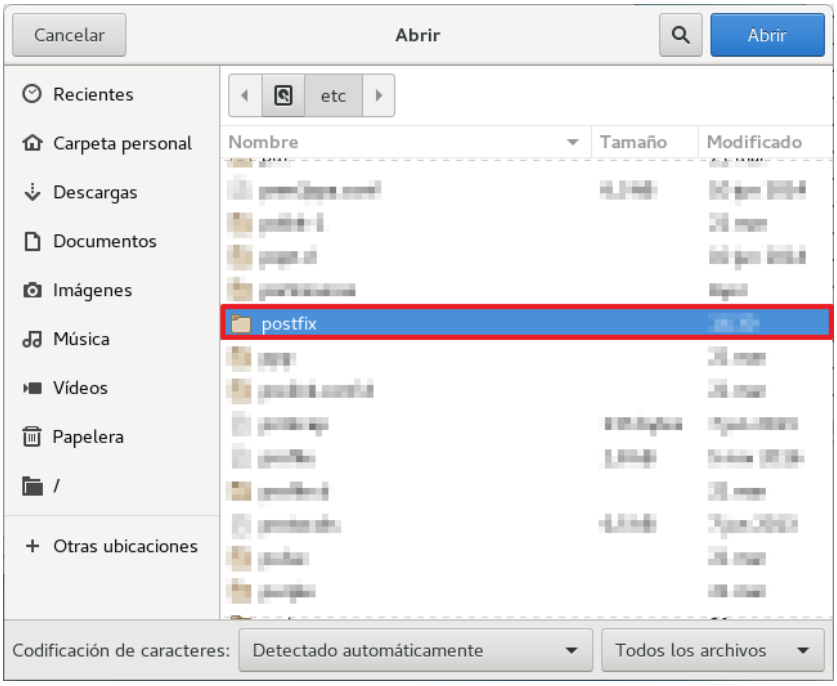
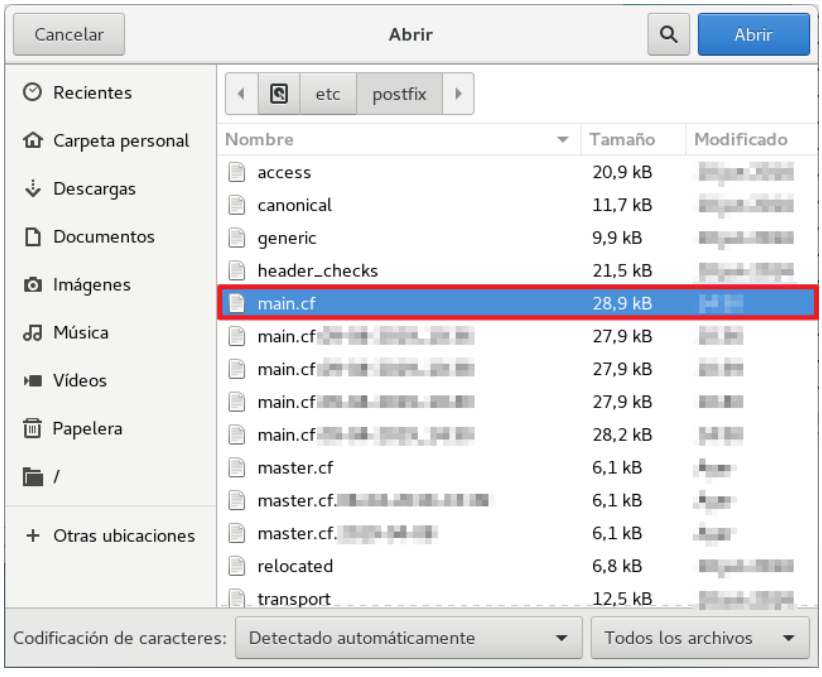
Nota: La instalación de Postfix se debe realizar en un volumen que debe haber sido formateado previamente con el formato XFS, formato que permite la aplicación de ACL's. Así mismo, antes de proceder a instalar las diferentes funcionalidades y complementos de Postfix, se debe haber reiniciado el servidor que se ha preparado hasta este momento, para garantizar que los servicios necesarios para Postfix están aplicados y en ejecución. La preparación del servidor debe haberse realizado de acuerdo con la implantación de la guía codificada como "CCN-STIC-619".
Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando.

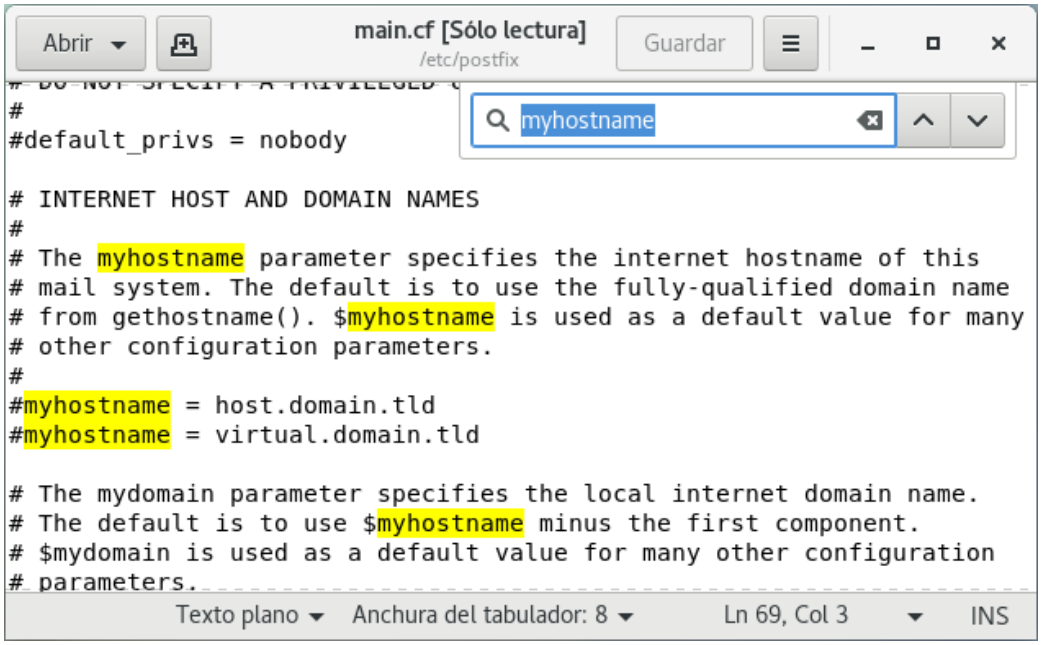
- **$ sudo setenforce 0**

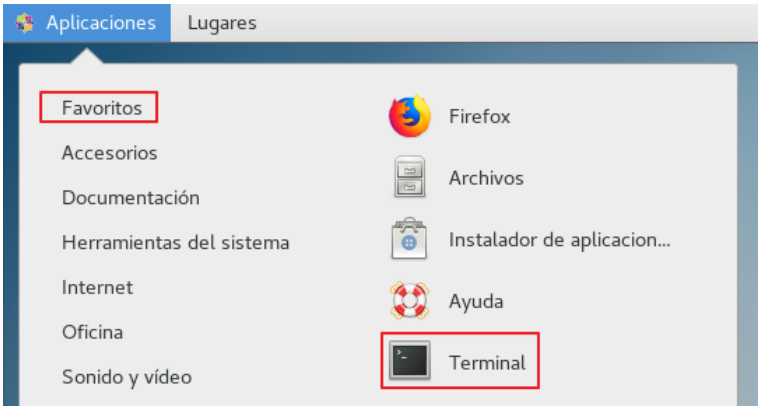
Deberá adaptar los parámetros de configuración de firewalld acorde a su organización. Tenga en cuenta que en esta guía se utilizan, a modo de ejemplo, varios puertos, que es necesario que estén abiertos para el correcto funcionamiento de los productos descritos.

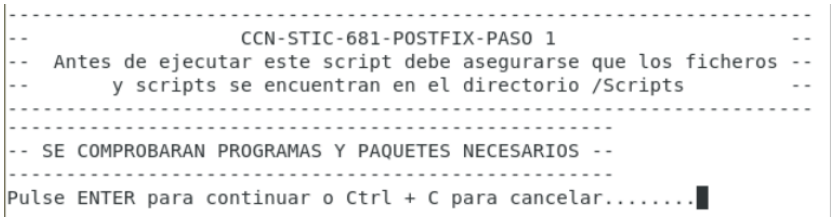
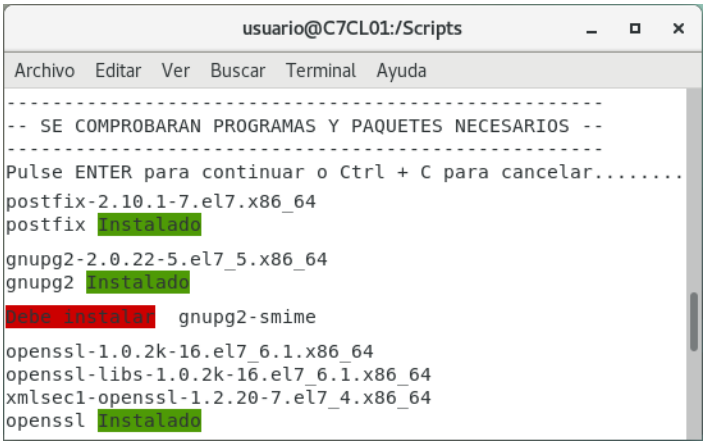
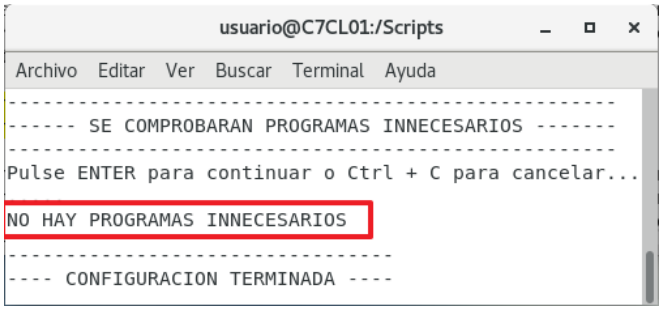
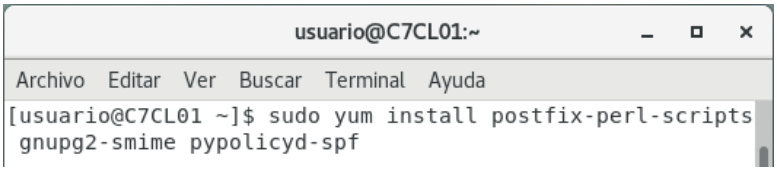
Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que pertenezca al grupo de administradores o "Sudoers".
2.	Diríjase a la barra de tareas superior, pulse sobre "Aplicaciones" y en el apartado "Accesorios" seleccione "Editor de textos". 
3.	Diríjase a la esquina superior izquierda del editor de textos y pulse sobre "Abrir" y en "Otros documentos…". 

Paso	Descripción
4.	Deberá pulsar sobre “+ Otras Ubicaciones” y posteriormente sobre “Equipo”. 
5.	Ingrese a la carpeta “etc”. 

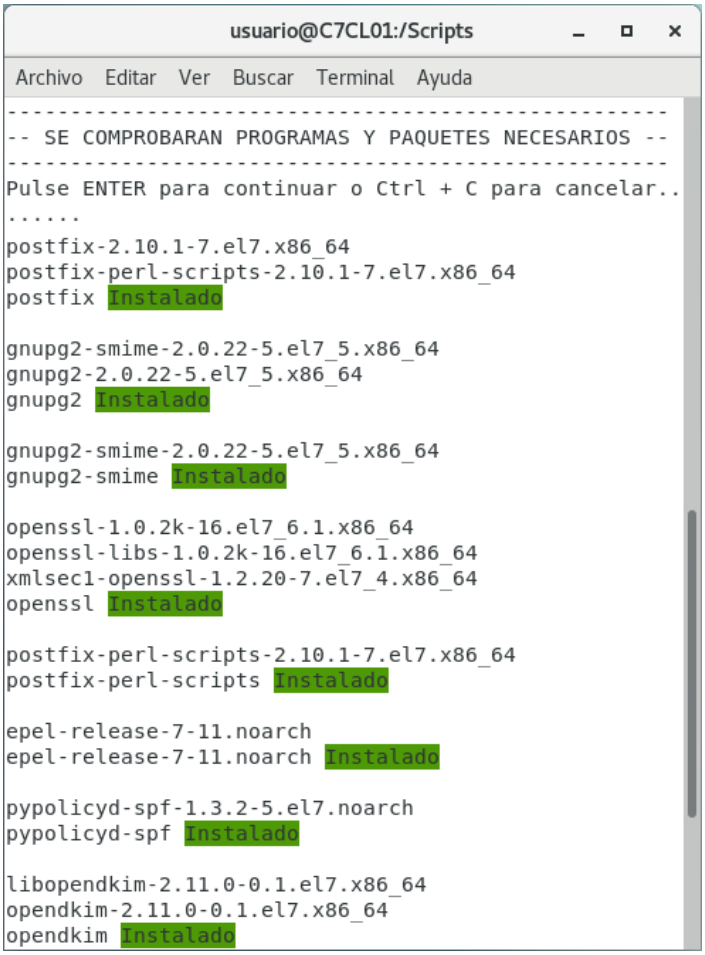
Paso	Descripción
6.	Ingrese en la carpeta “postfix”. 
7.	Ejecute el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón. 

Paso	Descripción
8.	A continuación, se muestran los parámetros a modificar. Estos parámetros responden a una configuración de tipo “parámetro=valor”, utilizando el símbolo “dólar” ($) para exportarlo globalmente en todo el fichero. – **Myhostname** = Nombre del servidor MTA Postfix. – **Mydomain** = Nombre del dominio de la organización. – **Inet_interfaces** = Interfaz de red por donde Postfix debe recibir mensajes. – **Smtpd_banner** = Mensaje deseado. – **Relayhost** = Servidor de correo al que se redireccionan los mensajes electrónicos procesados por Postfix. **Nota:** Estos parámetros se modificarán según las necesidades de cada organización.
9.	Por ser un archivo de configuración muy extenso, se recomienda pulsar “CTRL + f” y buscar el término deseado. 
10.	Una vez definidos los parámetros indicados, pulse “**Guardar**” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 

Paso	Descripción
11.	Diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Favoritos” seleccione “Terminal”. 
12.	Cree la carpeta “**Scripts**”. Para ello, en el terminal, ejecute el comando siguiente. **$ cd /** Para crear la carpeta en la ubicación ejecute el siguiente comando. **$ sudo mkdir Scripts** **Nota:** Puede comprobar que la carpeta ha sido creada ejecutando **ls /**.
13.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía “CCN-STIC-681- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE CENTOS 7 LINUX”. Introduzca las credenciales si se lo solicita.
14.	Copie el contenido de la carpeta con la categoría de seguridad “CATEGORIA_MEDIA” correspondiente al directorio “Scripts/ENS_MEDIA” asociado a esta guía en la ruta “**/Scripts**”. Pare ello, ejecute el comando siguiente. **$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_MEDIA/* /Scripts/** **Nota:** Se considera que los scripts están disponibles en un disco óptico que es sistema reconoce como ISO Label, en caso contrario adapte la ruta al medio de almacenamiento escogido. Los scripts asumen que su ubicación en el sistema será bajo “/Scripts”. Si se desea modificar la ubicación deberá editar los scripts para reflejar la nueva ubicación.
15.	Expulse el CD/DVD de la unidad y diríjase a la carpeta ¨Scripts¨. Para ello ejecute el comando siguiente. **$ cd /Scripts**
16.	Ejecute el siguiente comando. Introduzca la contraseña del usuario para continuar. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso1_comprobacion_paquetes_necesarios.sh** **Nota:** Los scripts están confeccionados para las versiones correspondientes de los paquetes que se describen en esta guía. Si se dispone de versiones más actualizadas, se deberán modificar los scripts con las nuevas versiones.

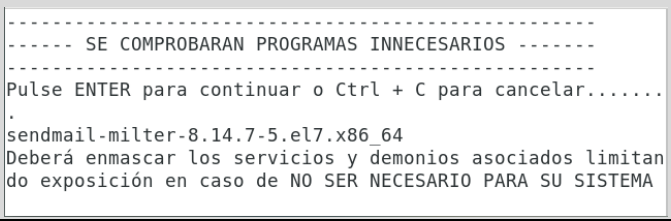
Paso	Descripción
17.	Pulse “ENTER” para continuar. 
18.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar.  **Nota:** Los resultados mostrados en pantalla pueden variar dependiendo de las configuraciones específicas de su organización.
19.	Como último paso comprobará si hay algún programa incompatible con la ejecución de postfix. Deberá mostrar el mensaje “NO HAY PROGRAMAS INNECESARIOS”. El script finalizará con el mensaje “CONFIGURACIÓN TERMINADA”. 
20.	Instale, actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. **$ sudo yum install <Paquete1 Paquete2 Paquete 3 …>** **$ sudo yum update <Paquete1 Paquete2 Paquete 3 …>** 

Paso	Descripción
21.	Ejecute el script de nuevo para comprobar que la configuración es correcta. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso1_comprobacion_paquetes_necesarios.sh**



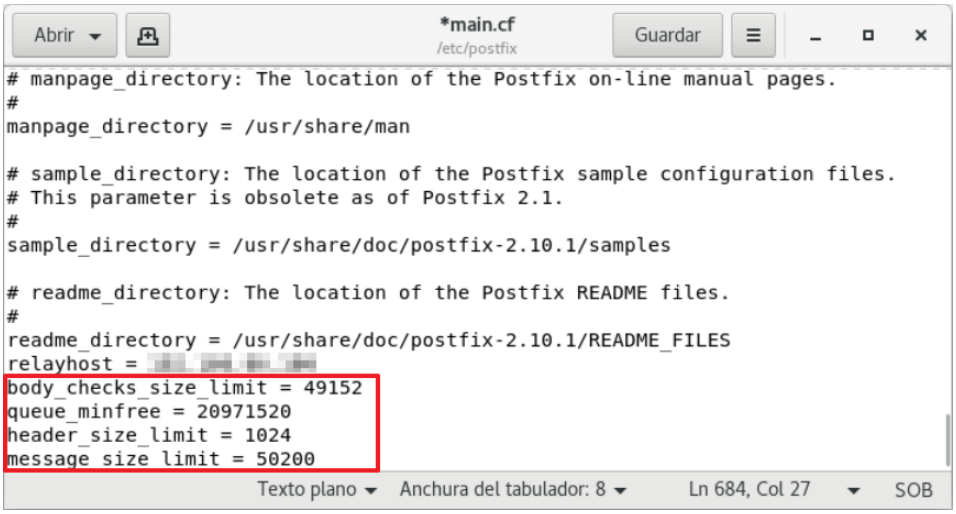
Nota: Si en el paso anterior ha instalado la herramienta **OpenDkim**, al volver a ejecutar el script le mostrará el error de la siguiente imagen. Esto es debido a la instalación por defecto de la herramienta OpenDkim, el sistema agrega librerías y dependencias de **sendmail** que si no se están utilizando son innecesarias junto con postfix.
Deberá en ese caso enmascarar servicios y demonios de sendmail evitando posibles incompatibilidades con la configuración de postfix y reduciendo el área de exposición.
Si se encuentra en esta situación ejecute el siguiente comando.

- **$ sudo systemctl mask sendmail**

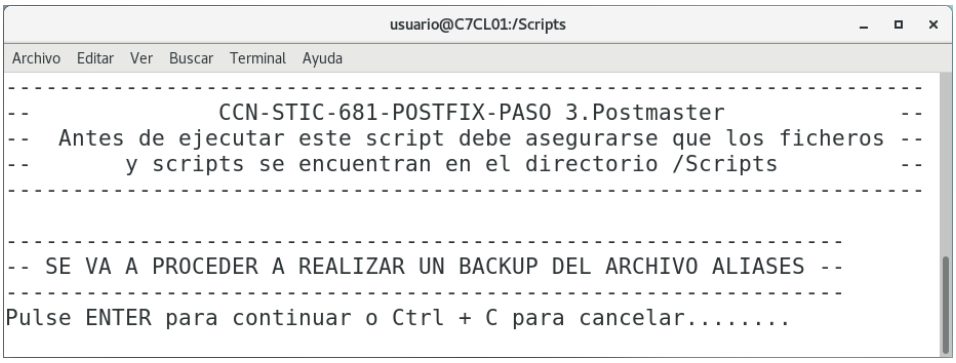
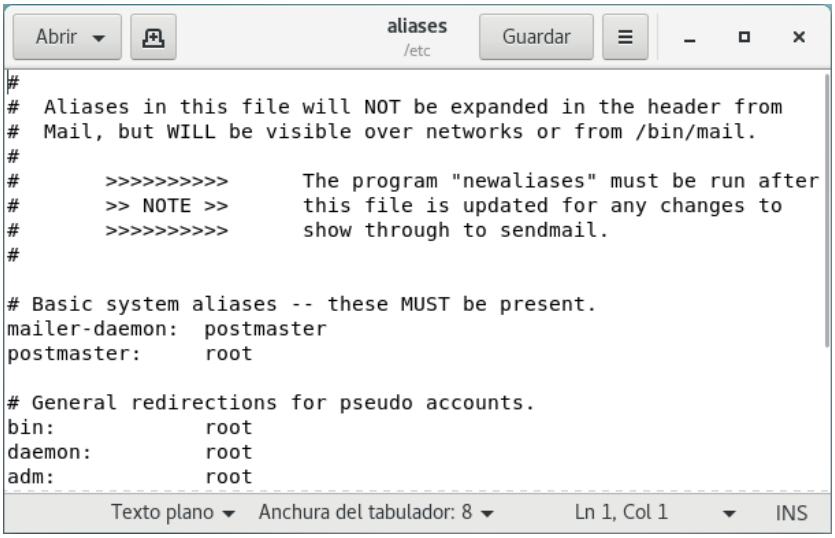


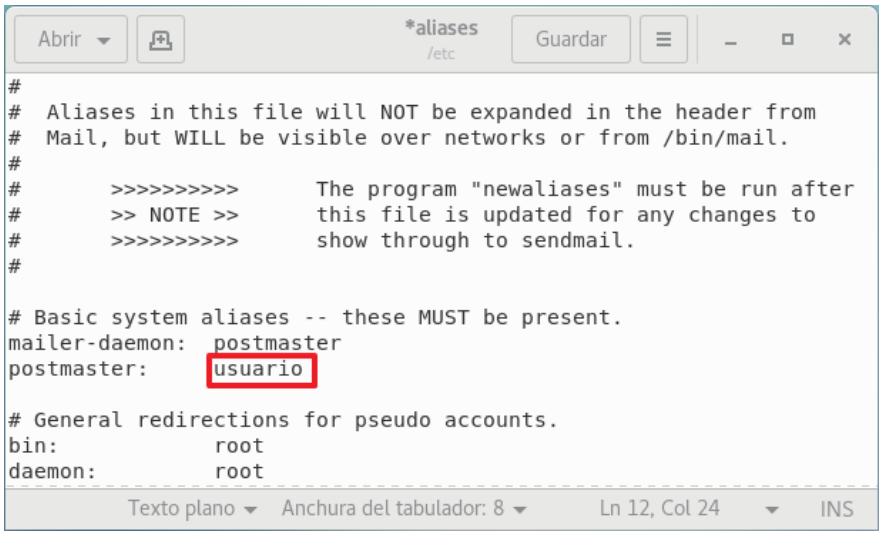
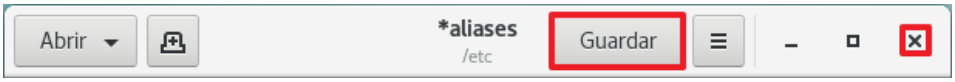
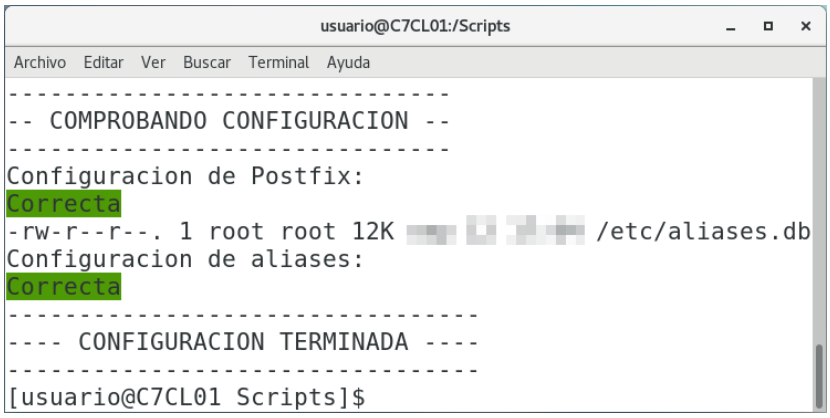
Paso	Descripción
22.	Por motivos de seguridad preservando los datos y configuraciones de su organización, se va a proceder a realizar una copia de seguridad de las configuraciones originales de todos los archivos de configuración susceptibles de ser cambiados por esta guía. Para dicho proceso, escriba los siguientes comandos. **$ sudo mkdir /home/usuario/BACKUP/** **$ sudo cp -f /etc/aliases /home/usuario/BACKUP/aliases_copia** **$ sudo cp -f /etc/postfix/main.cf /home/usuario/BACKUP/main.cf_copia** **$ sudo cp -f /etc/postfix/master.cf /home/usuario/BACKUP/master.cf_copia** **Nota:** Debe elegir una ruta o medio extraíble donde ubicar dichas configuraciones para una posible restauración a un punto anterior. La ubicación "/home/BACKUP/" es la ubicación elegida por esta guía a modo de ejemplo. Adapte la configuración según requisitos específicos de su organización.
23.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso2_configuracion_main.cf.sh**
24.	Para continuar con la ejecución del script, pulse "ENTER". usuario@C7CL01:/Scripts Archivo Editar Ver Buscar Terminal Ayuda -- CCN-STIC-681-POSTFIX-PASO 2 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- Pulse ENTER para continuar o Ctrl + C para cancelar.....
25.	Para configurar el fichero "main.cf" pulse "Enter". Introduzca los parámetros relativos a las interfaces de red y pulse "Enter" cuando finalice de configurar cada uno de los parámetros. usuario@C7CL01:/Scripts Archivo Editar Ver Buscar Terminal Ayuda -- SE PROCEDERA A CONFIGURAR EL ARCHIVO MAIN.CF -- Pulse ENTER para continuar o Ctrl + C para cancelar..... Escriba el valor de inet_interfaces: all Escriba la direccion IP del equipo de relay: 10.0.2.15 Escriba el banner del servidor: EL ACCESO A ESTE RECURSO ESTA RESTRINGIDO A LOS USUARIOS AUTORIZADOS ---- LOS VALORES ESCOGIDOS SON LOS SIGUIENTES ---- all inet_interfaces 10.0.2.15 relayhost EL ACCESO A ESTE RECURSO ESTA RESTRINGIDO A LOS USUARIOS AUTORIZADOS banner Pulse ENTER para continuar o Ctrl + C para cancelar..... **Nota:** Tras introducir cada parámetro, deberá pulsar "ENTER" de nuevo para que quede registrado en el fichero. Tenga en cuenta que un parámetro en blanco también puede ser una configuración correcta. Deberá adaptar la configuración a los parámetros de su organización.

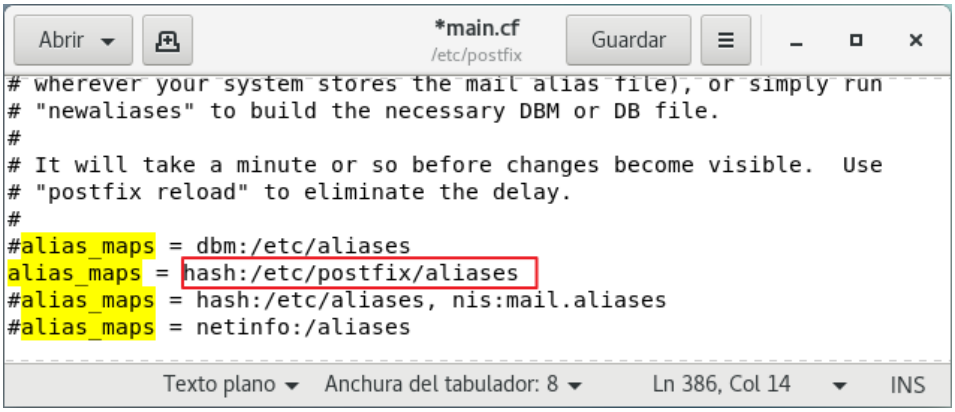
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>26.</td><td>Seguidamente se visualizan los parámetros seleccionados. Si por error se inserta un parámetro no deseado, pulse la combinación de teclas “Ctrl + c” y vuelva a ejecutar el script. Si la inserción ha sido correcta, pulse “ENTER” para continuar.
<pre>

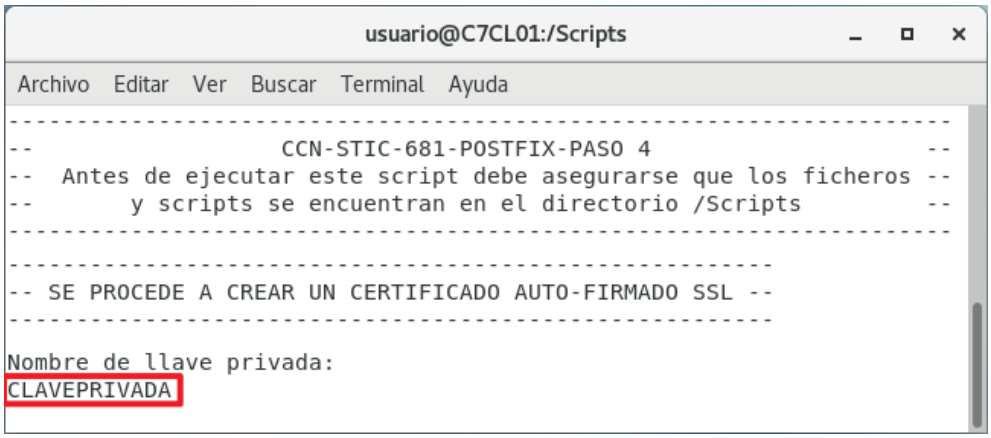
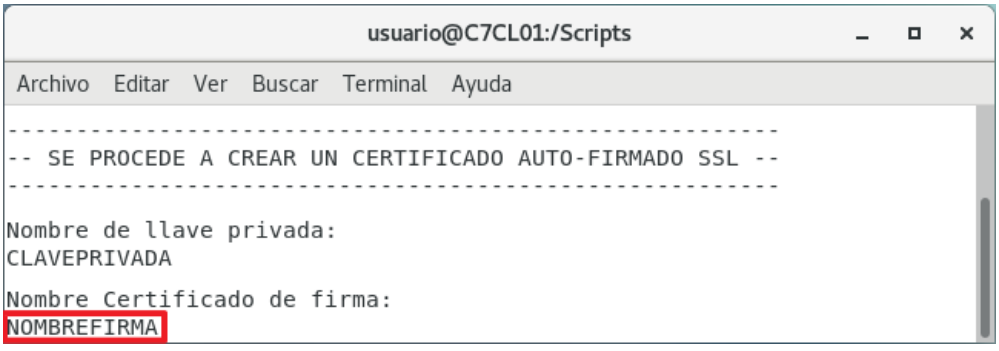
---- LOS VALORES ESCOGIDOS SON LOS SIGUIENTES ----
----
all inet_interfaces
10.0.2.15 relayhost
EL ACCESO A ESTE RECURSO ESTA RESTRINGIDO A LOS USUARIOS AUTORIZADOS
banner
Pulse ENTER para continuar o Ctrl + C para cancelar........
</pre></td></tr>
<tr><td>27.</td><td>El script editará el fichero de configuración, deberá insertar en el archivo los valores correspondientes al tamaño de mensajes, el mínimo de memoria para la correcta función de Postfix, el tamaño de cabecera de los correos electrónicos y el tamaño del cuerpo de los mensajes.
A continuación, se muestran los valores recomendados para cada opción.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>body_checks_size_limit =</td><td>49152</td></tr>
<tr><td>queue_minfree =</td><td>20971520</td></tr>
<tr><td>header_size_limit =</td><td>1024</td></tr>
<tr><td>message_size_limit =</td><td>50200</td></tr>
</table>
Nota: Deberá adaptar los valores a los requeridos por su organización.


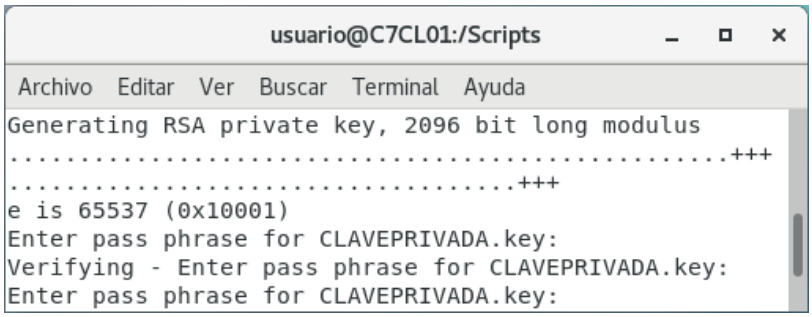
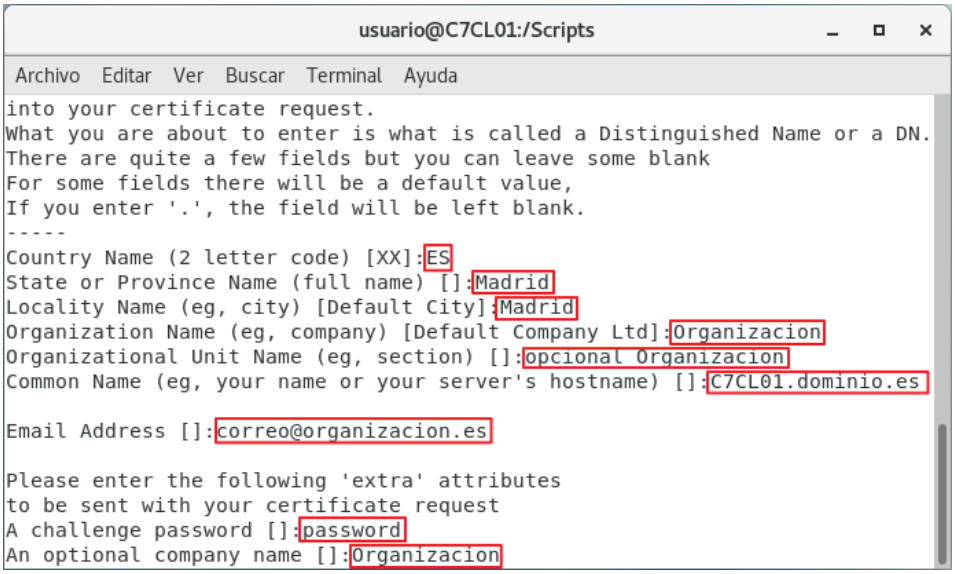
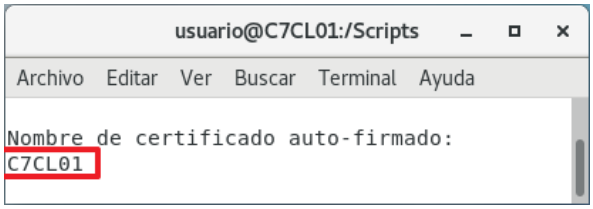
Además, deberá añadir la siguiente información en el fichero.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>Mydomain =</td><td><Su dominio></td></tr>
<tr><td>Myhostname =</td><td><El nombre del servidor></td></tr>
<tr><td>Myorigin =</td><td><Su dominio></td></tr>
</table></td></tr>
</table>

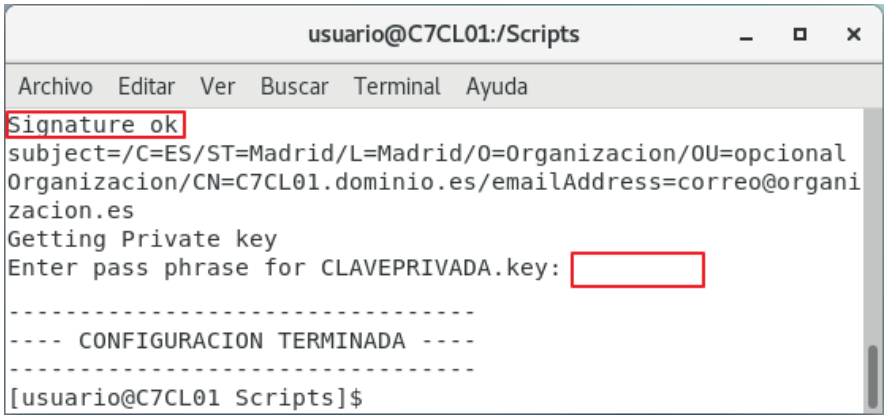
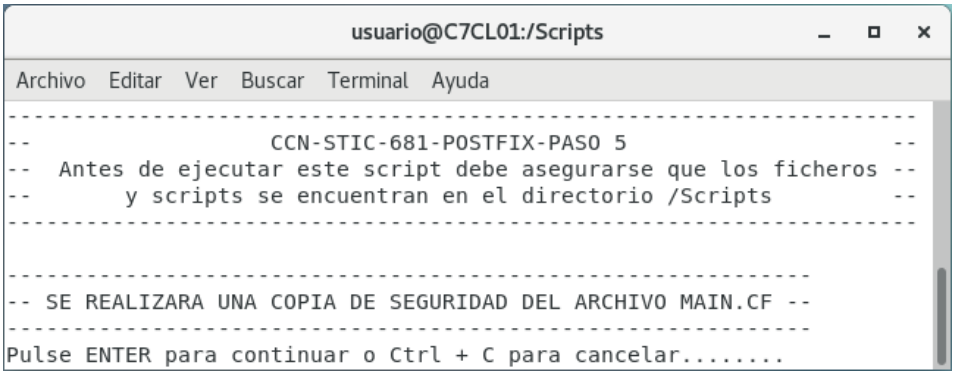
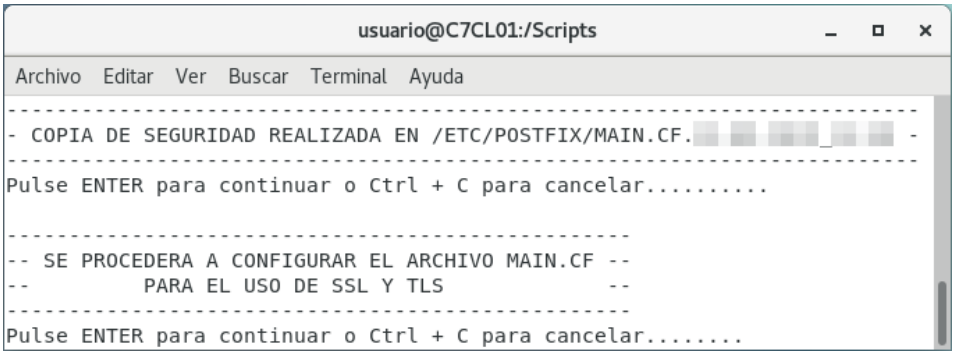
Paso	Descripción
28.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
29.	La configuración termina con la salida del proceso de configuración y el mensaje de finalización del mismo.
30.	Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso3_Postmaster.sh** 
31.	Se le comunicará la correcta realización de la copia de seguridad. 
32.	Seguidamente se abrirá una ventana editando el fichero /etc/aliases. 

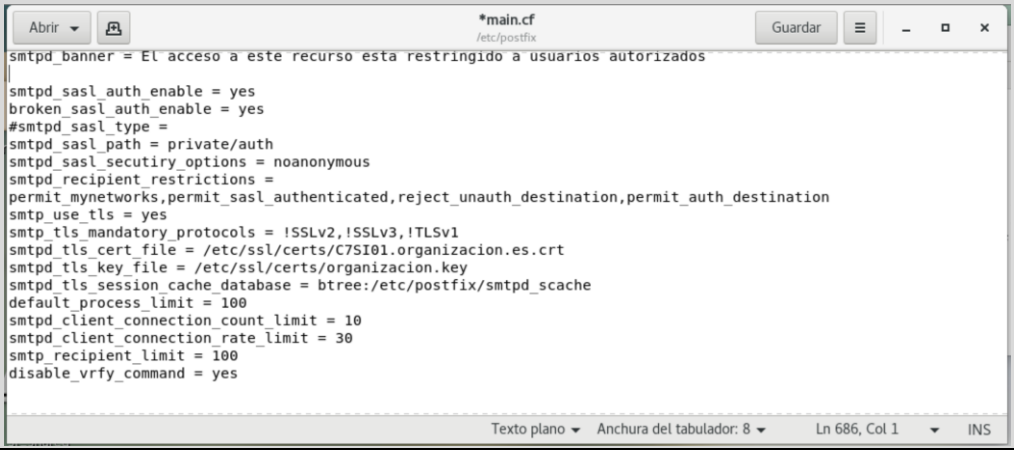
Paso	Descripción
33.	Por defecto la figura de “Postmaster” recae en el usuario “root”, Deberá asignar dicha figura a un usuario administrador. Modifique el documento con los parámetros requeridos.  **Nota:** En el ejemplo se le han entregado dichos privilegios al usuario “usuario”.
34.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
35.	El script comprobará el fichero y los permisos de /etc/aliases y finalizará con el mensaje “CONFIGURACIÓN TERMINADA”.  **Nota:** Si hubiera alguna discrepancia, restaure el archivo de copia de seguridad y ejecute de nuevo el script siguiendo los pasos de configuración.

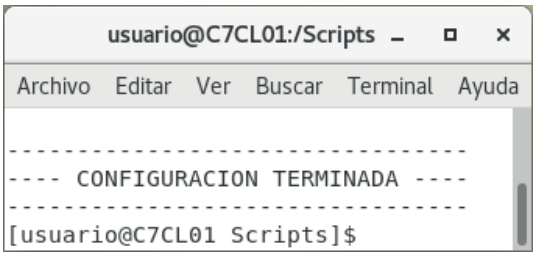
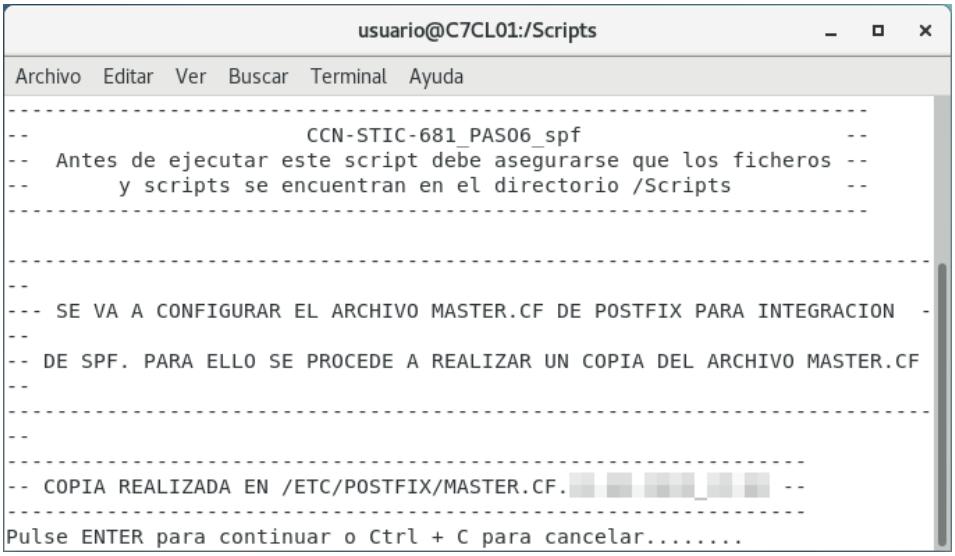
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>36.</td><td>Deberá editar el archivo de configuración main.cf de Postfix, para que el servidor postfix pueda detectar la nueva configuración. Introduzca la contraseña si se le solicita.
$ sudo gnome-text-editor /etc/postfix/main.cf &>/dev/null
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>alias_maps =</td><td>hash:/etc/postfix/aliases</td></tr>
</table>

</td></tr>
<tr><td>37.</td><td>Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.
 
</td></tr>
<tr><td>38.</td><td>Para actualizar la tabla de alias de CentOS 7 Linux, ejecute el siguiente comando. Si ejecuta sin errores, no mostrará resultado por pantalla.
$ sudo newaliases</td></tr>
<tr><td>39.</td><td>Para una correcta segregación de roles y permisos, deberá designar la monitorización de los logs y actividades de correo a un grupo específico designado por la organización. Además, deberá otorgar permisos al directorio de log de CentOS 7 Linux (/var/log/maillog).
Se muestran comandos de ejemplo para realizar estas tareas. Siendo, sin comillas, “monitorización” el grupo designado para tales tareas de mantenimiento, añadiendo al grupo el usuario o usuarios designados para dichas funciones.
$ sudo groupadd “monitorización”
$ sudo chgrp –R “monitorización” /var/log/maillog
$ sudo usermod –a –G “monitorización” “usuarios designados”
Nota: Los comandos anteriores nombran en modo de ejemplo y entre comillas (“”) a los usuarios y grupos. Para adaptar esta configuración a las necesidades de su organización, tendrá que escribir los usuarios y grupos sin comillas (“”) para la correcta aplicación del comando.</td></tr>
</table>

Paso	Descripción
40.	La modificación de permisos sobre la carpeta de logs de los correos electrónicos se realiza desde la línea de comandos, otorgando los permisos de escritura y lectura al usuario y al grupo designados. El usuario del sistema "root" será el poseedor de la carpeta para el correcto funcionamiento del sistema y poseerá los permisos equivalentes a "660". **$ sudo chmod -660 /var/log/maillog**
41.	La implementación de certificados puede realizarse empleando certificados emitidos por una entidad certificadora perteneciente a la organización o bien por un certificado adquirido a una entidad certificadora oficial de terceros. Para realizar las modificaciones relativas al uso de certificados ejecute el siguiente comando para generar un certificado SSL autofirmado. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso4_certificados_openSSL.sh** **Nota:** En este paso a paso, se va a realizar una configuración con certificados auto firmados, puesto que no todas las organizaciones poseen acceso a una entidad certificadora (CA) oficial.
42.	Se procederá a crear la clave privada RSA. Deberá dar un nombre al fichero ".key" y pulsar "ENTER" para continuar. 
43.	Posteriormente introduzca un nombre para el fichero CSR (solicitud de firma de certificado) que se generará posteriormente. Pulse "Enter" para continuar. 

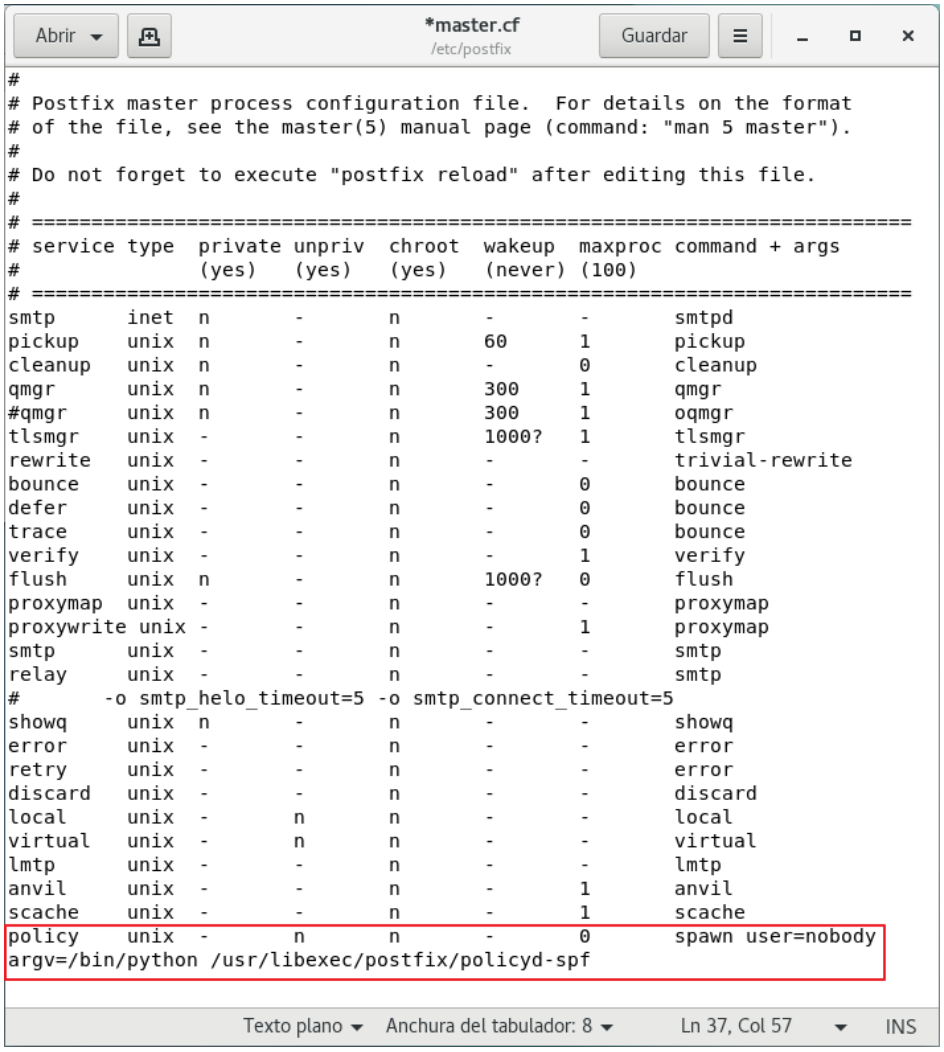
Paso	Descripción
44.	Se generará la clave privada RSA con una longitud de 2096 bits y seguidamente solicitará la contraseña, una verificación de la misma y una tercera solicitud. Introduzca la contraseña y pulse “Enter” repitiendo el proceso en las tres ocasiones. 
45.	Durante la generación del CSR, se solicitará diversa información sobre su organización relativa a los atributos X.509 del certificado. Uno de los puntos más relevantes es el dato “Common Name” que corresponde al nombre del equipo junto al dominio completo con el que se va a realizar la conexión SSL. Rellene cada campo con los requerimientos específicos de su organización y pulse “Enter” para continuar.  **Nota:** Deberá pulsar “ENTER” para que los datos queden introducidos en la información del certificado.
46.	Continúe con el proceso nombrando el certificado. Cuando finalice pulse “ENTER”. 

Paso	Descripción
47.	El proceso finaliza con el mensaje “Signature ok” y mostrando las configuraciones elegidas. Para finalizar el proceso de generación de firma “auto-firmada”, se solicita que ingrese la contraseña de su clave privada. 
48.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso5_Seguridad.sh**
49.	La primera acción que se realizará a través el script es la copia de seguridad del archivo a configurar, /etc/postfix/main.cf. Para continuar con la ejecución del script pulse la tecla “ENTER”. 
50.	Se confirma la realización de la copia de seguridad. Una vez realizada la copia, pulse “ENTER”. Se procederá a configurar el archivo main.cf. Pulse “ENTER” para continuar. Esto abrirá el fichero main.cf en el editor de texto. 

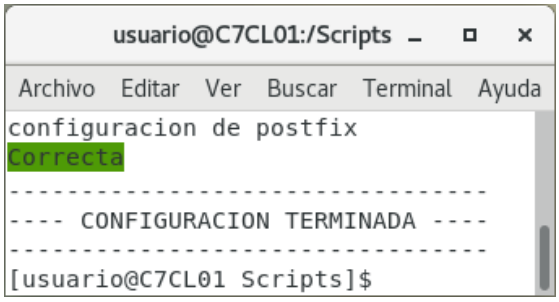
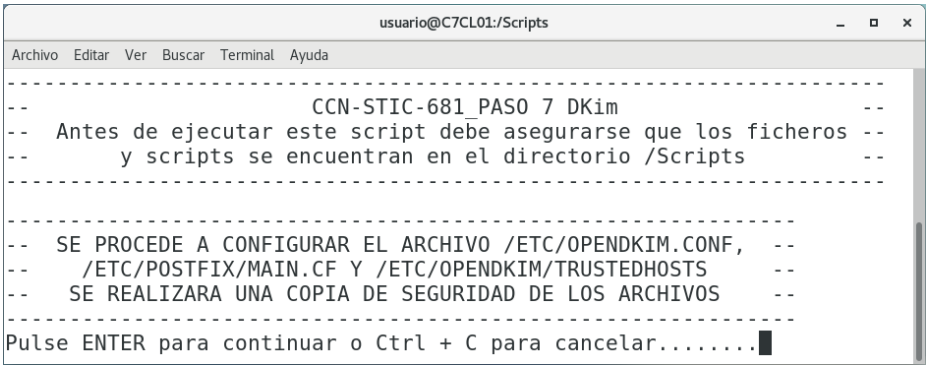
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>51.</td><td>A continuación, se muestra una tabla con los valores recomendados que se deberán aplicar en el archivo de configuración main.cf de Postfix.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>smtpd_sasl_auth_enable =</td><td>yes</td></tr>
<tr><td>broken_sasl_auth_clients =</td><td>yes</td></tr>
<tr><td>#smtpd_sasl_type =</td><td></td></tr>
<tr><td>smtpd_sasl_path =</td><td>private/auth</td></tr>
<tr><td>smtpd_sasl_security_options =</td><td>noanonymous</td></tr>
<tr><td>smtpd_recipient_restrictions =</td><td>permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_destination,
reject_unauth_destination,
permit_auth_destination</td></tr>
<tr><td>smtp_use_tls =</td><td>yes</td></tr>
<tr><td>smtp_tls_mandatory_protocols =</td><td>!SSLv2,!SSLv3, !TLSv1</td></tr>
<tr><td>smtpd_tls_cert_file =</td><td>/etc/ssl/certs/<certificado></td></tr>
<tr><td>smtpd_tls_key_file =</td><td>/etc/ssl/certs/<certificado></td></tr>
<tr><td>smtpd_tls_session_cache_database =</td><td>btree:/etc/postfix/smtpd_scache</td></tr>
<tr><td>default_process_limit =</td><td>100</td></tr>
<tr><td>smtpd_client_connection_count_limit =</td><td>10</td></tr>
<tr><td>smtpd_client_connection_rate_limit =</td><td>30</td></tr>
<tr><td>smtpd_recipient_limit =</td><td>100</td></tr>
<tr><td>disable_vrfy_command =</td><td>yes</td></tr>
</table>
Nota: Si detectara que alguno de estos parámetros ya existe en el documento , se deberá modificar el valor en lugar de generar una línea nueva.
Debe tener en cuenta que en Postfix, un parámetro sin ningún valor se considera como un parámetro válido de configuración. Así mismo deberá tener en consideración los valores establecidos en la tabla anterior y adaptarlos a los valores que más se ajusten a las necesidades de su organización.

</td></tr>
</table>

Paso	Descripción
52.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
53.	El script finalizará mostrando el mensaje “**CONFIGURACION TERMINADA**”. 
54.	Se procede a realizar una la integración de SPF sobre Postfix. Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso6_spf.sh** **Nota:** Para la integración en el servidor de la funcionalidad SPF, deberá de poseer anteriormente ciertas configuraciones específicas en un servidor DNS para que el complemento surta efecto. No es objetivo de esta guía la configuración de un servidor DNS para tal efecto.
55.	Para ello, primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar “ENTER” para continuar. 

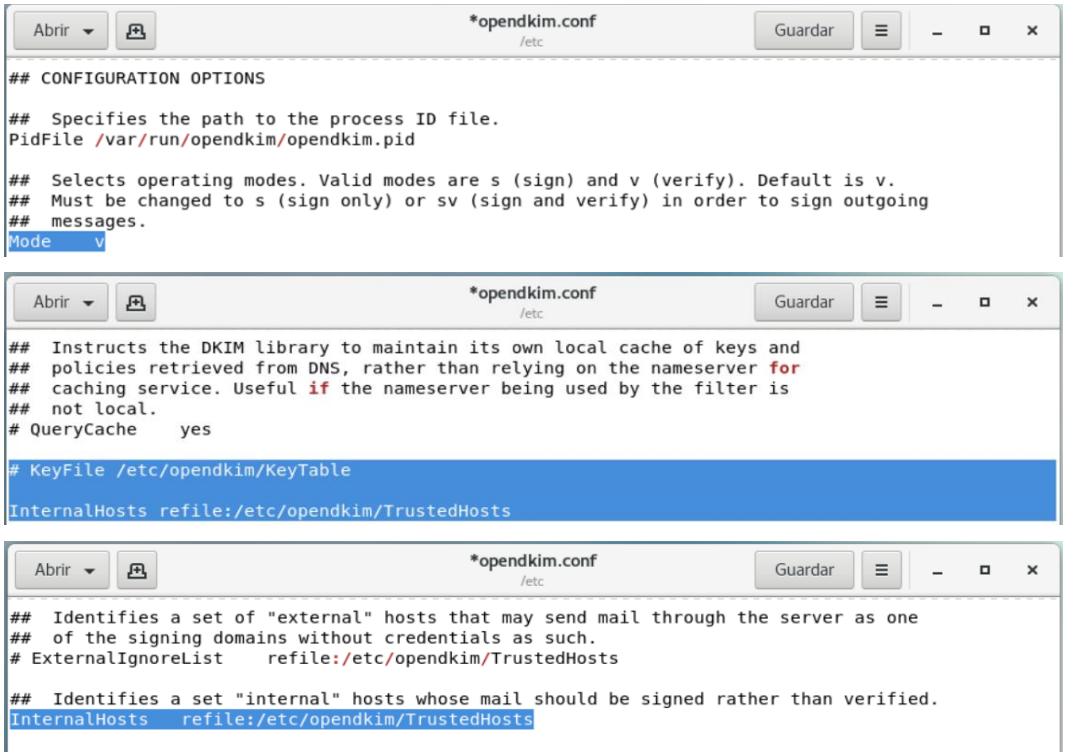
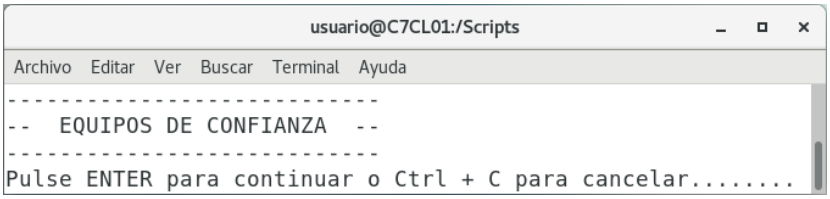
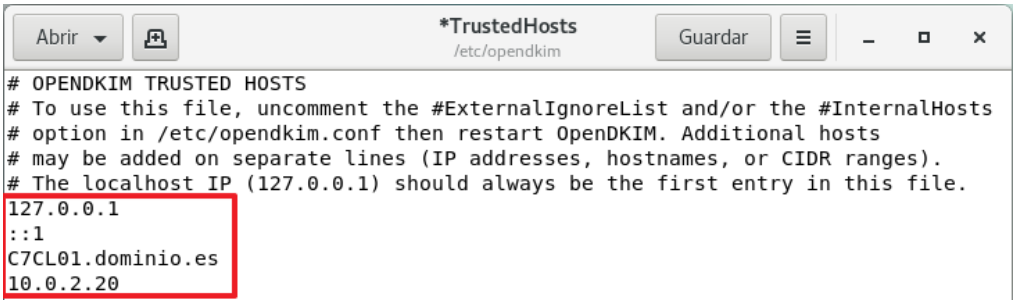
Paso	Descripción
56.	El script editará el fichero master.cf. Inserte la siguiente línea en master.cf para configurar SPF. **policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf**
57.	Pulse “Guardar” y cierre el Editor de textos pulsando la “**x**” situada en la zona superior derecha de la ventana.

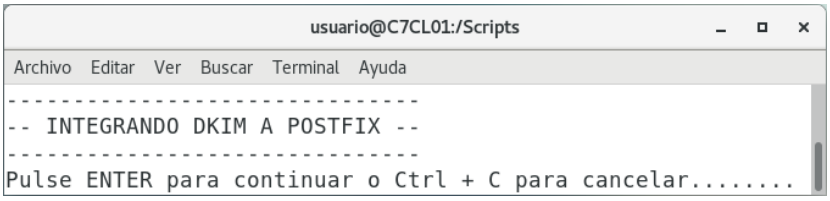
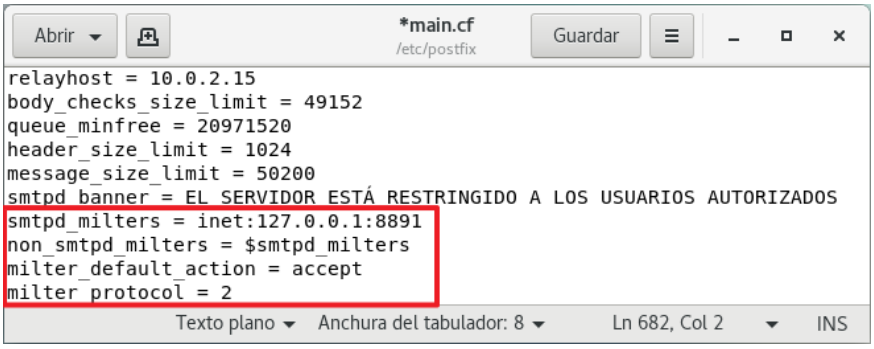


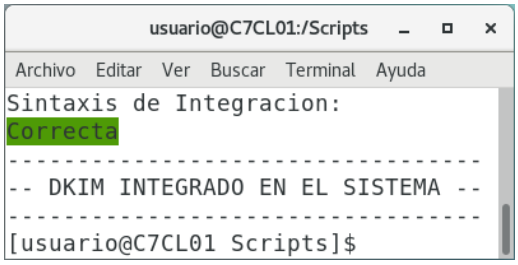
Nota: Tenga en cuenta que el fichero de configuración de la imagen se ha modificado del original para clarificar los parámetros que se deben modificar. Es posible que en su caso pueda tener varias líneas comentadas (#) intermedias.

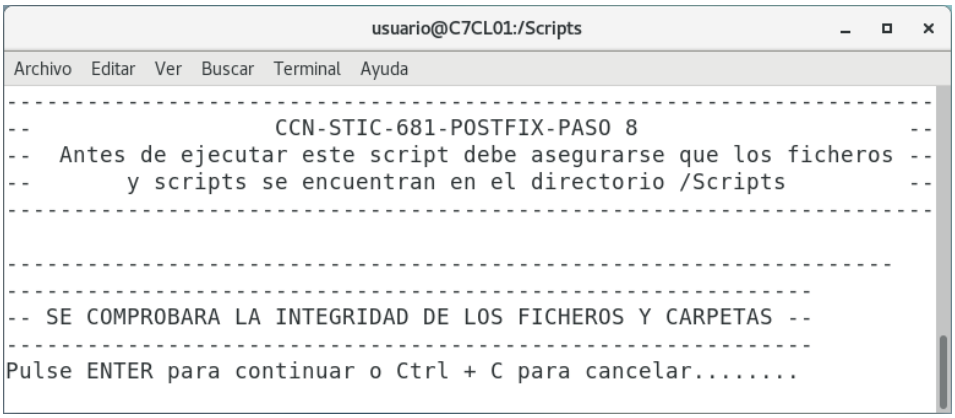
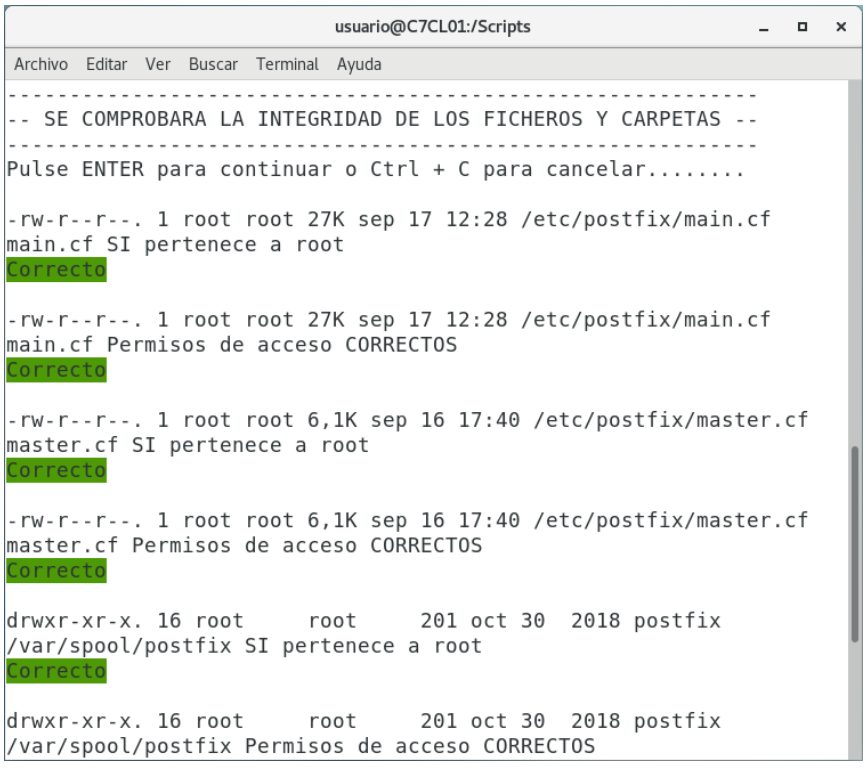
Paso	Descripción
58.	El proceso finaliza con el siguiente mensaje, realizándose una comprobación de sintaxis. 
59.	Ejecute el siguiente comando para continuar con la configuración. Ingrese la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_MEDIO_Paso7_Dkim.sh** **Nota:** Para la integración en el servidor de la herramienta OpenDkim, deberá de poseer anteriormente ciertas configuraciones específicas en un servidor DNS para que las acciones surtan efecto. No es objetivo de esta guía la configuración de un servidor DNS para tal efecto.
60.	Se procede a realizar una la integración de SPF sobre Postfix. Para ello primero se realiza una copia de seguridad de los archivos. Deberá pulsar “ENTER” para continuar. 
61.	Se muestra la configuración a modificar en opendkim.cf, los valores mostrados son los adecuados a la categoría de seguridad. **Nota:** Deberá adaptar los parametros de la tabla a los que mas convengan en su organización. Si el valor de la columna izquierda existe, deberá modificarlo con lo indicado en la tabla, si no existe añadir el valor de la columna derecha.

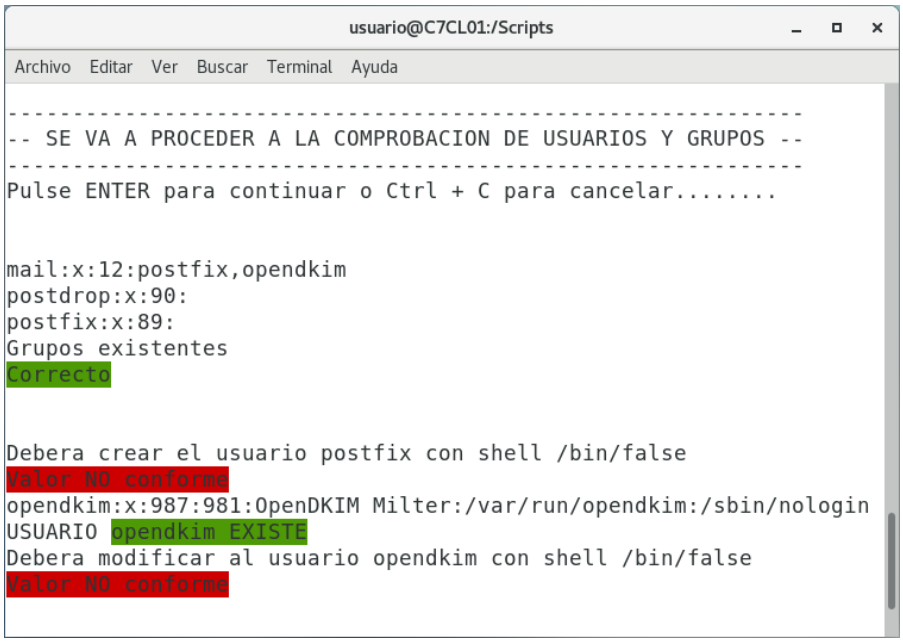
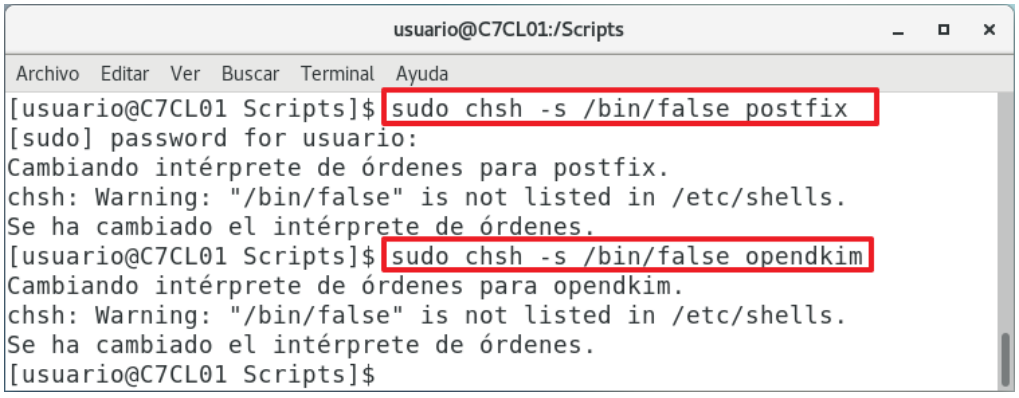
Parámetro	Valor
Mode <valor>	Mode v
KeyFile /etc/opendkim/keys/default.private	#KeyFile/etc/opendkim/keys/default.private
KeyTable /etc/opendkim/KeyTable	#KeyTable /etc/opendkim/KeyTable
#InternalHosts refile:/etc/opendkim/TrustedHosts	InternalHosts refile:/etc/opendkim/TrustedHosts

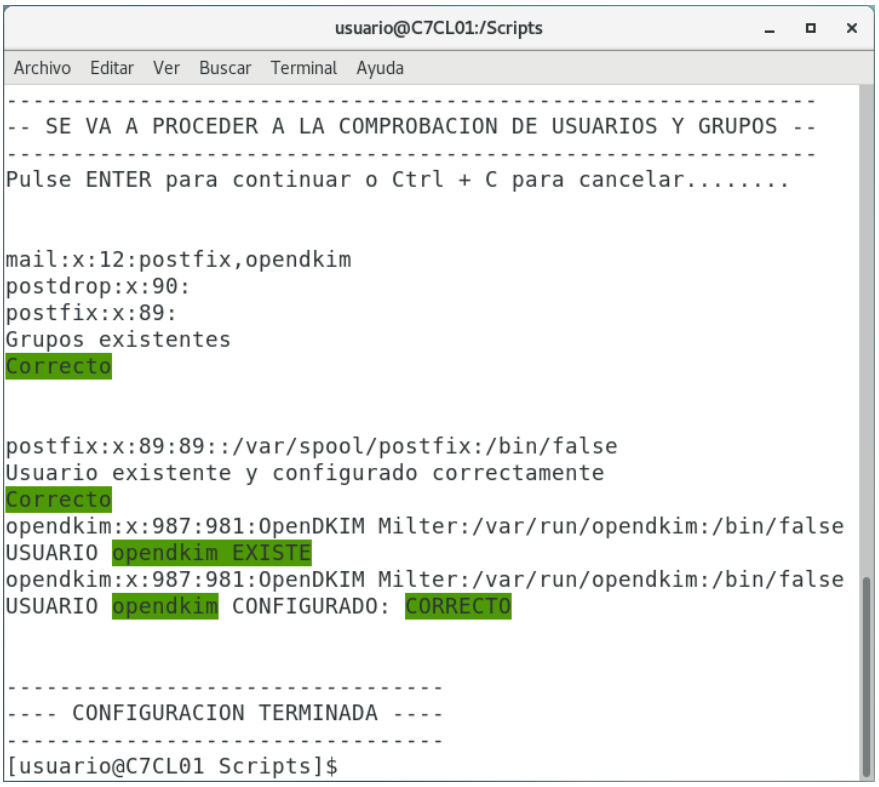
Paso	Descripción
62.	A continuación, se muestran a modo de ejemplo como deberán quedar establecidos los valores en el archivo de configuración. 
63.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
64.	Se procede a añadir la excepción de equipos de confianza, pulse “ENTER” para continuar. 
65.	A continuación, se muestra, a modo de ejemplo, una configuración del archivo /etc/opendkim/TrustedHosts. 

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>66.</td><td>Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.</td></tr>
<tr><td>67.</td><td>Con la inserción de valores en el archivo /etc/postfix/main.cf se concluirá la integración de OpenDkim con Postfix. Pulse “ENTER” para continuar.
 
</td></tr>
<tr><td>68.</td><td>El script editará el fichero de configuración, inserte los parámetros de seguridad recomendados contenidos en la siguiente tabla y adáptelos a los específicos de su organización.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>smtpd_milters =</td><td>inet:127.0.0.1:8891</td></tr>
<tr><td>non_smtpd_milters =</td><td>$smtpd_milters</td></tr>
<tr><td>milter_default_action =</td><td>accept</td></tr>
<tr><td>milter_protocol =</td><td>2</td></tr>
</table>


Nota: Tenga en cuenta que el fichero de configuración de la imagen se ha modificado del original para clarificar los parámetros que se deben modificar.</td></tr>
<tr><td>69.</td><td>Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.
 
</td></tr>
<tr><td>70.</td><td>El script finaliza el proceso con una comprobación de sintaxis.
 
</td></tr>
</table>

Paso	Descripción
71.	Para continuar ejecute el siguiente script. El script iniciará el proceso de verificación de acceso y pertenencia de los archivos y carpetas necesarias para el correcto funcionamiento seguro de Postfix. Pulse “ENTER” para continuar. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso8_comprobacion_configuracion.sh** 
72.	El script comprobará si permisos en archivos y carpetas pertenecientes a Postfix se encuentran correctamente configuradas según parámetros de seguridad recomendados. Seguidamente, pulsando “ENTER” continuará la ejecución del script.  **Nota:** Si en el caso de que los archivos no pertenezcan a root o no tengan los permisos adecuados deberá cambiarlos con los comandos **chmod** y **chown,** y según los parámetros que más se adecuen a los de su organización.

Paso	Descripción
73.	El Script continua con la comprobación de los usuarios y grupos y sus respectivas "shells". Pulse "ENTER" para continuar. El script finalizará con el mensaje "CONFIGURACION TERMINADA".  **Nota:** Si no existieran los grupos postdrop y postfix, o el usuario postfix, deberá reinstalar Postfix junto con su usuario y grupos correspondientes.
74.	Teniendo en consideración los parámetros de su organización deberá corregir las deficiencias encontradas en el paso anterior y repetir la ejecución del script posteriormente. Para ello y si se encuentra en este caso, ejecute los siguientes comandos. **$ sudo chsh -s /bin/false postfix** **$ sudo chsh -s /bin/false opendkim** 

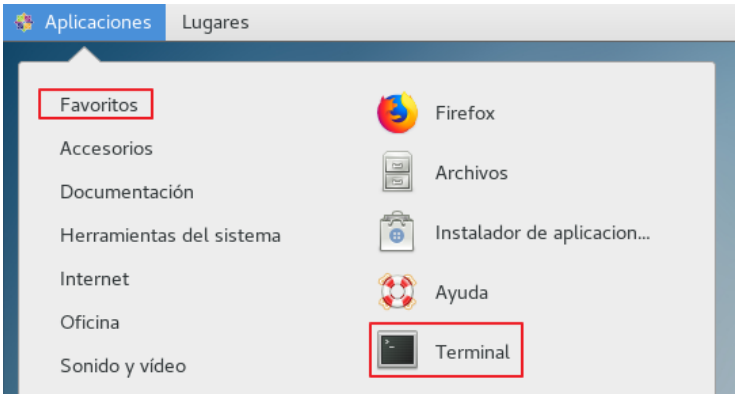
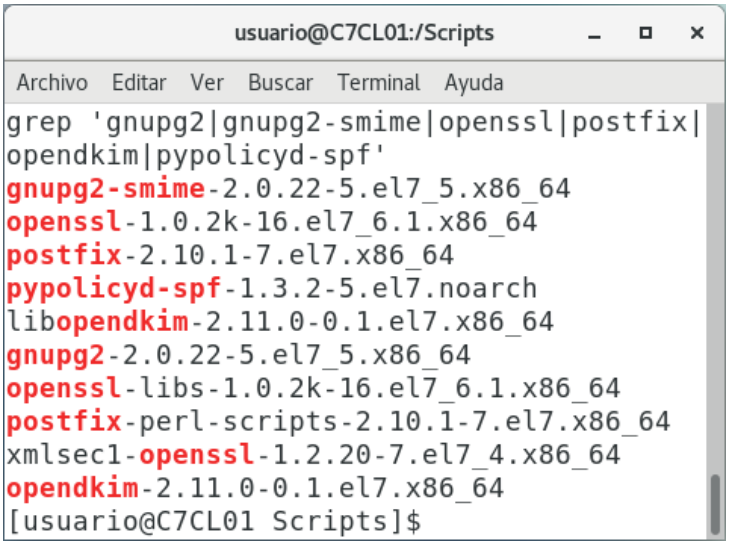
Paso	Descripción
75.	Repita la ejecución del script de la misma forma que en pasos anteriores y compruebe que las deficiencias encontradas se encuentran subsanadas. La ejecución del script finalizará con el mensaje “CONFIGURACION TERMINADA”. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso8_comprobacion_configuracion.sh** 
76.	El último paso consiste en habilitar los servicios necesarios para el correcto funcionamiento del sistema. Ejecute los siguientes comandos e introduzca la contraseña si se le solicita. **$ sudo systemctl unmask postfix.service** **$ sudo systemctl start postfix.service** **$ sudo systemctl enable postfix.service** **$ sudo systemctl restart opendkim**
77.	Elimine la carpeta **/Scripts** y todo su contenido.
78.	Guarde las aplicaciones que se encuentren abiertas y reinicie el servidor. **$ sudo shutdown -r**

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR CENTOS7 ENS CATEGORÍA MEDIA

Para realizar las comprobaciones pertinentes en el equipo se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán son las siguientes.

a) Terminal.

b) Editor de textos.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En uno de los equipos CentOS 7, inicie sesión con una cuenta que tenga privilegios de administración.
2. Inicie la Terminal de Linux.		Ejecute la "Terminal". Para ello Diríjase a la barra de tareas superior, pulse en Aplicaciones y en el apartado Favoritos seleccione "Terminal". 
3. Verifique que se encuentren instalados los paquetes necesarios.		En la "terminal" ejecute el siguiente comando. **$ sudo rpm -aq | egrep 'gnupg2|gnupg2-smime|openssl|postfix|opendkim|pypolicyd-spf'**  **Nota:** Deberá comprobar que las versiones de los paquetes que aquí se comprueban, se encuentran en sus últimas versiones.

Comprobación	OK/NOK	Cómo hacerlo

Parámetros	OK/NOK
gnupg2-smime-[**versión actualizada**]	
openssl-[**versión actualizada**]	
postfix-[**versión actualizada**]	
pypolicyd-spf-[**versión actualizada**]	
gnupg2-[**versión actualizada**]	
openssl-libs-[**versión actualizada**]	
postfix-perl-scripts-[**versión actualizada**]	
xmlsec1-openssl-[**versión actualizada**]	
opendkim-[**versión actualizada**]	

4. Copias de seguridad de la organización

Compruebe que se realizó exitosamente una copia de seguridad de los siguientes archivos antes de aplicar configuraciones de esta guía. Para ello, ejecute los siguientes comandos y compruebe que existen dichos archivos.

Nota: Ajuste las rutas a las específicas de su organización.

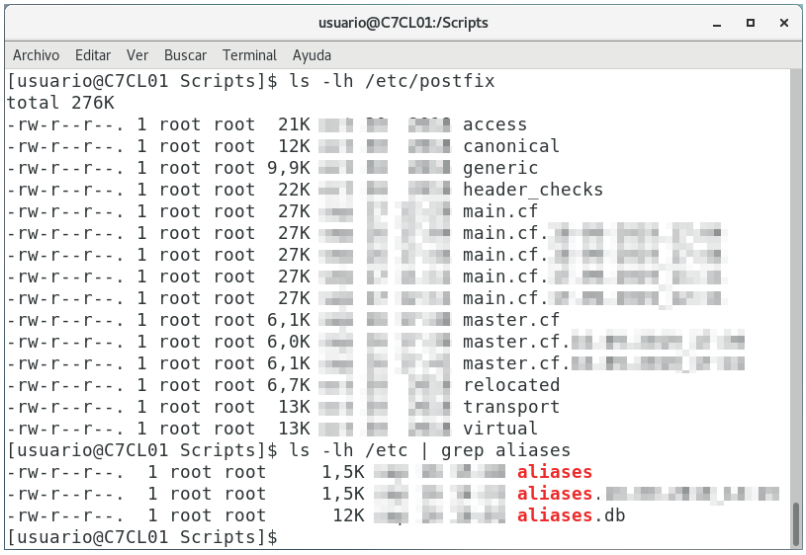
Configuración	OK/NOK
ls /home/usuario/BACKUP/ | egrep "main.cf"	
ls /home/usuario/BACKUP/ | egrep "master.cf"	

5. Copias de seguridad de la organización

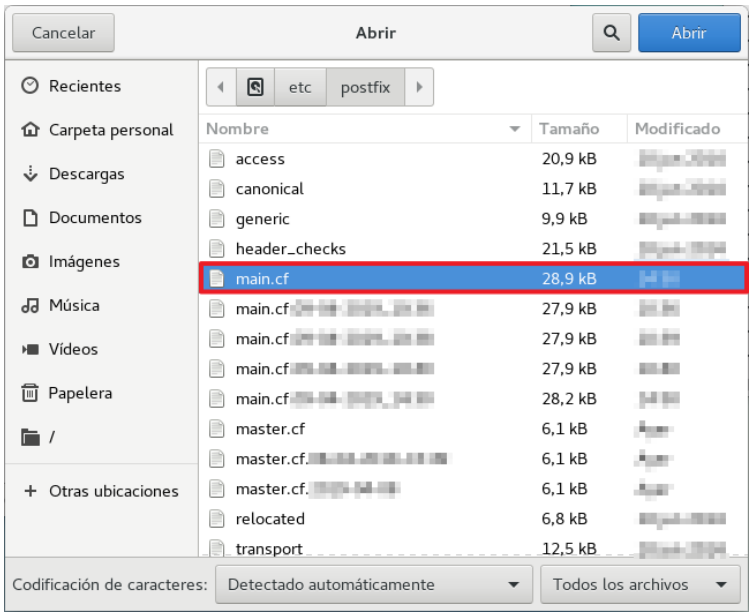
En un terminal ejecute los siguientes comandos.

```
$ ls -lh /etc/postfix
$ ls -lh /etc | grep aliases
```

Revise que se han realizado las correspondientes copias de seguridad de los archivos según la ejecución de los scripts correspondientes.



Nota: Tenga en consideración que poseerá tantas copias como veces haya ejecutado los scripts.

Comprobación	OK/NOK	Cómo hacerlo	
		Configuración	**OK/NOK**
		master.cf.[FECHA]	
		main.cf.[FECHA]	
		Aliases.[FECHA]	
6. Configuración del archivo main.cf		Edite el archivo "main.cf" pulsando sobre el botón "Abrir" o haciendo doble clic izquierdo con el ratón.  Compruebe los siguientes parámetros y cierre el editor de texto al finalizar la comprobación mediante la **"x"** de la esquina superior derecha de la ventana.	

Parámetros	Valor	OK/NOK
mydomain	[**DOMINIO**]	
myhostname	[**SERVIDOR POSTFIX**]	
myorigin	[**DOMINIO**]	
inet_protocols	Ipv4	
inet_interfaces	all	
mydestination	$myhostname, localhost.$mydomain, localhost	
relayhost	[**SERVIDOR DE CORREO PRINCIPAL**]	
smtpd_sasl_auth_enable	Yes	
broken_sasl_auth_clients	yes	
smtpd_sasl_path	private/auth	
smtpd_sasl_security_options	noanonymous	
smtpd_recipient_restrictions	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, permit_auth_destination	
smtp_use_tls	yes	

Comprobación	OK/NOK	Cómo hacerlo

Parámetros	Valor	OK/NOK
smtp_tls_mandatory_protocols	!SSLv2,SSLv3, TLSv1	
smtpd_tls_cert_file	/etc/ssl/private/<certificado.extensión>	
smtpd_tls_key_file	/etc/ssl/private/<clave.extensión>	
smtpd_tls_session_cache_database	btree:/etc/postfix/smtd_scache	
smtpd_banner =	[**MENSAJE DISUASORIO**]	
smtpd_milters =	inet:127.0.0.1:8891	
message_size_limit	50200	
non_smtpd_milters =	$smtpd_milters	
milter_default_action =	accept	
milter_protocol =	2	
#smtpd_sasl_type		
default_process_limit	100	
smtpd_client_connection_count_limit	10	
smtpd_client_connection_rate_limit	30	
queue_minfree	20971520	
header_size_limit	512	
smtpd_recipient_limit	100	
body_checks_size_limit	49152	
disable_vrfy_command	yes	

7. Comprobación de posesión de archivos

Se va a proceder a la comprobación del propietario de los ficheros main.cf y master.cf y de los directorios /var/spool/postfix y /var/log/mail. Todos ellos deben pertenecer al usuario “root”.
En la “terminal” ejecute los siguientes comandos.

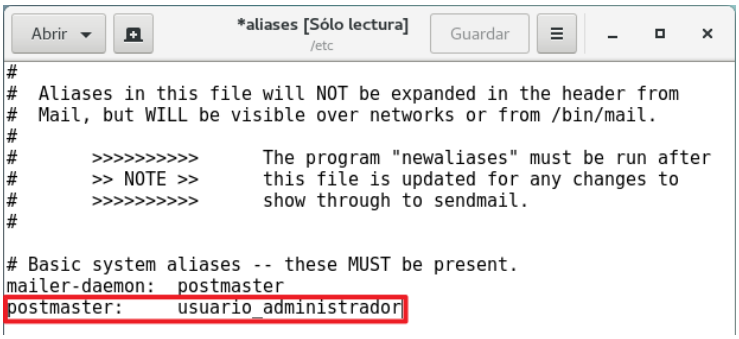
```
$ ls -lh /etc/postfix/main.cf |grep root
$ ls -lh /etc/postfix/master.cf | grep root
$ ls -lh /var/spool/ | grep postfix | grep root
$ ls -lh /var/log/maillog |grep root
```

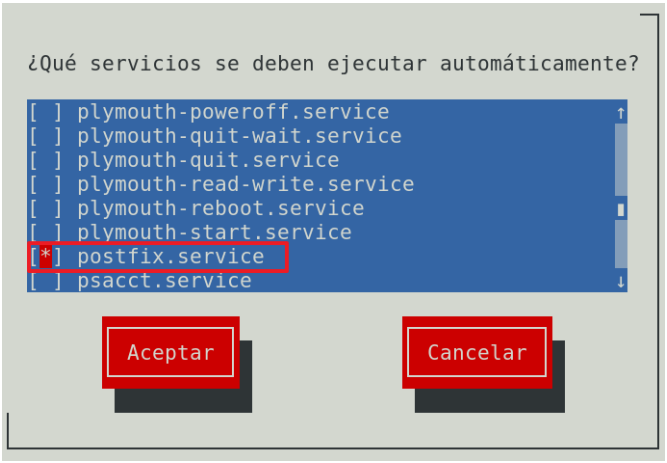
Ruta	Propietario	OK/NOK
/etc/postfix/main.cf	root	
/etc/postfix/master.cf	root	
/var/spool/	root	
/var/log/maillog	root	

8. Comprobación de permisos de archivos

Se comprobará los permisos de archivos y carpetas del sistema. Para ello ejecute los siguientes comandos.

```
$ ls -lh /etc/postfix/main.cf |grep '\-rw-r--r\--'
$ ls -lh /etc/postfix/master.cf |grep '\-rw-r--r\--'
$ ls -lh /var/spool/ | grep postfix | grep rwxr-xr-x
$ ls -lh /var/log/maillog |grep '\-rw\-------'
```

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2">Configuración</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">/etc/postfix/main.cf</td><td>-rw-r--r--</td><td></td></tr>
<tr><td></td><td colspan="2">/etc/postfix/master.cf</td><td>-rw-r--r--</td><td></td></tr>
<tr><td></td><td colspan="2">/var/spool/postfix</td><td>drwxr-xr-x</td><td></td></tr>
<tr><td></td><td colspan="2">/var/log/maillog</td><td>drw-------</td><td></td></tr>
<tr><td>9. Comprobación de Usuarios y Grupos</td><td></td><td colspan="3">Ejecute los siguientes comandos.
$ cat /etc/passwd |egrep "postfix|/bin/false "
$ cat /etc/group |egrep "postfix|postdrop"
$ cat /etc/passwd |egrep “opendkim|/bin/false "
$ cat /etc/group |egrep " opendkim”</td></tr>
<tr><td></td><td colspan="2">Configuración</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">Usuario: postfix</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Shell: postfix</td><td>/bin/false</td><td></td></tr>
<tr><td></td><td colspan="2">Grupo: postfix</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Grupo: postdrop</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Usuario: opendkim</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Shell: opendkim</td><td>/bin/false</td><td></td></tr>
<tr><td></td><td colspan="2">Grupo: opendkim</td><td>Existe</td><td></td></tr>
<tr><td>10. Cambio de usuario de Postmaster</td><td></td><td colspan="3">Compruebe que se han modificado los siguientes parámetros dentro del archivo aliases.
Para ello diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Accesorios” seleccione “Editor de textos”.
Abra el archivo “/etc/postfix/aliases” y compruebe que la figura de “postmaster” ha cambiado por otro usuario que no sea root.
 
</td></tr>
<tr><td>11. Comprobación de los certificados OpenSSL.</td><td></td><td colspan="3">En la “terminal” ejecute el siguiente comando para comprobar la creación de los certificados.
$ ls -lh /etc/ssl/certs
Nota: Los valores deben de ser coincidentes con los nombres y configuraciones específicos de su organización.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>“NOMBREFIRMA”.”extensión”</td><td>Existencia</td><td></td></tr>
<tr><td>“CLAVEPRIVADA”.key</td><td>Existencia</td><td></td></tr>
<tr><td>Permisos “CLAVEPRIVADA”.key</td><td>-r---------</td><td></td></tr>
<tr><td>Permisos “NOMBREFIRMA”.”extensión”</td><td>-rw-r--r--</td><td></td></tr>
</table></td></tr>
<tr><td>12.Servicios necesarios por medio de herramienta ntsysv</td><td></td><td colspan="3">Abra la Terminal y ejecute el siguiente comando.
$ sudo ntsysv
 

Compruebe la ejecución del siguiente servicio. Una vez realizada la comprobación utilice el tabulador para colocar el cursor y pulse “Aceptar” para cerrar “ntsysv”.
Nota: Los servicios activos están indicados con un asterisco (*).</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>postfix.service</td><td>Activo</td><td></td></tr>
<tr><td>opendkim.service</td><td>Activo</td><td></td></tr>
</table></td></tr>
<tr><td>13.Configuración del archivo master.cf</td><td></td><td colspan="3">Compruebe que se han modificado los siguientes parámetros del archivo master.cf.
Para ello, diríjase a la ruta /etc/postfix/ y edite el fichero “master.cf”.
 
</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Parámetros</th><th>OK/NOK</th></tr>
<tr><td>policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf</td><td></td></tr>
</table></td></tr>
</table>

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 2.10.1-7.EL17 SOBRE CENTOS 7 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar Postfix 2.10.1-7.el17 sobre CentOS 7, con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Este anexo será de igual aplicación cuando el sistema sobre el que se esté implementando la seguridad cumpla con los requisitos para una red clasificada con grado de clasificación Difusión Limitada. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría alta o difusión limitada, deberá realizar las implementaciones según se referencian en el presente anexo.

Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender a las peculiaridades del sistema operativo utilizado en el caso de una red de este tipo.

Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Los pasos que se describen a continuación se realizarán en todos aquellos clientes CentOS 7 con una configuración de Postfix que implementen servicios o información de categoría alta – DL y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

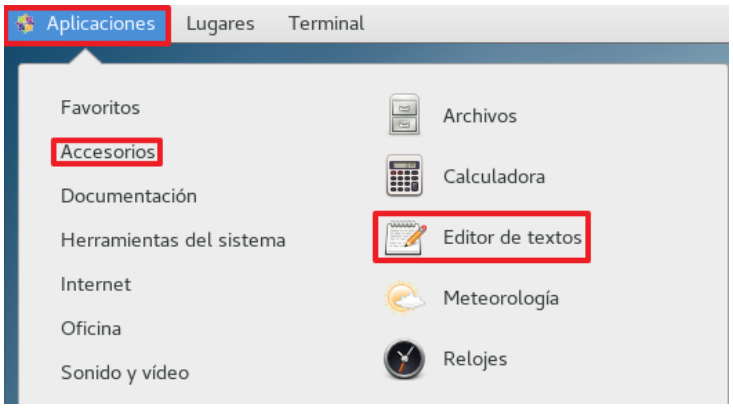
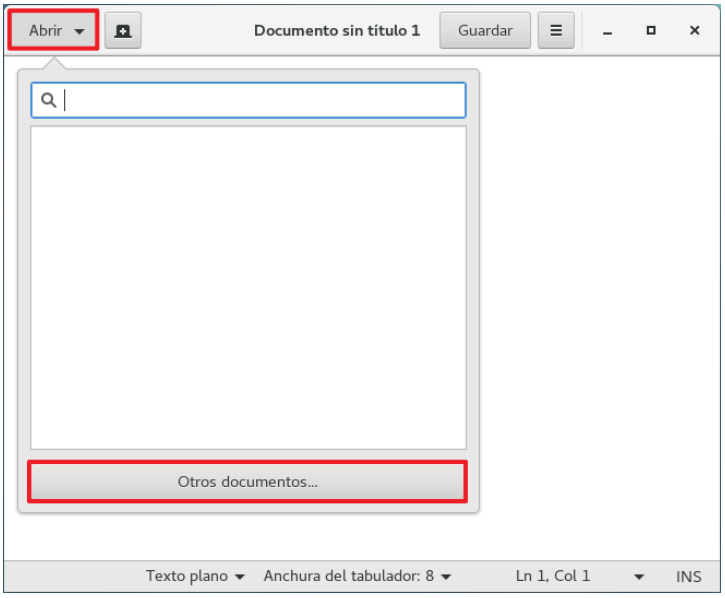
Postfix 2.10.1-6.el17.x86_64 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Postfix, en caso de necesitar información sobre los requisitos previos de instalación de Postfix visite el siguiente enlace.

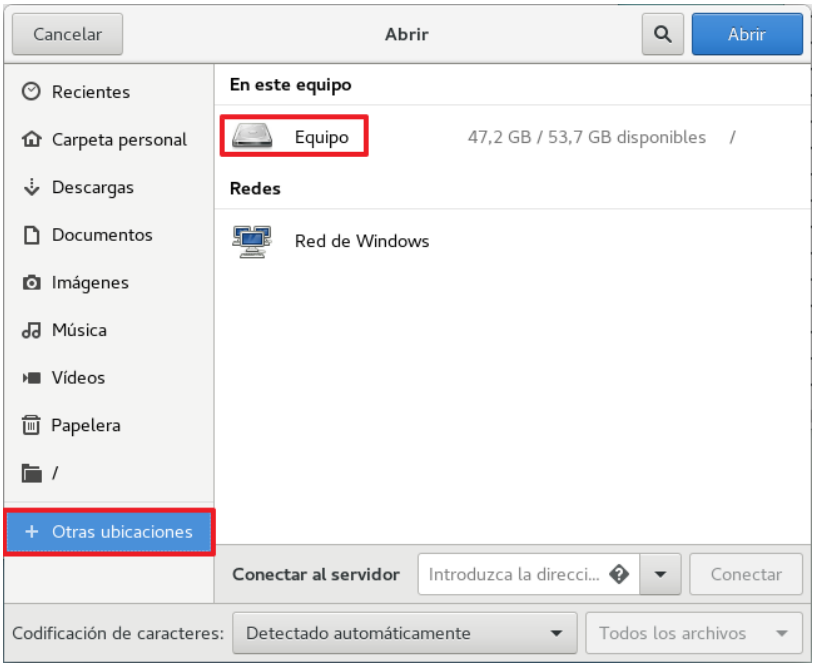
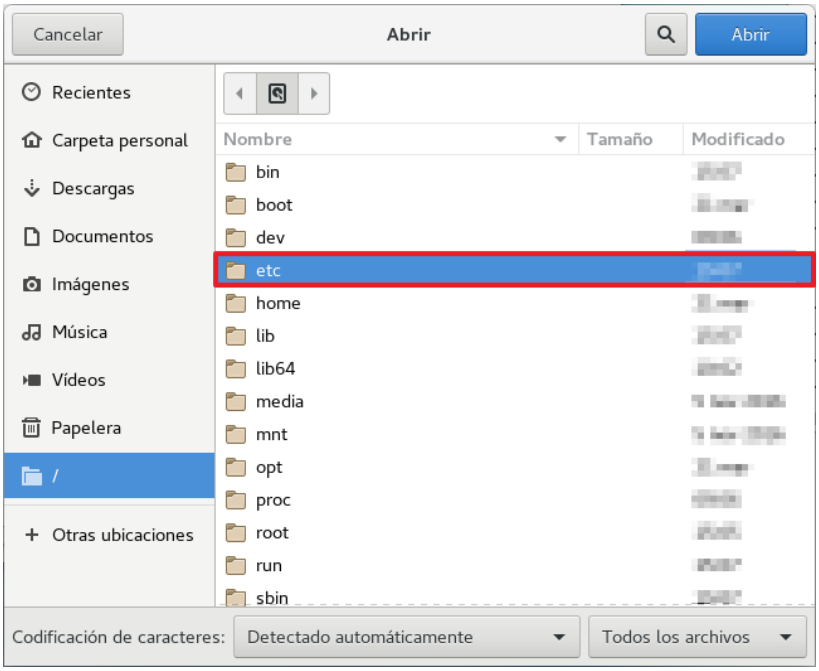
http://www.postfix.org/features.html#fs-requirements

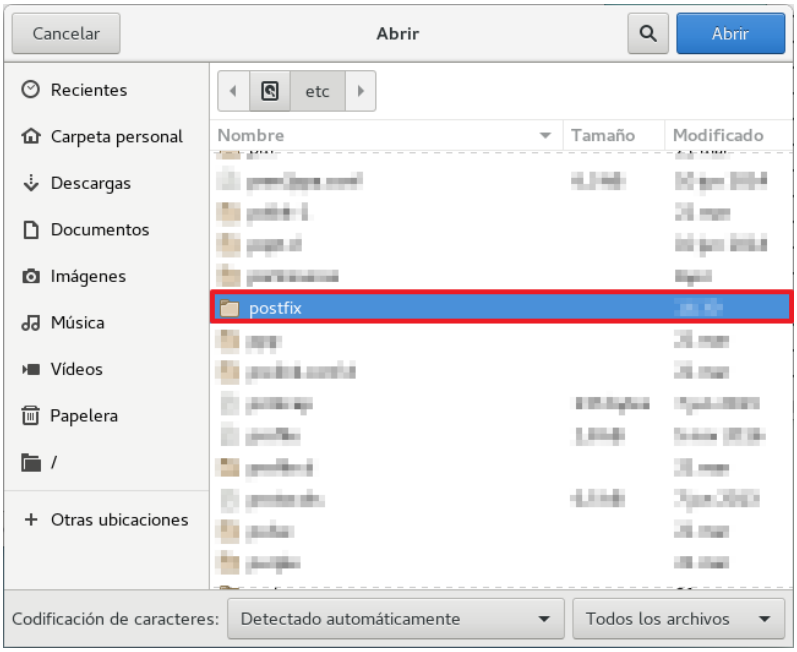
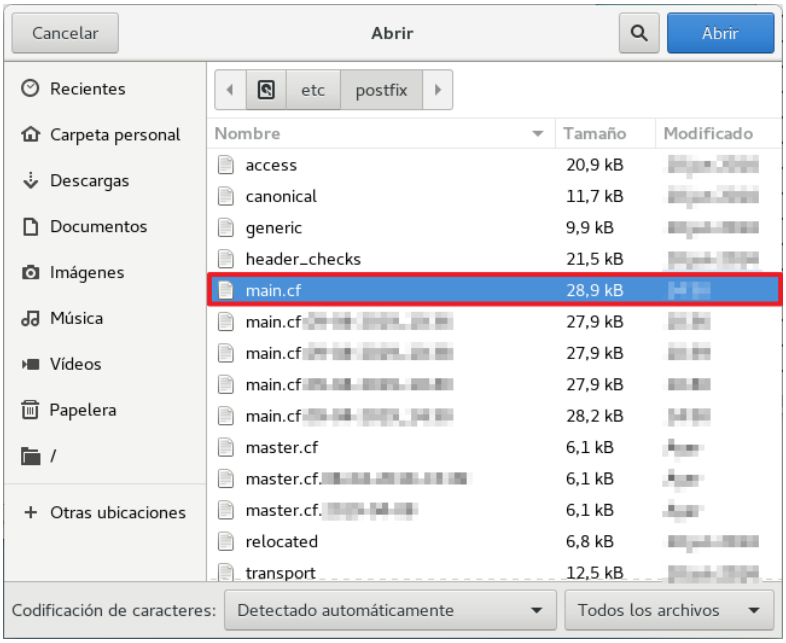
Nota: La instalación de Postfix se debe realizar en un volumen que debe haber sido formateado previamente con el formato XFS, formato que permite la aplicación de ACL's. Así mismo, antes de proceder a instalar las diferentes funcionalidades y complementos de Postfix, se debe haber reiniciado el servidor que se ha preparado hasta este momento, para garantizar que los servicios necesarios para Postfix están aplicados y en ejecución. La preparación del servidor debe haberse realizado de acuerdo con la implantación de la guía codificada como "CCN-STIC-619".
Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando.

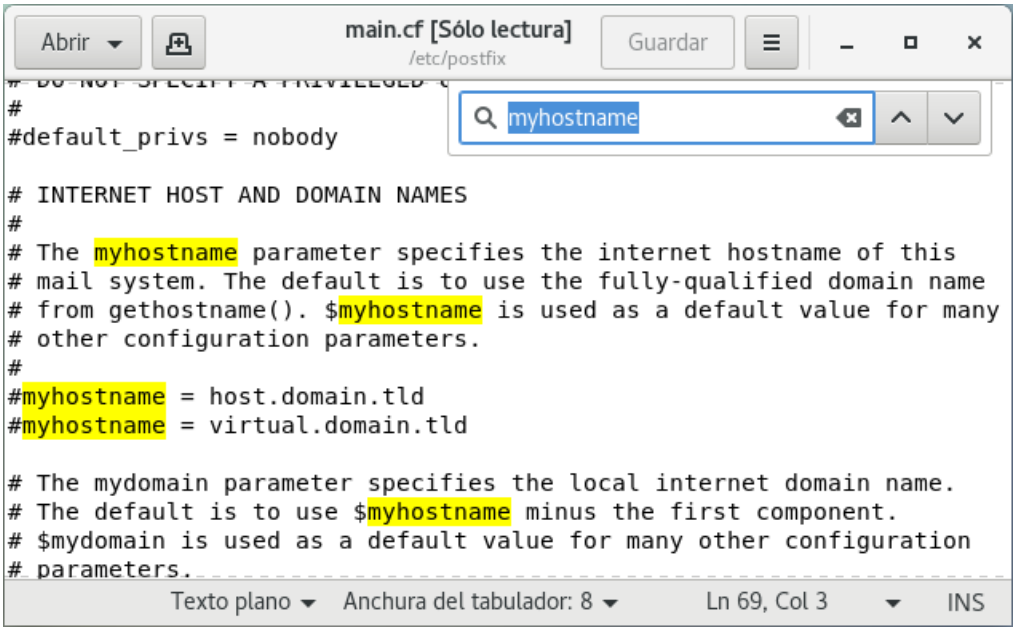
- **$ sudo setenforce 0**

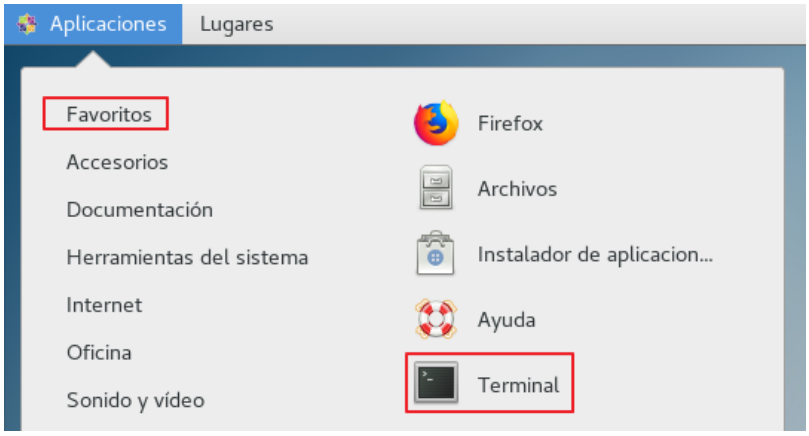
Deberá adaptar los parámetros de configuración de firewalld acorde a su organización. Tenga en cuenta que en esta guía se utilizan, a modo de ejemplo, varios puertos, que es necesario que estén abiertos para el correcto funcionamiento de los productos descritos.

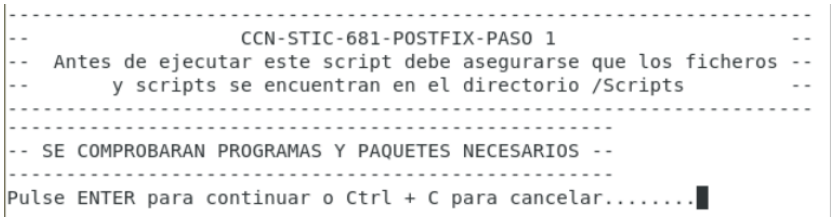
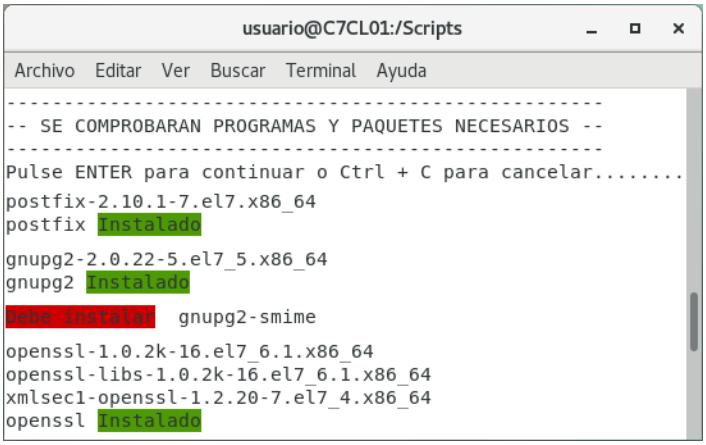
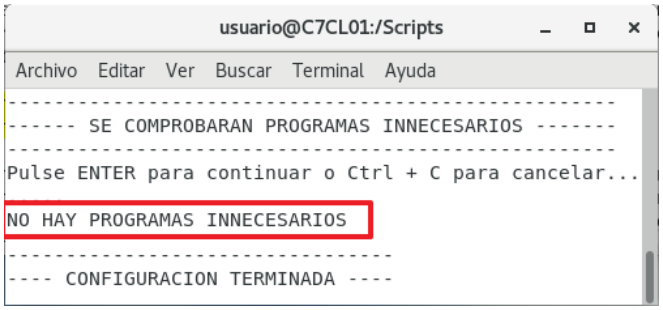
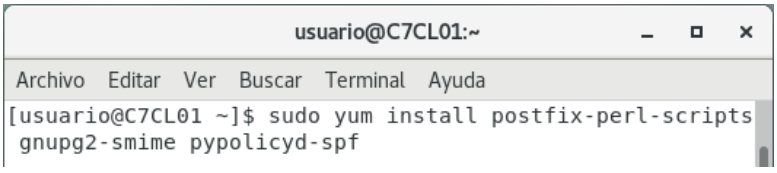
Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".
2.	Diríjase a la barra de tareas superior, pulse sobre "Aplicaciones" y en el apartado "Accesorios" seleccione "Editor de textos". 
3.	Diríjase a la esquina superior izquierda del editor de textos y pulse sobre "Abrir" y en "Otros documentos…". 

Paso	Descripción
4.	Deberá pulsar sobre “+ Otras Ubicaciones” y posteriormente sobre “Equipo”. 
5.	Ingrese a la carpeta “etc”. 

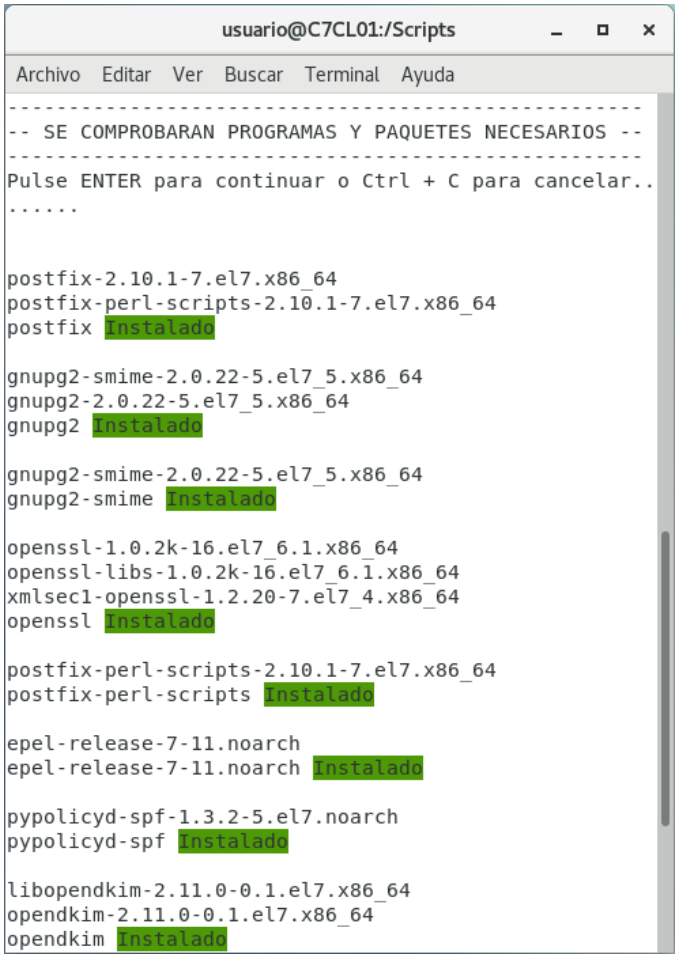
Paso	Descripción
6.	Ingrese en la carpeta “postfix”. 
7.	Ejecute el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón. 

Paso	Descripción
8.	A continuación, se muestran los parámetros a modificar. Estos parámetros responden a una configuración de tipo “parámetro=valor”, utilizando el símbolo “dólar” ($) para exportarlo globalmente en todo el fichero. – **Myhostname** = Nombre del servidor MTA Postfix. – **Mydomain** = Nombre del dominio de la organización. – **Inet_interfaces** = Interfaz de red por donde Postfix debe recibir mensajes. – **Smtpd_banner** = Mensaje deseado. – **Relayhost** = Servidor de correo al que se redireccionan los mensajes electrónicos procesados por Postfix. **Nota:** Estos parámetros se modificarán según las necesidades de cada organización.
9.	Por ser un archivo de configuración muy extenso, se recomienda pulsar “CTRL + f” y buscar el término deseado. 
10.	Una vez definidos los parámetros indicados, pulse “**Guardar**” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 

Paso	Descripción
11.	Diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Favoritos” seleccione “Terminal”. 
12.	Cree la carpeta “**Scripts**”. Para ello, en el terminal, ejecute el comando siguiente. **$ cd /** Para crear la carpeta en la ubicación ejecute el siguiente comando. **$ sudo mkdir Scripts** **Nota:** Puede comprobar que la carpeta ha sido creada ejecutando **ls /**.
13.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía CCN-STIC-681- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE CENTOS 7 LINUX. Introduzca las credenciales si se lo solicita.
14.	Copie el contenido de la carpeta con la categoría de seguridad “CATEGORIA_ALTA” correspondiente al directorio “Scripts/ENS_ALTA” asociado a esta guía en la ruta “**/Scripts**”. Pare ello, ejecute el comando siguiente. **$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_ALTA/* /Scripts/** **Nota:** Se considera que los scripts están disponibles en un disco óptico que es sistema reconoce como ISO Label, en caso contrario adapte la ruta al medio de almacenamiento escogido. Los scripts asumen que su ubicación en el sistema será bajo “/Scripts”. Si se desea modificar la ubicación deberá editar los scripts para reflejar la nueva ubicación.
15.	Expulse el CD/DVD de la unidad y diríjase a la carpeta ¨Scripts¨. Para ello ejecute el comando siguiente. **$ cd /Scripts**
16.	Ejecute el siguiente comando. Introduzca la contraseña del usuario para continuar. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso1_comprobacion_paquetes_necesarios.sh** **Nota:** Los scripts están confeccionados para las versiones correspondientes de los paquetes que se describen en esta guía. Si se dispone de versiones más actualizadas, se deberán modificar los scripts con las nuevas versiones.

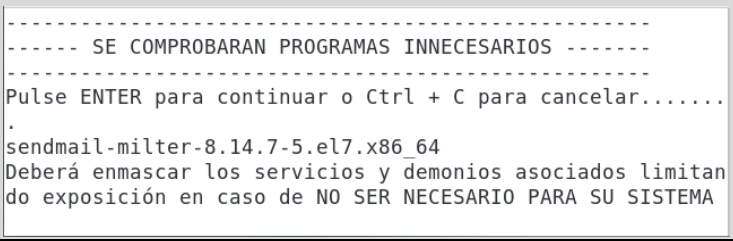
Paso	Descripción
17.	Pulse “ENTER” para continuar. 
18.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar.  **Nota:** Los resultados mostrados en pantalla pueden variar dependiendo de las configuraciones específicas de su organización.
19.	Como último paso comprobará si hay algún programa incompatible con la ejecución de postfix. Deberá mostrar el mensaje “NO HAY PROGRAMAS INNECESARIOS”. El script finalizará con el mensaje “CONFIGURACIÓN TERMINADA”. 
20.	Instale, actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. **$ sudo yum install <Paquete1 Paquete2 Paquete 3 …>** **$ sudo yum update <Paquete1 Paquete2 Paquete 3 …>** 

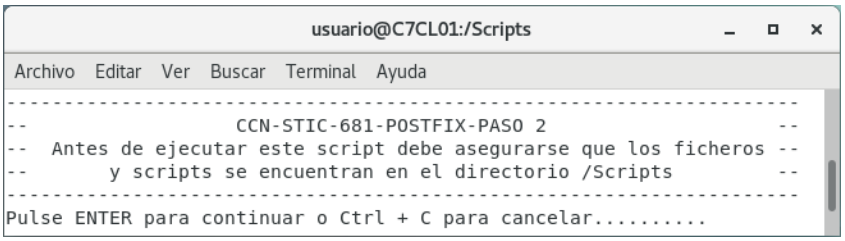
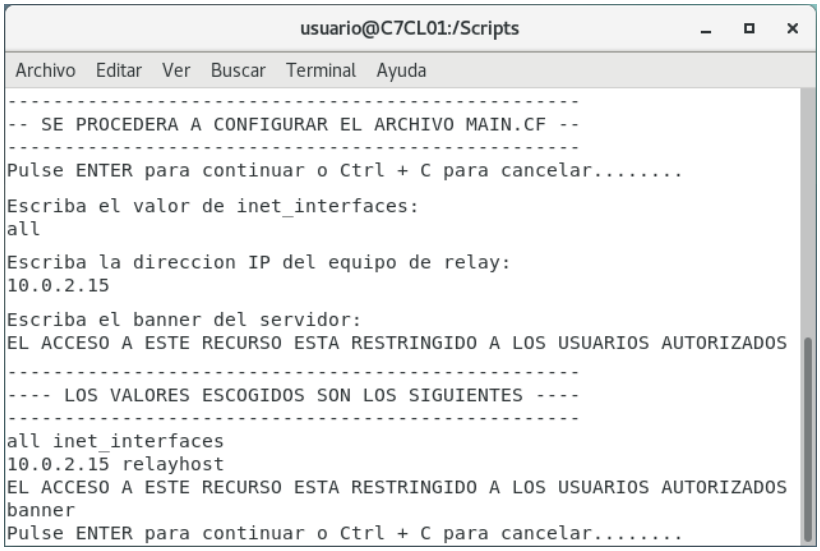
Paso	Descripción
21.	Ejecute el script de nuevo para comprobar que la configuración es correcta. **$ sudo sh CCN-STIC-681_ENS_MEDIA_Paso1_comprobacion_paquetes_necesarios.sh**



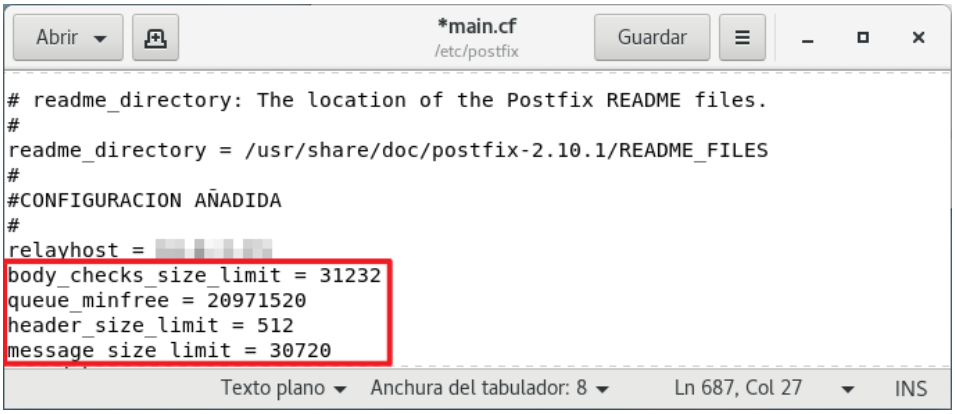
Nota: Si en el paso anterior ha instalado la herramienta **OpenDkim**, al volver a ejecutar el script le mostrará el error de la siguiente imagen. Esto es debido a la instalación por defecto de la herramienta OpenDkim, el sistema agrega librerías y dependencias de **sendmail** que si no se están utilizando son innecesarias junto con postfix.
Deberá en ese caso enmascarar servicios y demonios de sendmail evitando posibles incompatibilidades con la configuración de postfix y reduciendo el área de exposición.
Si se encuentra en esta situación ejecute el siguiente comando.

- **$ sudo systemctl mask sendmail**

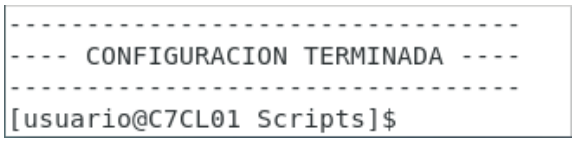
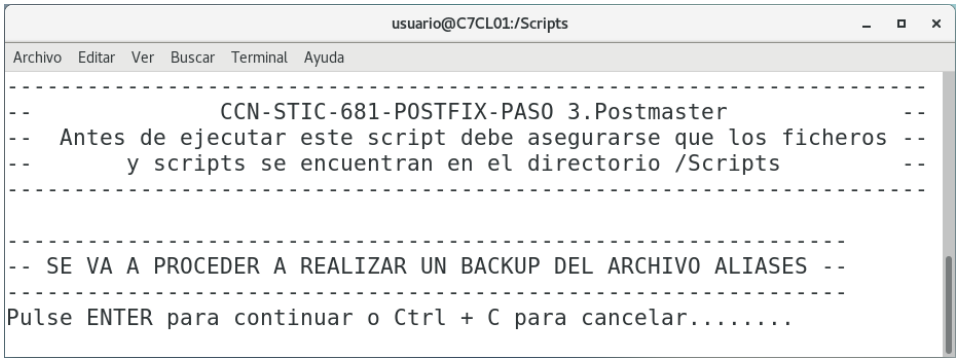


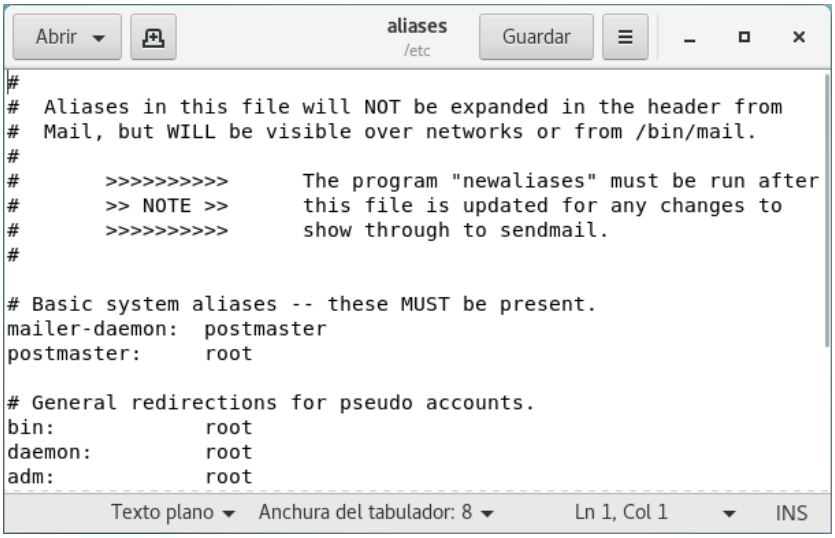
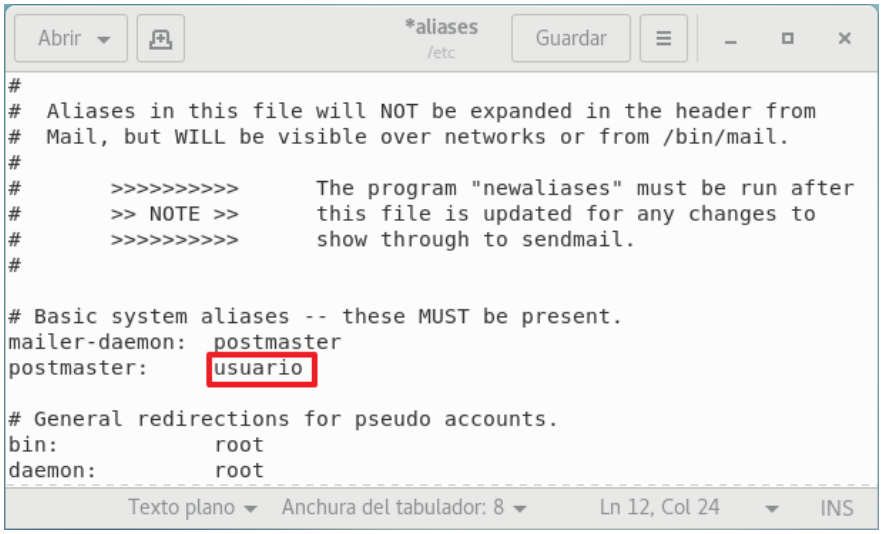
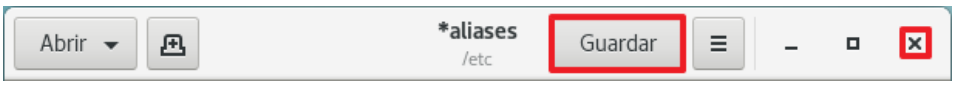
Paso	Descripción
22.	Por motivos de seguridad preservando los datos y configuraciones de su organización, se va a proceder a realizar una copia de seguridad de las configuraciones originales de todos los archivos de configuración susceptibles de ser cambiados por esta guía. Para dicho proceso, escriba los siguientes comandos. **$ sudo mkdir /home/usuario/BACKUP/** **$ sudo cp -f /etc/aliases /home/usuario/BACKUP/aliases_copia** **$ sudo cp -f /etc/postfix/main.cf /home/usuario/BACKUP/main.cf_copia** **$ sudo cp -f /etc/postfix/master.cf /home/usuario/BACKUP/master.cf_copia** **Nota:** Debe elegir una ruta o medio extraíble donde ubicar dichas configuraciones para una posible restauración a un punto anterior. La ubicación "/home/BACKUP/" es la ubicación elegida por esta guía a modo de ejemplo. Adapte la configuración según requisitos específicos de su organización.
23.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso2_configuracion_main.cf.sh**
24.	Para continuar con la ejecución del script, pulse "ENTER". 
25.	Para configurar el fichero "main.cf" pulse "Enter". Introduzca los parámetros relativos a las interfaces de red y pulse "Enter" cuando finalice de configurar los parámetros.  **Nota:** Tras introducir cada parámetro, deberá pulsar "ENTER" de nuevo para que quede registrado en el fichero. Tenga en cuenta que un parámetro en blanco también puede ser una configuración correcta. Deberá adaptar la configuración a los parámetros de su organización.

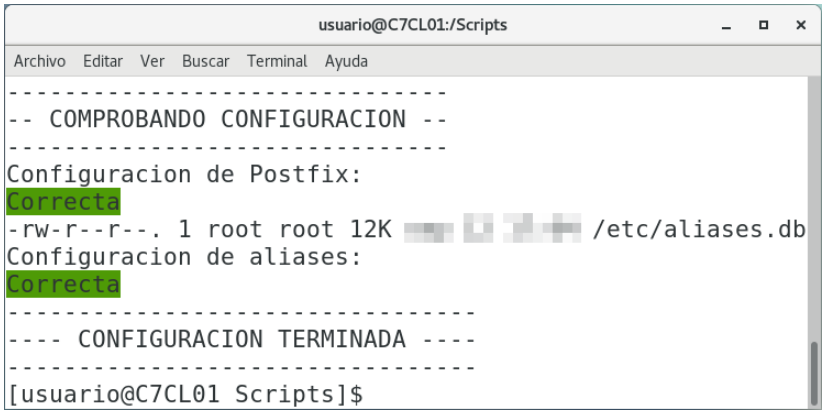
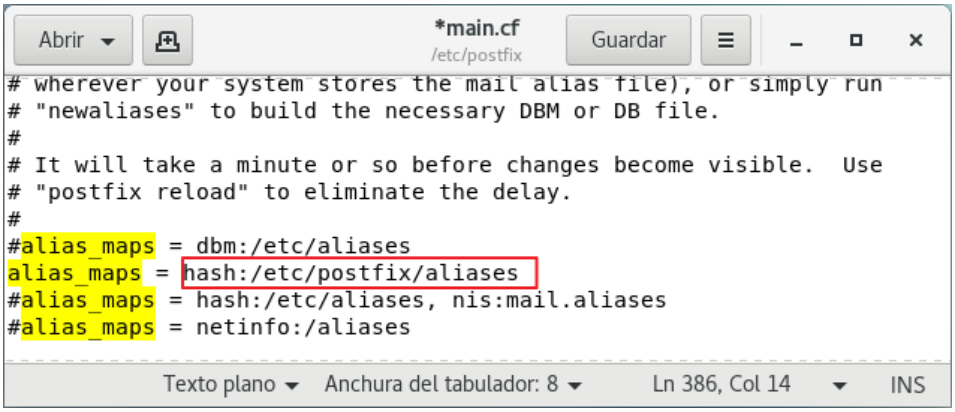
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>26.</td><td>Seguidamente se visualizan los parámetros seleccionados. Si por error se inserta un parámetro no deseado, pulse la combinación de teclas “Ctrl + c” y vuelva a ejecutar el script. Si la inserción ha sido correcta, pulse “ENTER” para continuar.
<pre>

---- LOS VALORES ESCOGIDOS SON LOS SIGUIENTES ----
----
all inet_interfaces
10.0.2.15 relayhost
EL ACCESO A ESTE RECURSO ESTA RESTRINGIDO A LOS USUARIOS AUTORIZADOS
banner
Pulse ENTER para continuar o Ctrl + C para cancelar........
</pre></td></tr>
<tr><td>27.</td><td>El script editará el fichero de configuración, deberá insertar en el archivo los valores correspondientes al tamaño de mensajes, el mínimo de memoria para la correcta función de Postfix, el tamaño de cabecera de los correos electrónicos y el tamaño del cuerpo de los mensajes.
A continuación, se muestran los valores recomendados para cada opción.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>body_checks_size_limit =</td><td>31232</td></tr>
<tr><td>queue_minfree =</td><td>20971520</td></tr>
<tr><td>header_size_limit =</td><td>512</td></tr>
<tr><td>message_size_limit =</td><td>30720</td></tr>
</table>
Nota: Deberá adaptar los valores a los requeridos por su organización.


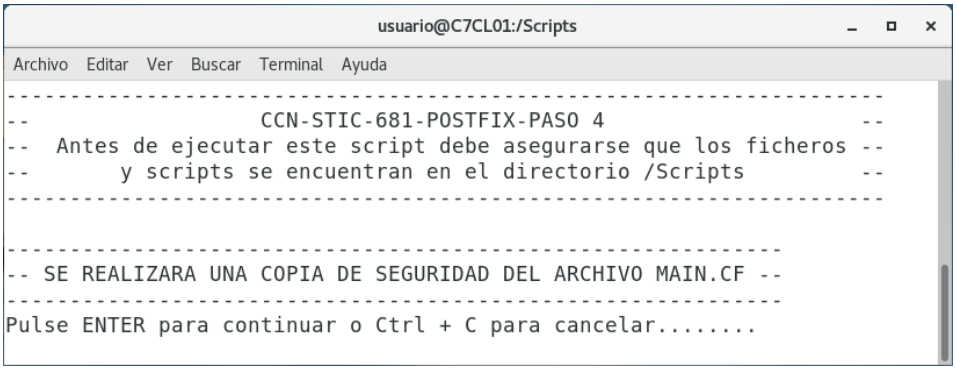
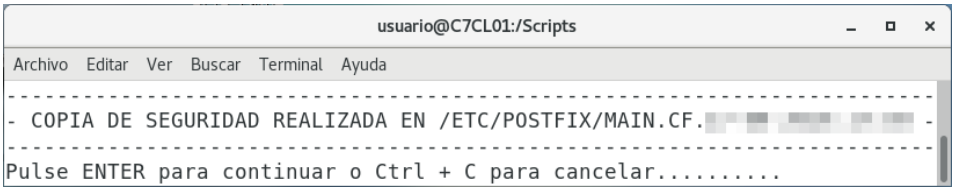
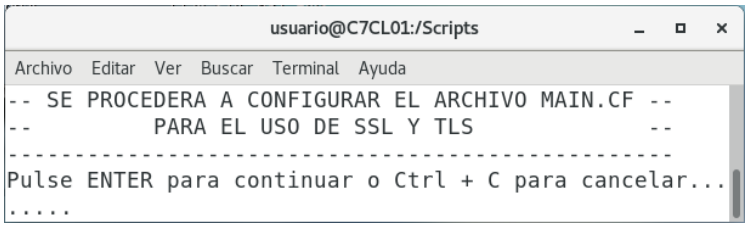
Nota: Tenga en cuenta que el fichero de configuración de la imagen se ha modificado del original para clarificar los parámetros que se deben modificar. Es posible que en su caso pueda tener varias líneas comentadas (#) intermedias.
Además, deberá añadir la siguiente información en el fichero.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>Mydomain =</td><td><Su dominio></td></tr>
<tr><td>Myhostname =</td><td><El nombre del servidor></td></tr>
<tr><td>Myorigin =</td><td><Su dominio></td></tr>
</table></td></tr>
</table>

Paso	Descripción
28.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
29.	La configuración termina con la salida del proceso de configuración y el mensaje de finalización del mismo. 
30.	Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso3_Postmaster.sh** 
31.	Se le comunicará la correcta realización de la copia de seguridad. 

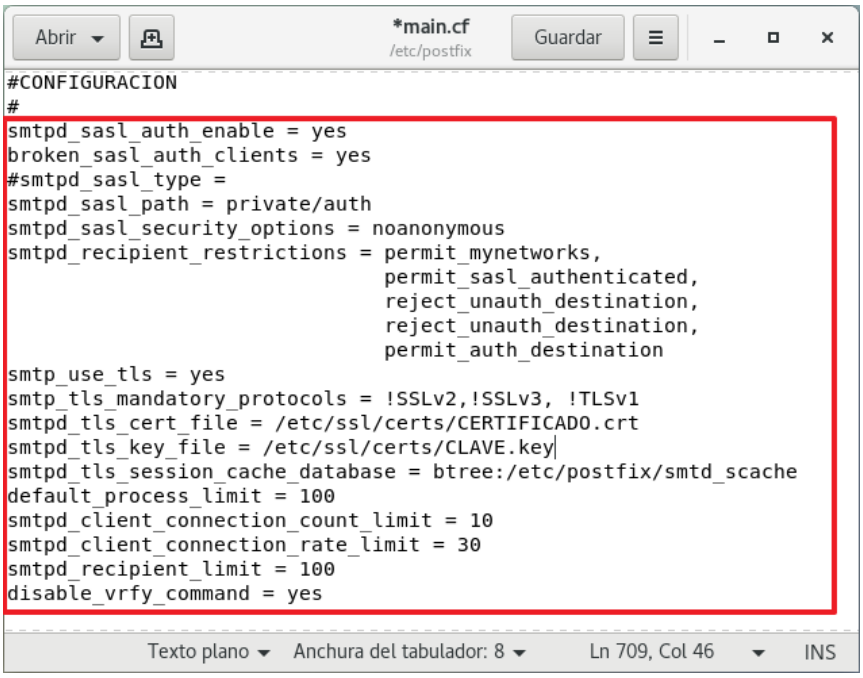
Paso	Descripción
32.	Seguidamente se abrirá una ventana editando el fichero /etc/aliases. 
33.	Por defecto la figura de “Postmaster” recae en el usuario “root”, Deberá asignar dicha figura a un usuario administrador. Modifique el documento con los parámetros requeridos.  **Nota:** En el ejemplo se le han entregado dichos privilegios al usuario “usuario”.
34.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 

Paso	Descripción
35.	El script comprobará el fichero y los permisos de /etc/aliases y finalizará con el mensaje “CONFIGURACIÓN TERMINADA”.  **Nota:** Si hubiera alguna discrepancia, restaure el archivo de copia de seguridad y ejecute de nuevo el script siguiendo los pasos de configuración.
36.	Deberá editar el archivo de configuración main.cf de Postfix, para que el servidor postfix pueda detectar la nueva configuración. Introduzca la contraseña si se le solicita. **$ sudo gnome-text-editor /etc/postfix/main.cf &>/dev/null** **Parámetro** / **Valor**: alias_maps = / hash:/etc/postfix/aliases 
37.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
38.	Para actualizar la tabla de alias de CentOS 7 Linux, ejecute el siguiente comando. Si ejecuta sin errores, no mostrará resultado por pantalla. **$ sudo newaliases**

Paso	Descripción
39.	Para una correcta segregación de roles y permisos, deberá designar la monitorización de los logs y actividades de correo a un grupo específico designado por la organización. Además, deberá otorgar permisos al directorio de log de CentOS 7 Linux (/var/log/maillog). Se muestran comandos de ejemplo para realizar estas tareas. Siendo, sin comillas, "monitorización" el grupo designado para tales tareas de mantenimiento, añadiendo al grupo el usuario o usuarios designados para dichas funciones. **$ sudo groupadd "monitorización"** **$ sudo chgrp –R "monitorización" /var/log/maillog** **$ sudo usermod –a –G "monitorización" "usuarios designados"** **Nota:** Los comandos anteriores nombran en modo de ejemplo y entre comillas ("") a los usuarios y grupos. Para adaptar esta configuración a las necesidades de su organización, tendrá que escribir los usuarios y grupos sin comillas ("") para la correcta aplicación del comando.
40.	La modificación de permisos sobre la carpeta de logs de los correos electrónicos se realiza desde la línea de comandos, otorgando los permisos de escritura y lectura al usuario y al grupo designados. El usuario del sistema "root" será el poseedor de la carpeta para el correcto funcionamiento del sistema y poseerá los permisos equivalentes a "660". **$ sudo chmod -660 /var/log/maillog**
41.	Se va a proceder a realizar una configuración, en modo de ejemplo, del archivo de configuración /etc/postfix/main.cf, para Postfix. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**
42.	Debido a la categorización del presente anexo (**alta-DL**), se asume para la realización de los siguientes pasos el uso de certificados emitidos por entidades certificadoras autorizadas. Inserte en el sistema los certificados permitidos por medio de un dispositivo de almacenamiento autorizado y guárdelos en ruta predeterminada por su organización.
43.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso4_Seguridad.sh** **Nota:** A modo de ejemplo la guía, hará referencia al almacén de los certificados en la siguiente ruta "/etc/ssl/certs/", si por necesidades de la organización quisiera modificar la misma, deberá adaptar los ficheros de configuración, así como los scripts a la nueva ruta.

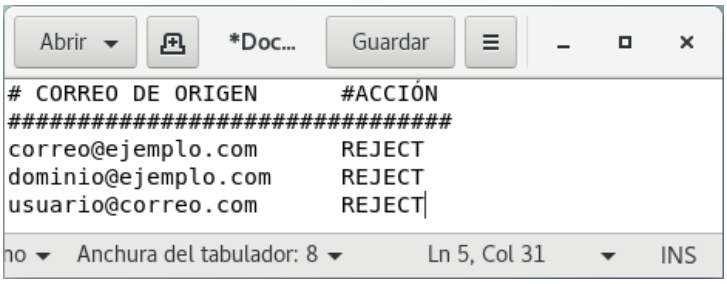
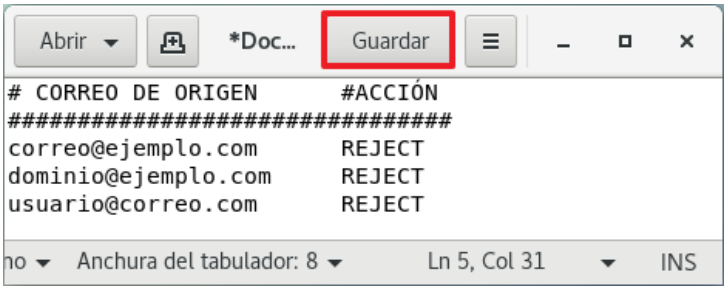
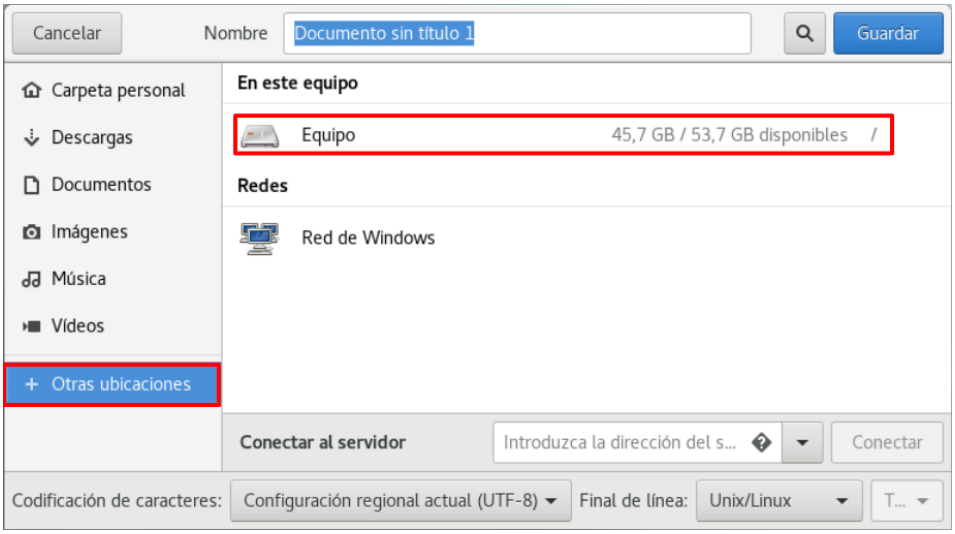
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>44.</td><td>El script iniciará realizando de una copia de seguridad del archivo a configurar, “/etc/postfix/main.cf”. Para continuar pulse la tecla “ENTER”.
 
</td></tr>
<tr><td>45.</td><td>Se confirma la realización de la copia de seguridad. Deberá pulsar la tecla “ENTER” para continuar.
 
</td></tr>
<tr><td>46.</td><td>Posteriormente se procederá a editar el archivo main.cf para el uso de ssl y tls. Pulse “ENTER” para continuar.
 
</td></tr>
<tr><td>47.</td><td>El script habrá agregado las líneas necesarias al final del documento, introduzca los siguientes valores para los parámetros añadidos.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>smtpd_sasl_auth_enable =</td><td>yes</td></tr>
<tr><td>broken_sasl_auth_clients =</td><td>yes</td></tr>
<tr><td>#smtpd_sasl_type =</td><td></td></tr>
<tr><td>smtpd_sasl_path =</td><td>private/auth</td></tr>
<tr><td>smtpd_sasl_security_options =</td><td>noanonymous</td></tr>
<tr><td>smtpd_recipient_restrictions =</td><td>permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_destination,
reject_unauth_destination,
permit_auth_destination</td></tr>
<tr><td>smtp_use_tls =</td><td>yes</td></tr>
<tr><td>smtp_tls_mandatory_protocols =</td><td>!SSLv2,!SSLv3, !TLSv1</td></tr>
</table></td></tr>
</table>

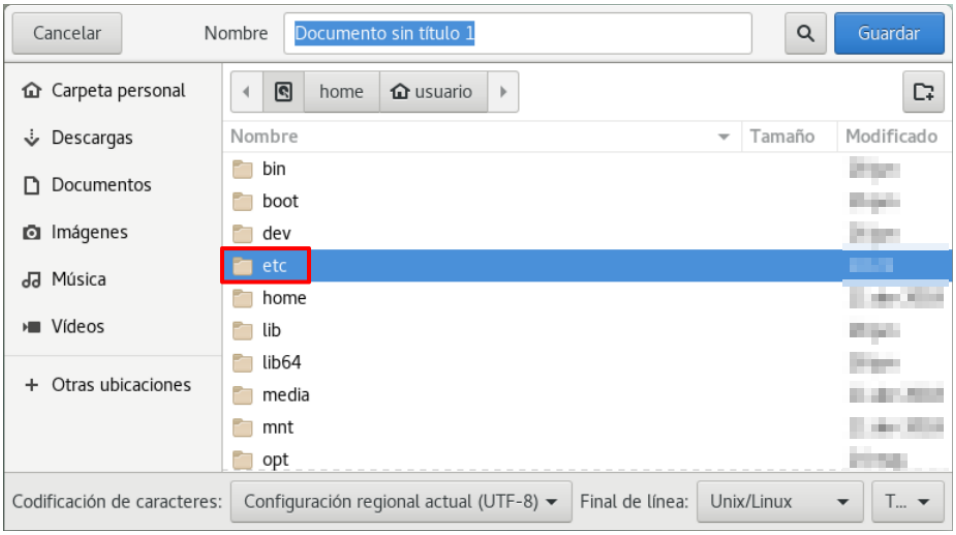
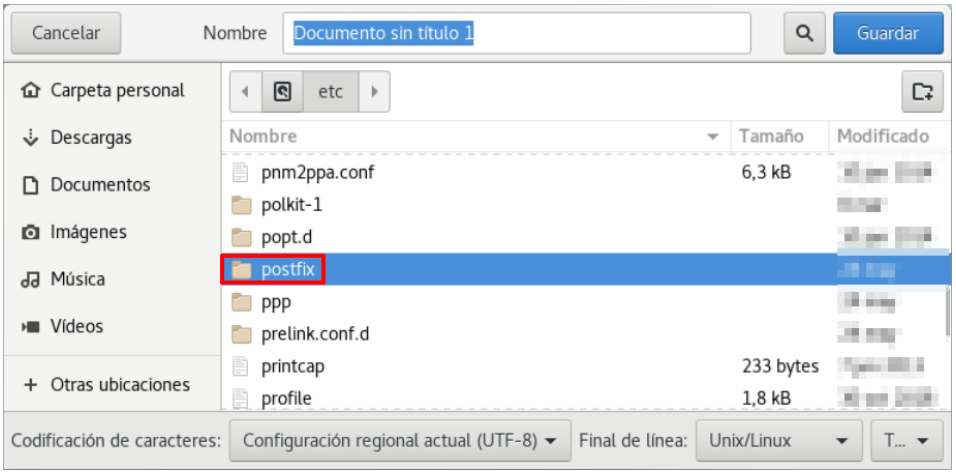
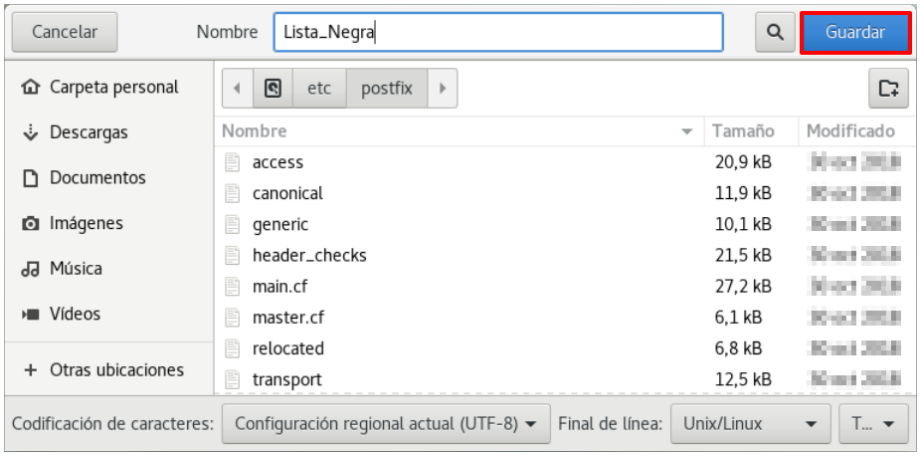
Paso	Descripción	
	Parámetro	**Valor**
	smtpd_tls_cert_file =	/etc/ssl/certs/<certificado.extension> **Nota:** Adapte la ruta y el nombre del certificado a la definida por su organización.
	smtpd_tls_key_file =	/etc/ssl/certs/<clave.extension> **Nota:** Adapte la ruta y el nombre del certificado a la definida por su organización.
	smtpd_tls_session_cache_database =	btree:/etc/postfix/smtd_scache
	default_process_limit =	100
	smtpd_client_connection_count_limit =	10
	smtpd_client_connection_rate_limit =	30
	smtpd_recipient_limit =	100
	disable_vrfy_command =	yes

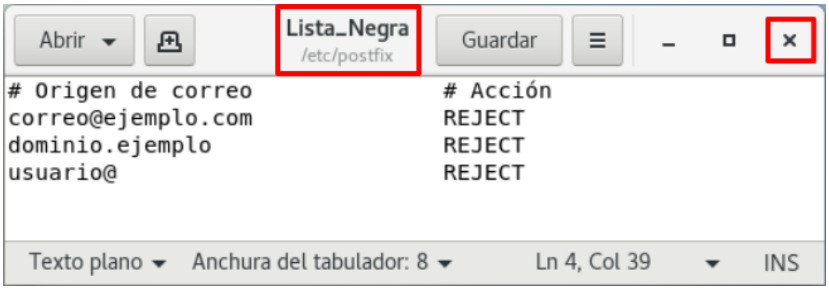
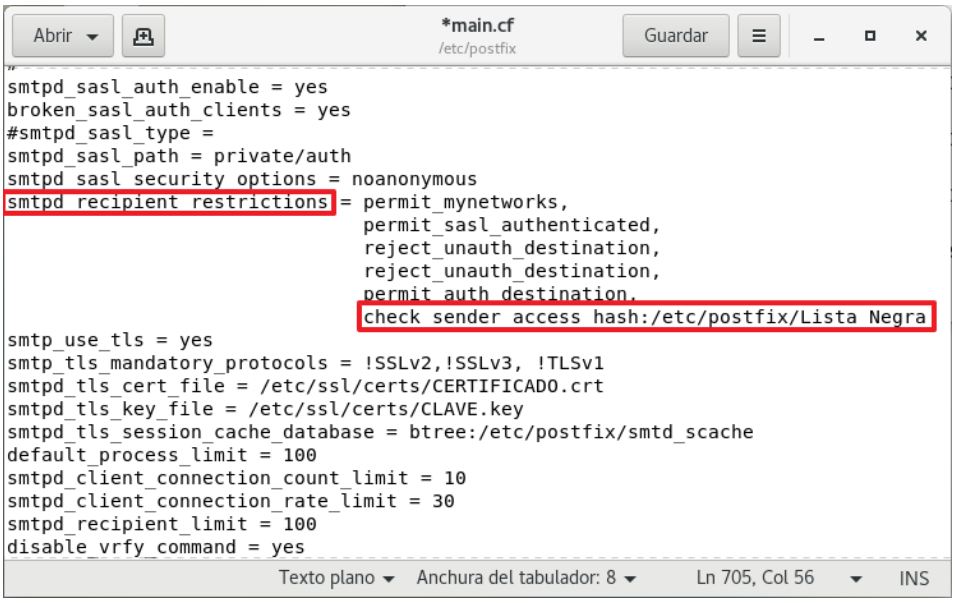


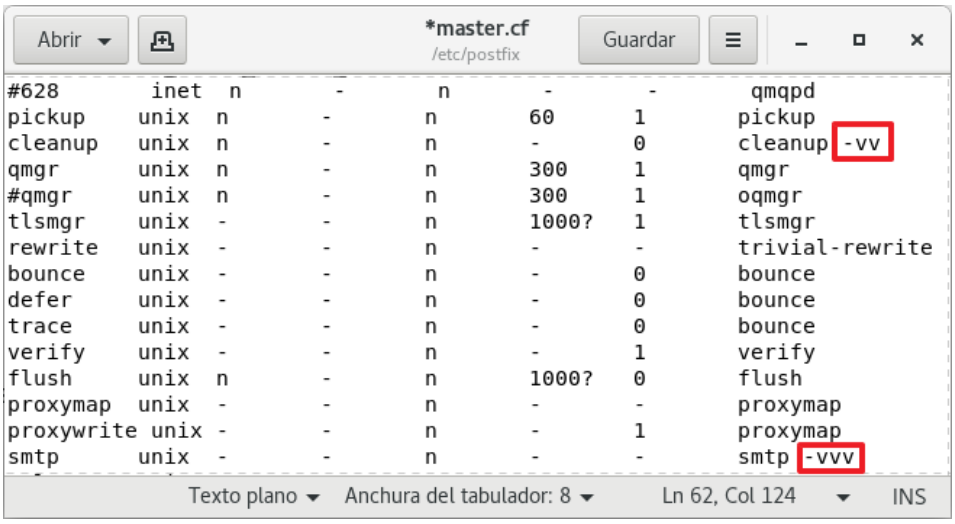
Nota: Si detecta un parámetro duplicado elimine el que se encuentra por encima en el documento. Debe tener en cuenta que en el fichero de configuración de Postfix un parámetro sin ningún valor se considera como un valor válido de configuración. Así mismo, deberá tener en consideración los valores establecidos en la tabla anterior y adaptarlos según necesidades de su organización.

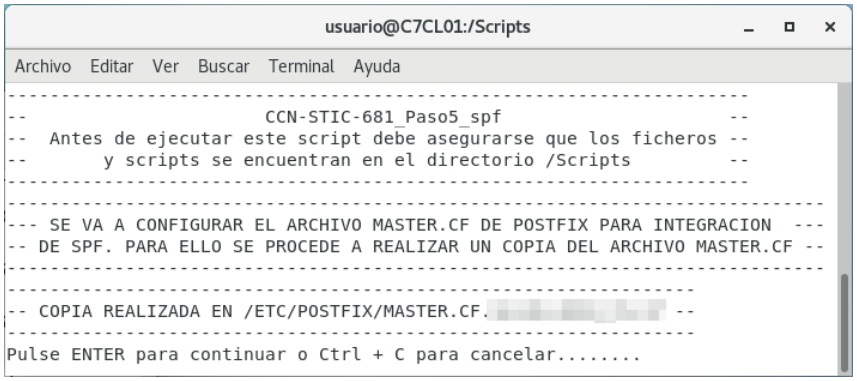
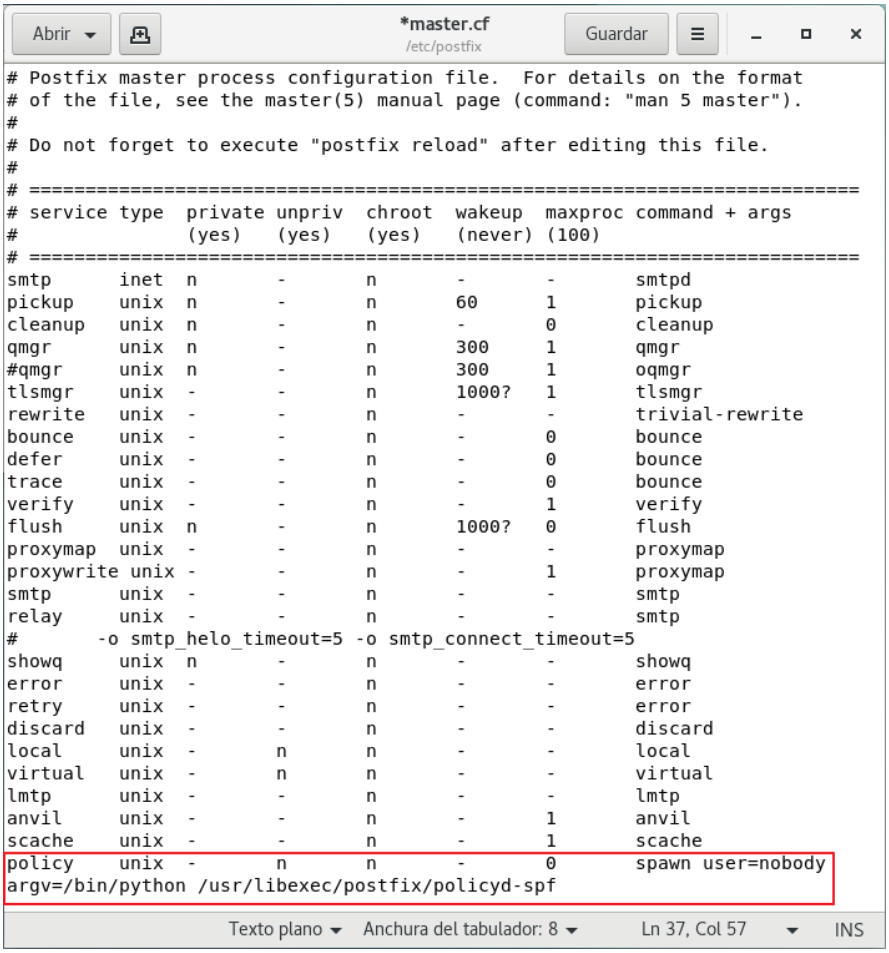
48. Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana.

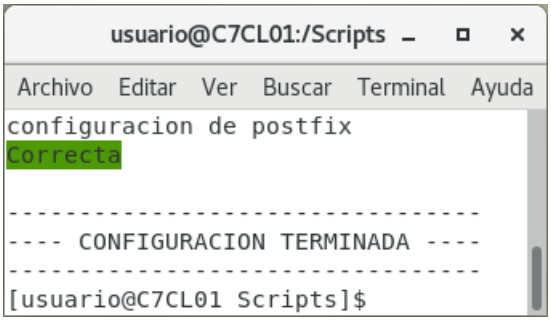
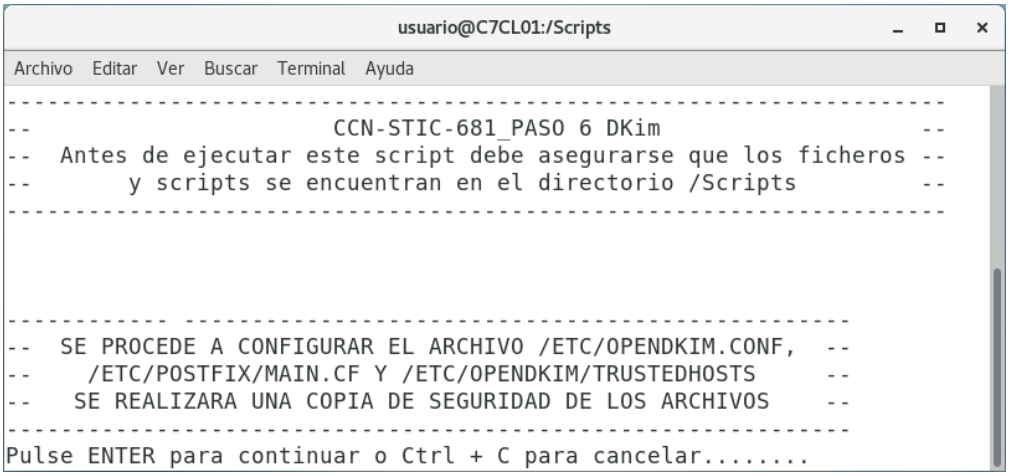
Paso	Descripción
49.	El proceso termina con el mensaje mostrado como en la siguiente imagen. ---------- ---- CONFIGURACION TERMINADA ---- ----------
50.	Se va a proceder a realizar una configuración para que se tenga en consideración una lista negra de spam. Para ello ejecute el siguiente comando para iniciar el editor de textos con un documento vacío. **$ sudo gnome-text-editor &>/dev/null**
51.	Deberá crear un documento con el listado de origen de correo electrónico a bloquear.  **Nota:** Adapte el documento con las necesidades específicas de su organización.
52.	Seguidamente, deberá guardar el documento. Para ello pulse en “Guardar”. 
53.	Pulse en “+ Otras ubicaciones” y a continuación en “Equipo”. 

Paso	Descripción
54.	Seleccione la carpeta “etc”. 
55.	Seleccione la carpeta “postfix”. 
56.	En el recuadro de “Nombre” escriba “Lista_Negra” y seguidamente pulse el botón “Guardar” para finalizar. 

Paso	Descripción
57.	Deberá cerrar el documento una vez guardado. Asegúrese de que la ruta de guardado es la correcta. 
58.	Deberá ejecutar el siguiente comando para convertir el fichero de texto creado en una base de datos legible por Postfix. Introduzca la contraseña si se le solicita. **$ sudo postmap hash:/etc/postfix/Lista_Negra**
59.	Para que postfix añada el fichero "Lista_Negra" como una regla interna suya, debe modificar el archivo "main.cf". Para ello edite el fichero de configuración ejecutando el siguiente comando. **$ sudo gnome-text-editor /etc/postfix/main.cf &>/dev/null**
60.	Añada la siguiente línea en el fichero de configuración de tal manera que se asemeje a la configuración de la siguiente imagen. **smtpd_recipient_restrictions = check_sender_access hash:/etc/postfix/Lista_Negra** 
61.	Pulse "Guardar" y cierre el Editor de textos pulsando la **"x"** situada en la zona superior derecha de la ventana. 

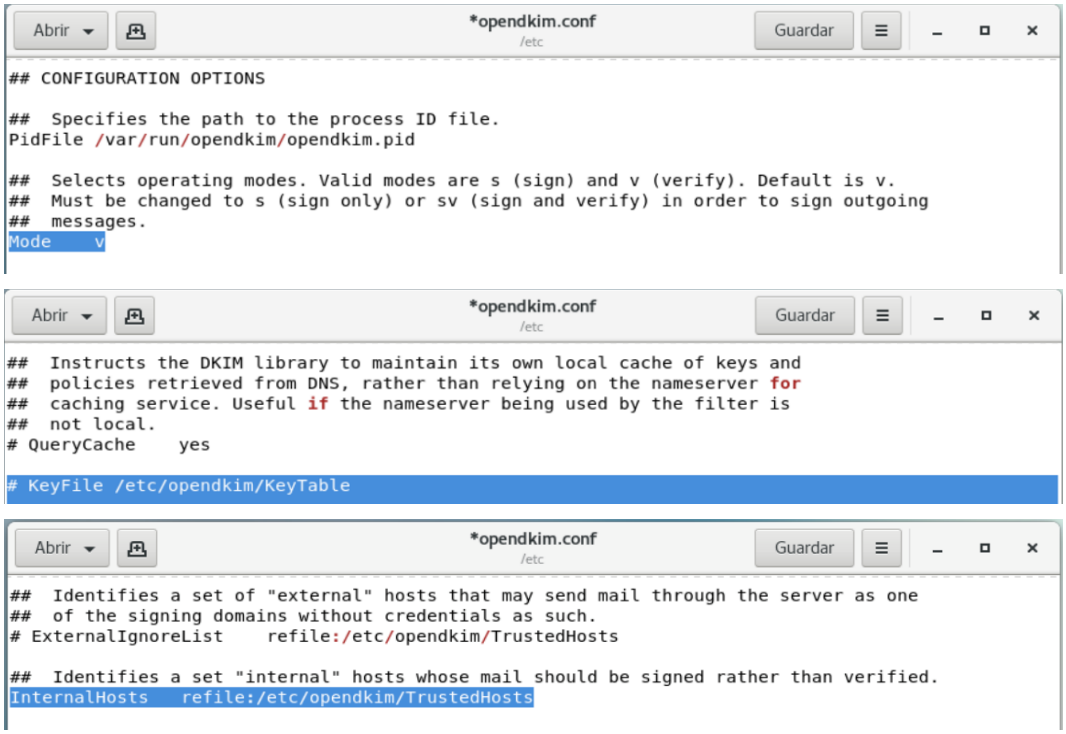
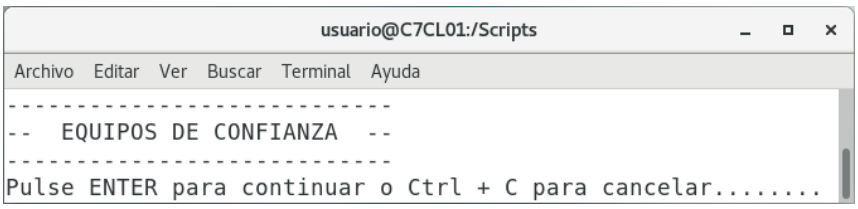
Paso	Descripción
62.	Posteriormente deberá modificar los registros del documento master.cf estableciendo un registro de actividad más elevado y detallado. Para tal fin, en una terminal, ejecute el siguiente comando. **$ sudo gnome-text-editor /etc/postfix/master.cf &>/dev/null**  **Nota:** Deberá identificar el demonio que tendrá mayor nivel de auditoría e insertar al final de la línea el valor mayor según necesidades de su organización. La visualización de la actividad de Postfix se ve reflejada en el archivo de log ubicado en /var/log/maillog. Para monitorizar la actividad de postfix ejecute el siguiente comando "**tail -f /var/log/maillog"**.
63.	Pulse "Guardar" y cierre el Editor de textos pulsando la **"x"** situada en la zona superior derecha de la ventana. 
64.	Se va a proceder a realizar una configuración básica del archivo de configuración /etc/postfix/master.cf de Postfix para la integración de SPF. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**
65.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso5_spf.sh** **Nota:** Para la integración en el servidor de la funcionalidad SPF, deberá de poseer anteriormente ciertas configuraciones específicas en un servidor DNS para que el complemento surta efecto. No es objetivo de esta guía la configuración de un servidor DNS para tal efecto.

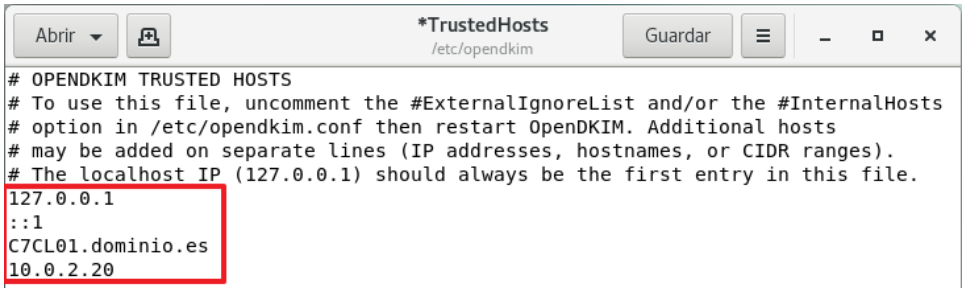
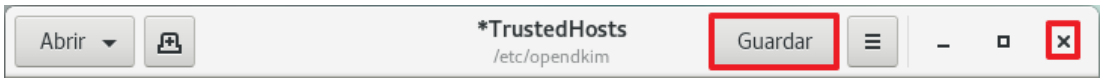
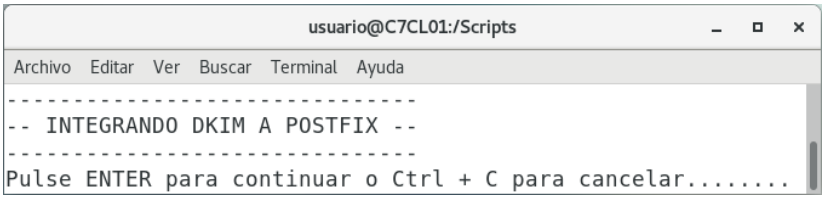
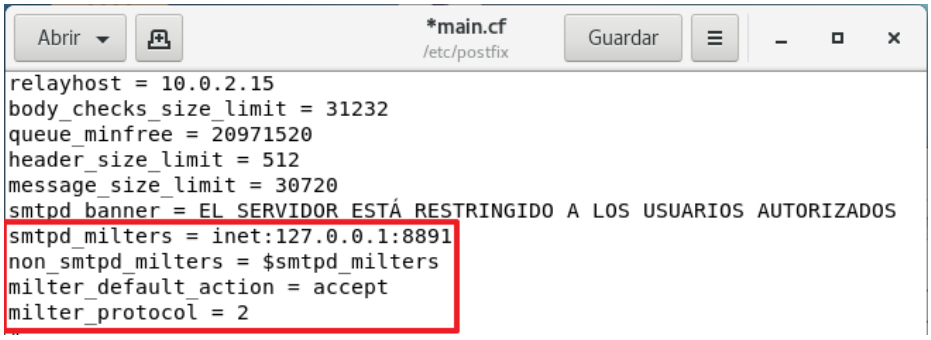
Paso	Descripción
66.	Para ello, primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar “ENTER” para continuar. 
67.	El script editará el fichero master.cf. Inserte la siguiente línea en master.cf para configurar SPF. **policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf**  **Nota:** Tenga en cuenta que el fichero de configuración de la imagen se ha modificado del original para clarificar los parámetros que se deben modificar. Es posible que en su caso pueda tener varias líneas comentadas (#) intermedias.

Paso	Descripción
68.	Pulse “Guardar” y cierre el Editor de textos pulsando la “**x**” situada en la zona superior derecha de la ventana. 
69.	El proceso finaliza con el siguiente mensaje, realizándose una comprobación de sintaxis de Postfix. 
70.	Ejecute el siguiente comando para continuar con la configuración. Ingrese la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso6_Dkim.sh** **Nota:** Para la integración completa en el servidor de la herramienta OpenDkim, deberá poseer anteriormente de ciertas configuraciones adicionales que permitan firmar por certificado los correos desde su origen. No es objetivo de esta guía el tratamiento de esta configuración adicional.
71.	En un primer paso, se realiza una copia de seguridad de los archivos a configurar. Deberá pulsar “ENTER” para continuar. 

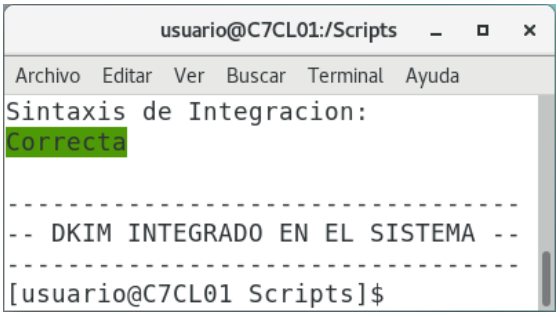
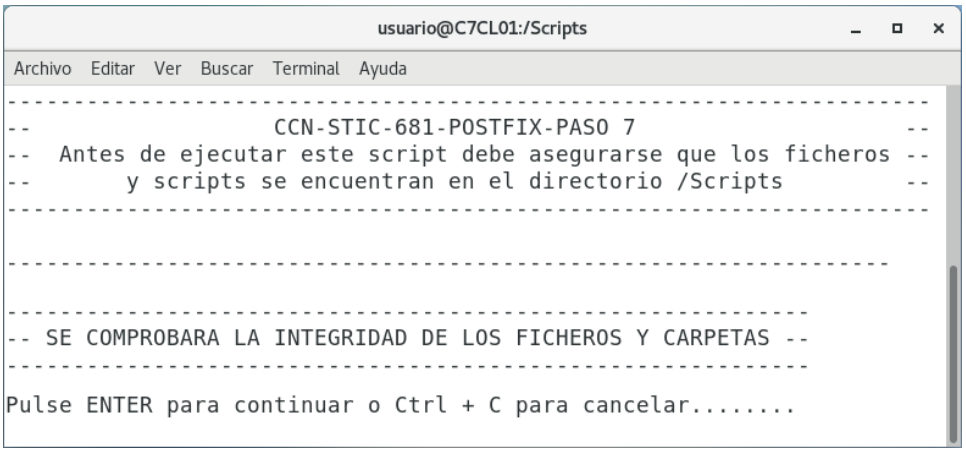
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>72.</td><td>Se muestra la configuración a modificar en opendkim.cf, los valores mostrados son los adecuados a la categoría de seguridad.

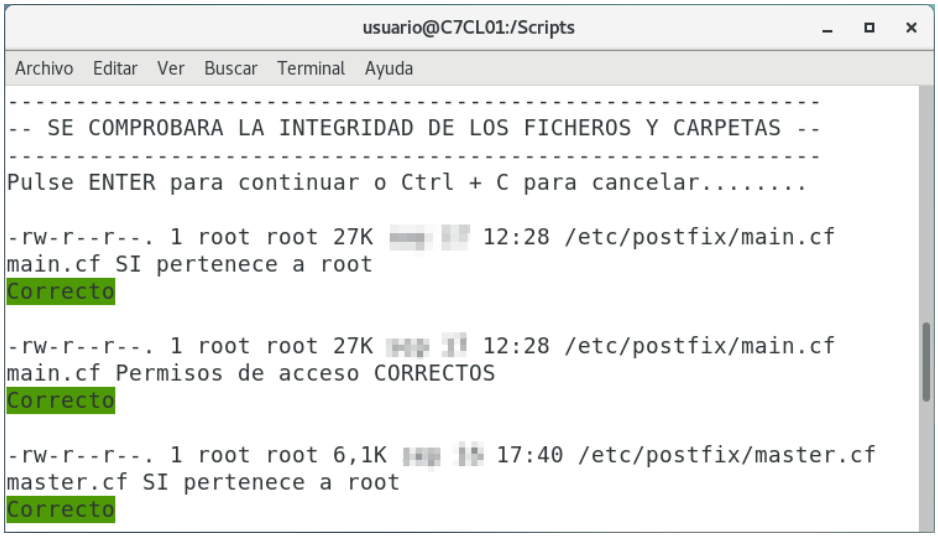
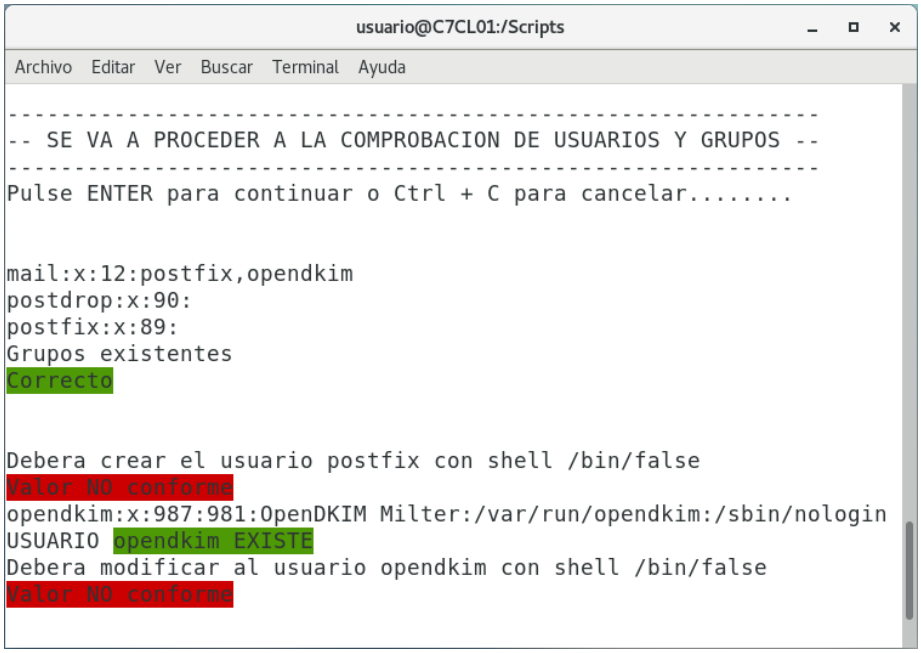
Nota: Deberá adaptar los parametros de la tabla a los que mas convengan en su organización. Si el valor de la columna izquierda existe, deberá modificarlo con lo indicado en la tabla, si no existe añadir el valor de la columna derecha.

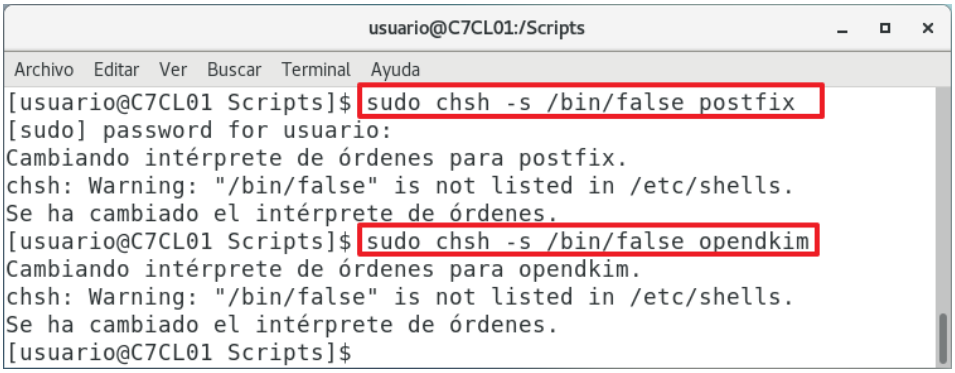
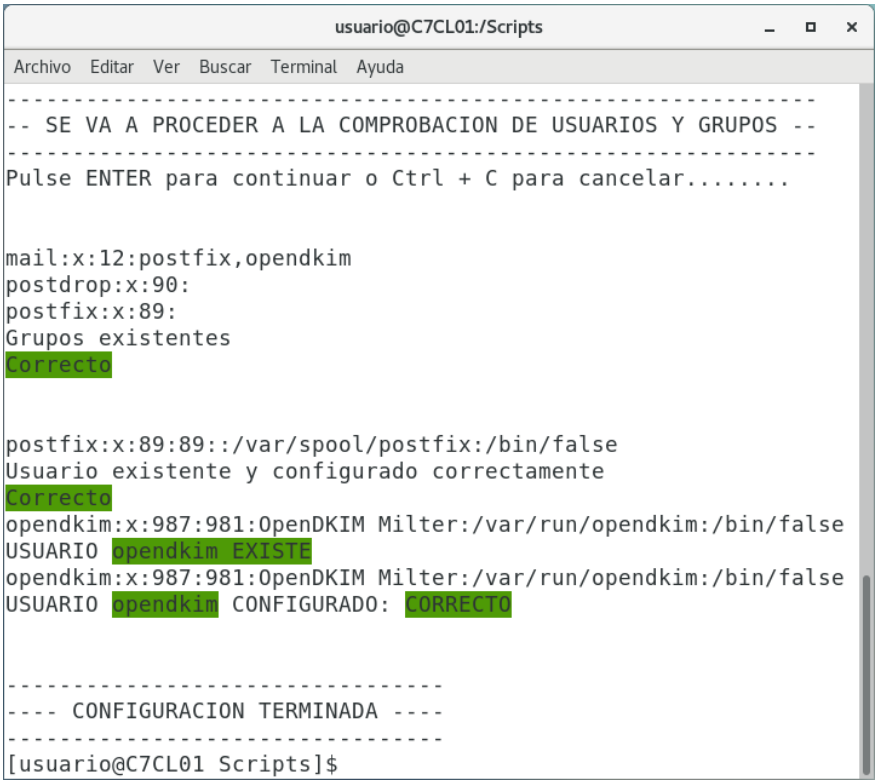
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>Mode <valor></td><td>Mode v</td></tr>
<tr><td>KeyFile /etc/opendkim/keys/default.private</td><td>#KeyFile/etc/opendkim/keys/default.private</td></tr>
<tr><td>KeyTable /etc/opendkim/KeyTable</td><td>#KeyTable /etc/opendkim/KeyTable</td></tr>
<tr><td>#InternalHosts refile:/etc/opendkim/TrustedHosts</td><td>InternalHosts refile:/etc/opendkim/TrustedHosts</td></tr>
</table>

</td></tr>
<tr><td>73.</td><td>Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.</td></tr>
<tr><td>74.</td><td>Se procede a añadir la excepción de equipos de confianza. Pulse “ENTER” para continuar.
 
</td></tr>
</table>

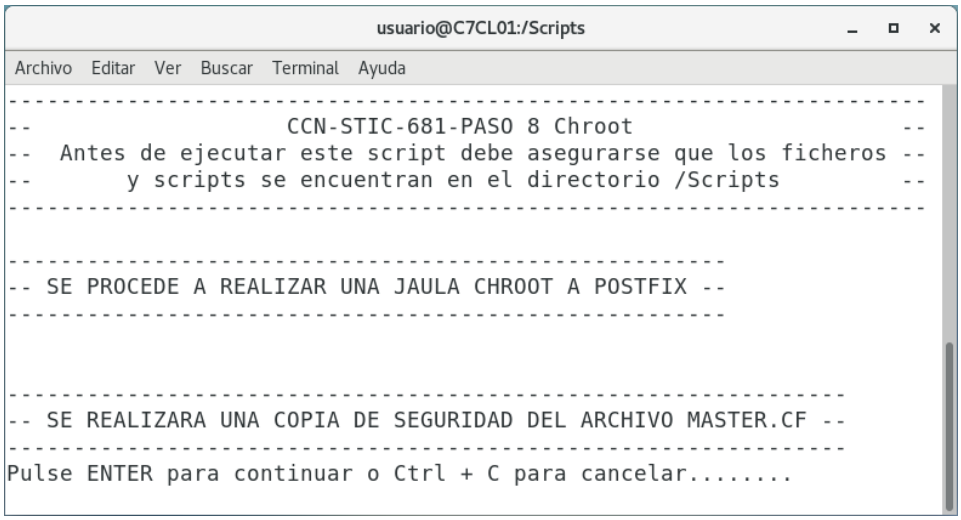
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>75.</td><td>A continuación, se muestra, a modo de ejemplo, una configuración del archivo /etc/opendkim/TrustedHosts.
 
</td></tr>
<tr><td>76.</td><td>Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.
 
</td></tr>
<tr><td>77.</td><td>Con la inserción de valores en el archivo /etc/postfix/main.cf se concluirá la integración de OpenDkim con Postfix. Pulse “ENTER” para continuar.
 
</td></tr>
<tr><td>78.</td><td>El script editará el fichero de configuración, inserte los parámetros de seguridad recomendados contenidos en la siguiente tabla y adáptelos a los específicos de su organización.
<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>smtpd_milters =</td><td>inet:127.0.0.1:8891</td></tr>
<tr><td>non_smtpd_milters =</td><td>$smtpd_milters</td></tr>
<tr><td>milter_default_action =</td><td>accept</td></tr>
<tr><td>milter_protocol =</td><td>2</td></tr>
</table>


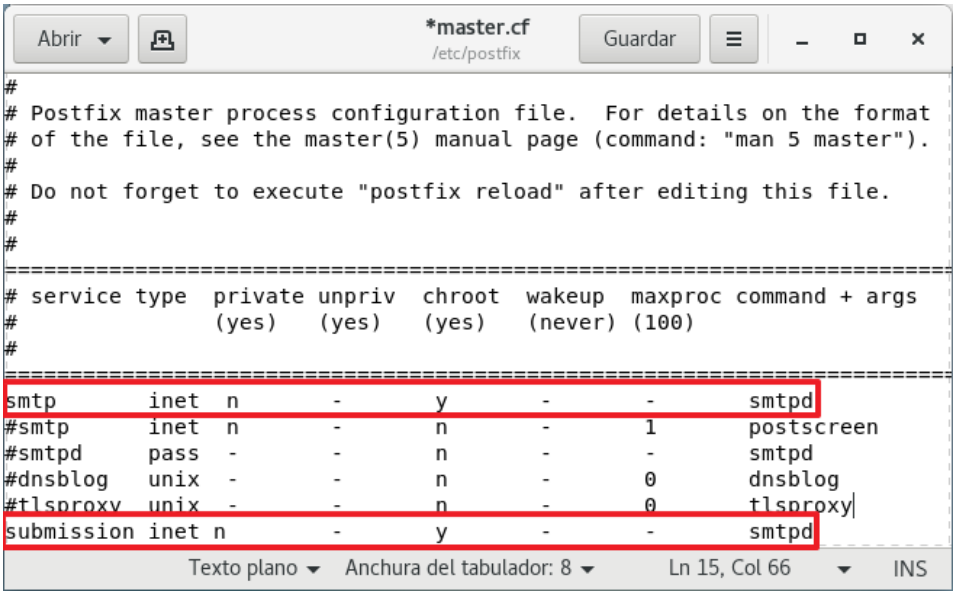
Nota: Tenga en cuenta que el fichero de configuración de la imagen se ha modificado del original para clarificar los parámetros que se deben modificar.</td></tr>
</table>

Paso	Descripción
79.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
80.	El script finaliza el proceso con una comprobación de sintaxis y el mensaje de finalización “DKIM INTEGRADO EN EL SISTEMA”. 
81.	Para continuar ejecute el siguiente script. El script iniciará el proceso de verificación de acceso y pertenencia de los archivos y carpetas necesarias para el correcto funcionamiento seguro de Postfix. Pulse “ENTER” para continuar. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso7_comprobacion_configuracion.sh** 

Paso	Descripción
82.	El script comprobará si permisos en archivos y carpetas pertenecientes a Postfix se encuentran correctamente configuradas según parámetros de seguridad recomendados. Seguidamente, pulsando "ENTER" continuará la ejecución del script.  **Nota:** Si en el caso de que los archivos no pertenezcan a root o no tengan los permisos adecuados deberá cambiarlos con los comandos **chmod** y **chown,** y según los parámetros que más se adecuen a los de su organización.
83.	El Script continua con la comprobación de los usuarios y grupos y sus respectivas "shells". Pulse "ENTER" para continuar. El script finalizará con el mensaje "CONFIGURACION TERMINADA".  **Nota:** Si no existieran los grupos postdrop y postfix, o el usuario postfix, deberá reinstalar Postfix junto con su usuario y grupos correspondientes.

Paso	Descripción
84.	Teniendo en consideración los parámetros de su organización deberá corregir las deficiencias encontradas en el paso anterior y repetir la ejecución del script posteriormente. Para ello, ejecute los siguientes comandos. **$ sudo chsh -s /bin/false postfix** **$ sudo chsh -s /bin/false opendkim** 
85.	Repita la ejecución del script de la misma forma que en pasos anteriores y compruebe que las deficiencias encontradas se encuentran subsanadas. La ejecución del script finalizará con el mensaje “CONFIGURACION TERMINADA”. **$ sudo sh CCN-STIC-681_ENS_ALTA_Paso7_comprobacion_configuracion.sh** 

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>86.</td><td>El último paso consiste en habilitar los servicios necesarios para el correcto funcionamiento del sistema. Ejecute los siguientes comandos e introduzca la contraseña si se le solicita.
$ sudo systemctl unmask postfix.service
$ sudo systemctl start postfix.service
$ sudo systemctl enable postfix.service
$ sudo systemctl restart opendkim</td></tr>
<tr><td>87.</td><td>Se va a proceder a realizar una configuración, en modo de ejemplo, del archivo de configuración “/etc/postfix/main.cf”, para Postfix. Para ello diríjase a la carpeta “Scripts”.
$ cd /Scripts
Nota: El script presentado en esta guía ejecuta, en su parte, el script original dl fabricante.</td></tr>
<tr><td>88.</td><td>Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador.
$ sudo sh CCN-STIC-681_ENS_ALTA_Paso8_master.cf_chroot.sh</td></tr>
<tr><td>89.</td><td>Se procede a realizar una jaula chroot sobre los procesos de Postfix. Para ello primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar “ENTER” para continuar.
 
</td></tr>
<tr><td>90.</td><td>Posteriormente se abrirá, con el editor de textos el archivo “/etc/postfix/master.cf”. Deberá modificar los siguientes valores.
<table>
<tr><th>Valor Inicial</th><th>Valor final</th></tr>
<tr><td>smtp inet n - n - - smtpd</td><td>smtp inet n - y - - smtpd</td></tr>
<tr><td>#submission inet n - n - - smtpd</td><td>submission inet n - y - - smtpd</td></tr>
</table></td></tr>
</table>

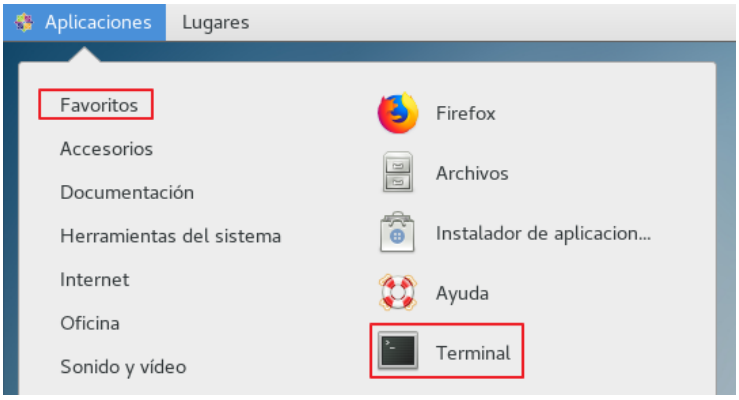
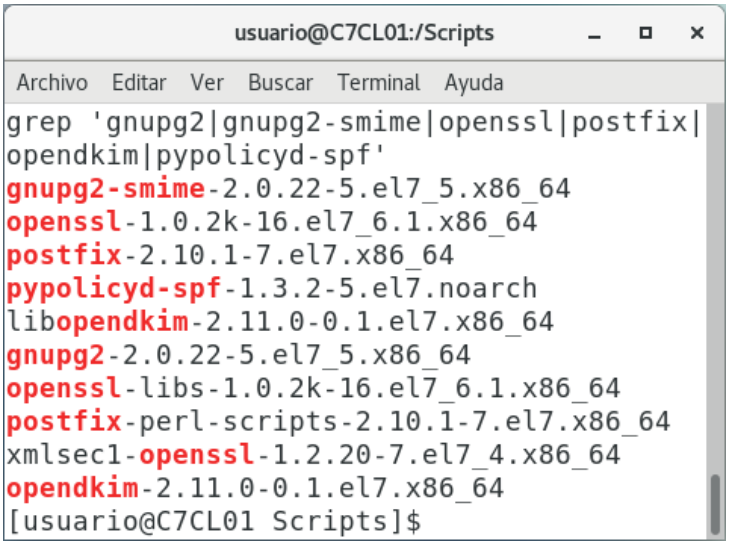
Paso	Descripción
91.	En la siguiente imagen se muestra como deberán quedar definidos los parámetros en el archivo de configuración según la tabla anterior. 
92.	Pulse “Guardar” y cierre el Editor de textos pulsando la **“x”** situada en la zona superior derecha de la ventana. 
93.	Se procede a habilitar los servicios necesarios para el correcto funcionamiento del sistema. Ejecute los siguientes comandos. **$ sudo systemctl unmask postfix.service** **$ sudo systemctl restart postfix.service** **$ sudo systemctl enable postfix.service** **$ sudo systemctl unmask opendkim.service** **$ sudo systemctl restart opendkim.service** **$ sudo systemctl enable opendkim.service** **Nota:** Si se solicita la contraseña para elevar privilegios, introdúzcala.
94.	Elimine la carpeta **“/Scripts”** y todo su contenido.
95.	Guarde las aplicaciones que se encuentren abiertas y reinicie el servidor. **$ sudo shutdown -r**

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR CENTOS7 ENS CATEGORÍA ALTA

Para realizar las comprobaciones pertinentes en el equipo se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán son las siguientes.

a) Terminal.

b) Editor de textos.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En uno de los equipos CentOS 7, inicie sesión con una cuenta que tenga privilegios de administración.
2. Inicie la Terminal de Linux.		Ejecute la "Terminal". Para ello Diríjase a la barra de tareas superior, pulse en Aplicaciones y en el apartado Favoritos seleccione "Terminal". 
3. Verifique que se encuentren instalados los paquetes necesarios.		En la "terminal" ejecute el siguiente comando. **$ sudo rpm -aq | egrep 'gnupg2|gnupg2-smime|openssl|postfix|opendkim|pypolicyd-spf'**  **Nota:** Deberá comprobar que las versiones de los paquetes que aquí se comprueban, se encuentran en sus últimas versiones.

Comprobación	OK/NOK	Cómo hacerlo

Parámetros	OK/NOK
gnupg2-smime-[**versión actualizada**]	
openssl-[**versión actualizada**]	
postfix-[**versión actualizada**]	
pypolicyd-spf-[**versión actualizada**]	
gnupg2-[**versión actualizada**]	
openssl-libs-[**versión actualizada**]	
postfix-perl-scripts-[**versión actualizada**]	
xmlsec1-openssl-[**versión actualizada**]	
opendkim-[**versión actualizada**]	

4. Copias de seguridad de la organización

Compruebe que se realizó exitosamente una copia de seguridad de los siguientes archivos antes de aplicar configuraciones de esta guía. Para ello, ejecute los siguientes comandos para comprobar que existen dichos archivos.

Nota: Ajuste las rutas a las específicas de su organización.

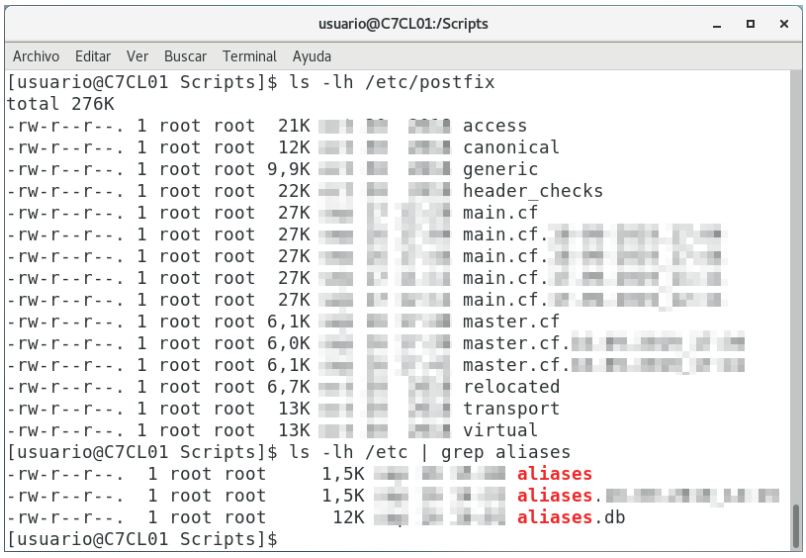
Configuración	OK/NOK
ls /home/usuario/BACKUP/ | egrep "main.cf"	
ls /home/usuario/BACKUP/ | egrep "master.cf"	

5. Copias de seguridad de la organización

En un terminal ejecute los siguientes comandos.

```
$ ls -lh /etc/postfix
$ ls -lh /etc | grep aliases
```

Revise que se han realizado las correspondientes copias de seguridad de los archivos según la ejecución de los scripts correspondientes



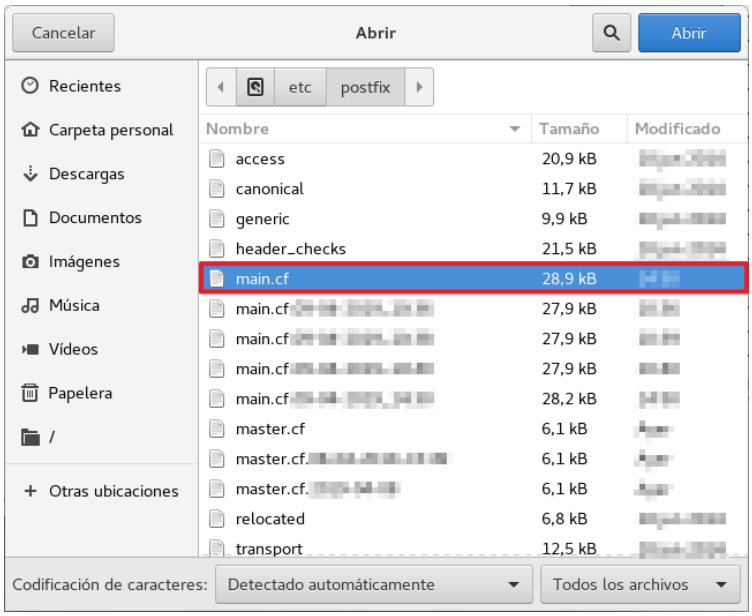
Nota: Tenga en consideración que poseerá tantas copias como veces haya ejecutado los scripts.

Comprobación	OK/NOK	Cómo hacerlo

Configuración	OK/NOK
master.cf.[**FECHA**]	
main.cf.[**FECHA**]	
Aliases.[**FECHA**]	

6. Configuración del archivo main.cf

Edite el archivo "main.cf" pulsando sobre el botón "Abrir" o haciendo doble clic izquierdo con el ratón.



Compruebe los siguientes parámetros y cierre el editor de texto al finalizar la comprobación mediante la **"x"** de la esquina superior derecha de la ventana.

Parámetros	Valor	OK/NOK
mydomain	[**DOMINIO**]	
myhostname	[**SERVIDOR POSTFIX**]	
myorigin	[**DOMINIO**]	
inet_protocols	Ipv4	
inet_interfaces	all	
mydestination	$myhostname, localhost.$mydomain, localhost	
relayhost	[**SERVIDOR DE CORREO PRINCIPAL**]	
smtpd_sasl_auth_enable	Yes	
broken_sasl_auth_clients	yes	
smtpd_sasl_path	private/auth	
smtpd_sasl_security_options	noanonymous	
smtpd_recipient_restrictions	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, permit_auth_destination, check_sender_access hash:/etc/postfix/Lista_Negra	

Comprobación	OK/NOK	Cómo hacerlo

Parámetros	Valor	OK/NOK
smtp_use_tls	yes	
smtp_tls_mandatory_protocols	!SSLv2,SSLv3, TLSv1	
smtpd_tls_cert_file	/etc/ssl/private/<certificado.extensión>	
smtpd_tls_key_file	/etc/ssl/private/<clave.extensión>	
smtpd_tls_session_cache_database	btree:/etc/postfix/smtd_scache	
smtpd_banner =	[MENSAJE DISUASORIO]	
smtpd_milters =	inet:127.0.0.1:8891	
message_size_limit	30720	
non_smtpd_milters =	$smtpd_milters	
milter_default_action =	accept	
milter_protocol =	2	
#smtpd_sasl_type		
default_process_limit	100	
smtpd_client_connection_count_limit	10	
smtpd_client_connection_rate_limit	30	
queue_minfree	20971520	
header_size_limit	512	
smtpd_recipient_limit	100	
body_checks_size_limit	31232	
disable_vrfy_command	yes	

7. Comprobación de posesión de archivos

Se va a proceder a la comprobación del propietario de los ficheros main.cf y master.cf y de los directorios "/var/spool/postfix" y "/var/log/maillog". Todos ellos deben pertenecer al usuario "root".
En la "terminal" ejecute los siguientes comandos.

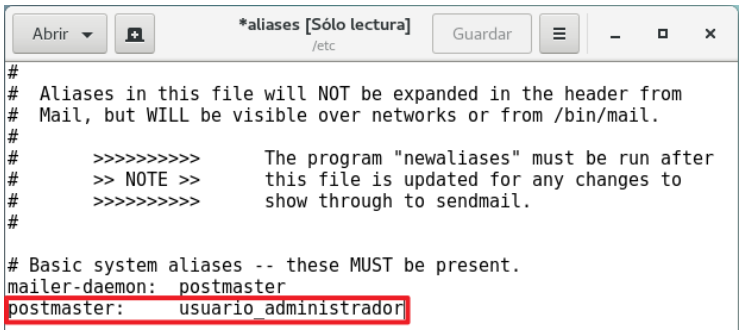
```
$ ls -lh /etc/postfix/main.cf |grep root
$ ls -lh /etc/postfix/master.cf | grep root
$ ls -lh /var/spool/ | grep postfix | grep root
$ ls -lh /var/log/maillog |grep root
```

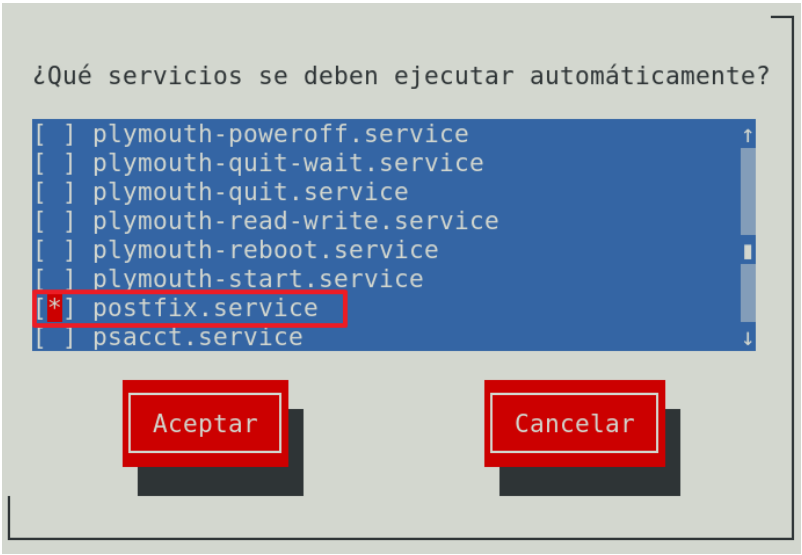
Ruta	Propietario	OK/NOK
/etc/postfix/main.cf	root	
/etc/postfix/master.cf	root	
/var/spool/	root	
/var/log/maillog	root	

8. Comprobación de permisos de archivos

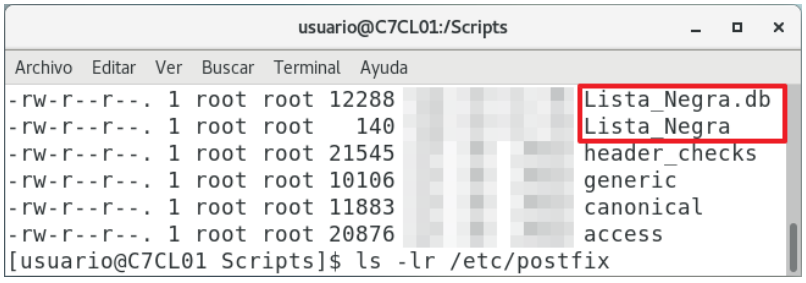
Se comprobará los permisos de archivos y carpetas del sistema. Para ello ejecute los siguientes comandos.

```
$ ls -lh /etc/postfix/main.cf |grep '\-rw-r--r\--'
$ ls -lh /etc/postfix/master.cf |grep '\-rw-r--r\--'
$ ls -lh /var/spool/ | grep postfix | grep rwxr-xr-x.
$ ls -lh /var/log/maillog |grep '\-rw\-------'
```

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2">Fichero</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">/etc/postfix/main.cf</td><td>-rw-r--r--</td><td></td></tr>
<tr><td></td><td colspan="2">/etc/postfix/master.cf</td><td>-rw-r--r--</td><td></td></tr>
<tr><td></td><td colspan="2">/var/spool/postfix</td><td>drwxr-xr-x</td><td></td></tr>
<tr><td></td><td colspan="2">/var/log/maillog</td><td>drw-------</td><td></td></tr>
<tr><td>9. Comprobación de Usuarios y Grupos</td><td></td><td colspan="3">Ejecute los siguientes comandos.
$ cat /etc/passwd |egrep "postfix|/bin/false "
$ cat /etc/group |egrep "postfix|postdrop"
$ cat /etc/passwd |egrep “opendkim|/bin/false "
$ cat /etc/group |egrep " opendkim”</td></tr>
<tr><td></td><td colspan="2">Configuración</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">Usuario: postfix</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Shell: postfix</td><td>/bin/false</td><td></td></tr>
<tr><td></td><td colspan="2">Grupo: postfix</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Grupo: postdrop</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Usuario: opendkim</td><td>Existe</td><td></td></tr>
<tr><td></td><td colspan="2">Shell: opendkim</td><td>/bin/false</td><td></td></tr>
<tr><td></td><td colspan="2">Grupo: opendkim</td><td>Existe</td><td></td></tr>
<tr><td>10. Cambio de usuario de Postmaster</td><td></td><td colspan="3">Compruebe que se han modificado los siguientes parámetros dentro del archivo aliases.
Para ello diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Accesorios” seleccione “Editor de textos”.
Abra el archivo “/etc/postfix/aliases” y compruebe que la figura de “postmaster” ha cambiado por otro usuario que no sea root.
 
</td></tr>
<tr><td>11. Comprobación de los certificados OpenSSL.</td><td></td><td colspan="3">En la “terminal” ejecute el siguiente comando para comprobar la creación de los certificados.
$ ls -lh /etc/ssl/certs
Nota: Los valores deben de ser coincidentes con los nombres y configuraciones específicos de su organización.</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Configuración	**Valor**	**OK/NOK**
		"NOMBREFIRMA"."extensión"	Existencia	
		"CLAVEPRIVADA".key	Existencia	
		Permisos "CLAVEPRIVADA".key	-r---------	
		Permisos "NOMBREFIRMA"."extensión"	-rw-r--r--	
12.Servicios necesarios por medio de herramienta ntsysv		Abra la Terminal y ejecute el siguiente comando. **$ sudo ntsysv**  Compruebe la ejecución del siguiente servicio. Una vez realizada la comprobación utilice el tabulador para colocar el cursor y pulse "Aceptar" para cerrar "ntsysv". **Nota:** Los servicios activos están indicados con un asterisco (*).		
		Configuración	**Valor**	**OK/NOK**
		postfix.service	Activo	
		opendkim.service	Activo	
13.Configuración de jaula chroot		Se procede a la comprobación de los directorios necesarios para la ejecución de un entorno chroot. Para tal proceso ejecute, en un terminal, el siguiente comando y compruebe la existencia de los directorios. **$ ls -lh /var/spool/postfix**		
		Parámetros		**OK/NOK**
		Etc		
		Lib		
		Lib64		
		Private		
		Public		
		usr		

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>14.Configuración del archivo master.cf</td><td></td><td>Compruebe que se han modificado los siguientes parámetros del archivo master.cf.
Para ello diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Accesorios” seleccione “Editor de textos”. Abra el archivo /etc/postfix/master.cf
 

<table>
<tr><th>Parámetros</th><th>OK/NOK</th></tr>
<tr><td>smtp inet n - y - - smtpd</td><td></td></tr>
<tr><td>submission inet n - y - - smtpd</td><td></td></tr>
<tr><td>policyunix-nn-0spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf</td><td></td></tr>
</table></td></tr>
<tr><td>15.Comprobación de la existencia de una lista negra.</td><td></td><td>Compruebe la existencia de una lista negra en la ruta “/etc/postfix”. Para ello, compruebe el contenido de la carpeta “/etc/postfix” mediante el siguiente comando.
$ ls -lr /etc/postfix
 

<table>
<tr><th>Fichero</th><th>Comprobación</th><th>OK/NOK</th></tr>
<tr><td>[nombre fichero lista negra]</td><td>Existencia</td><td></td></tr>
<tr><td>[nombre fichero base de datos].db</td><td>Existencia</td><td></td></tr>
</table></td></tr>
</table>

ANEXO A.5. TAREAS ADICIONALES

ANEXO A.5.1. TAREAS DE MANTENIMIENTO

Para mantener actualizado Postfix y todo su entorno, se deberán atender a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento del mismo. Se realizará un seguimiento continuo para garantizar la seguridad del sistema. Para ello, deberá existir un procedimiento que permita analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. El procedimiento tendrá en cuenta la evaluación del riesgo en función de la aplicación o no de la actualización.

Postfix y sus complementos no se actualizan automáticamente, utiliza las actualizaciones del sistema operativo CentOS 7 Linux, pudiendo forzar su actualización por medio de la consola de comandos.

Según necesidades de su organización, puede actualizar el producto descargando de manera manual versiones actualizadas de Postfix y sus complementos adicionales de las respectivas URLs de los fabricantes.

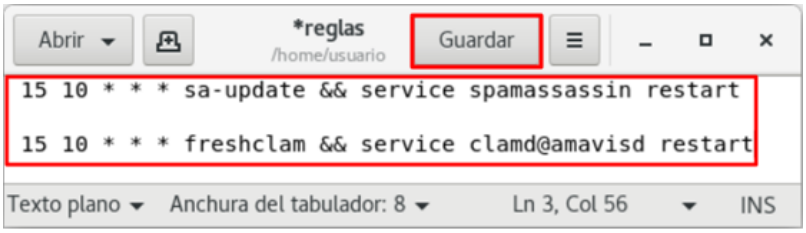
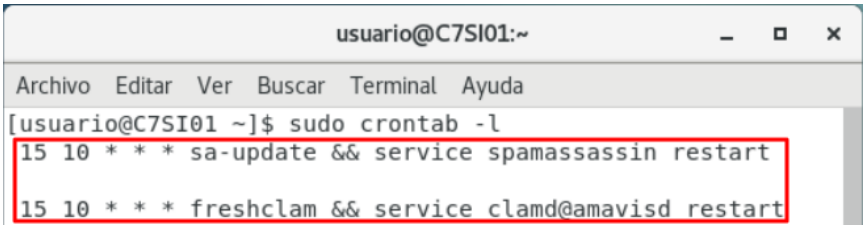
Nota: Si desea obtener más información sobre las actualizaciones de Postfix y derivados visite los sitios web de los fabricantes mediante los siguientes enlaces.
http://www.postfix.org/download.html
https://spamassassin.apache.org/downloads.cgi?update=201809160000
https://www.openssl.org/source/

Para el cumplimiento del ENS es recomendable realizar todas las tareas de actualización previamente en un entorno de pruebas controlado que refleje el entorno de producción de su organización.

Nota: No es objetivo de esta guía especificar los mecanismos o procedimientos necesarios para mantener los sistemas actualizados.

1. AUTOMATIZACIÓN DE ACTUALIZACIONES

Paso	Descripción
1.	Inicie sesión en el equipo CentOS 7 Linux en el que se van a instalar tareas adicionales, con una cuenta de usuario administrador.  **Nota:** Deberá iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".

Paso	Descripción
2.	Diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Favoritos” seleccione “**Terminal**”. Ejecute el comando **“cd /”** y pulse la tecla “ENTER”.
3.	Se procede a la configuración de forma automática de las reglas de SpamAssassin y ClamAV. Para ello se añadirá una tarea programada, en forma de ejemplo, en la herramienta cron incluida en CentOS 7 Linux. Para ello, ejecute el siguiente comando. **$ sudo gnome-text-editor reglas &>/dev/null**
4.	Inserte un texto similar al que se aprecia en la siguiente imagen para realizar las tareas siguientes. – Una actualización diaria de reglas y reinicio del servicio spamassassin a las 10:15. – Una actualización diaria de reglas y reinicio del servicio clamav a las 10:15. Pulse sobre el botón “Guardar” y la **“x”** de la esquina superior derecha para cerrar el editor de texto. 
5.	Deberá de redireccionar, como super usuario, el archivo creado al comando encargado de la realización de las tareas programadas “cron”. **$ sudo crontab < reglas**
6.	Deberá borrar el archivo “reglas” y comprobar la creación de la tarea programada en cron. Para ello ejecute los siguientes comandos. **$ sudo rm /reglas** **$ sudo crontab -l** 

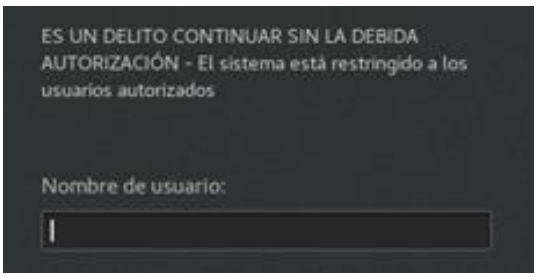
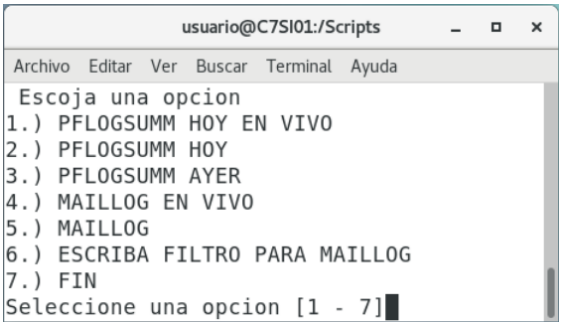
2. PFLOGSUMM

Pflogsumm es un analizador de registros de actividad para el MTA de Postfix, diseñado para tener una visión general del tráfico producido por el servidor Postfix y tiene la capacidad de dar detalles suficientes para la administración del sistema en busca de discrepancias de funcionamiento.

Pflogsumm genera resúmenes e informes detallados de volúmenes de tráfico del servidor de correo, correo electrónico rechazado o devuelto. La herramienta registra tanto advertencias como errores.

Entre las opciones más comunes de Pflogsumm se incluyen la generación de informes diarios y del día anterior.

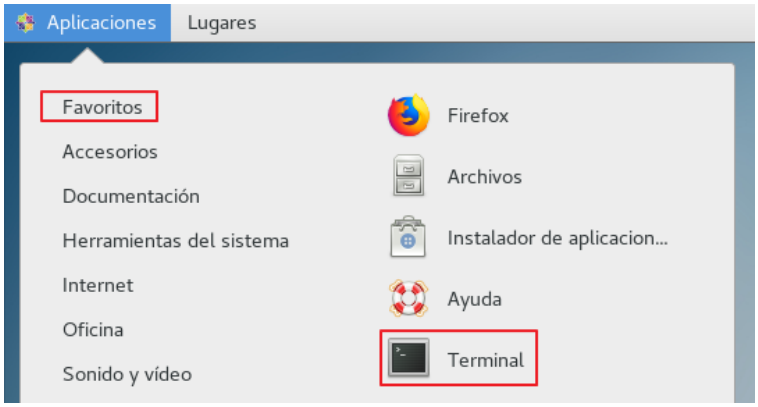
```
$ sudo pflogsumm -d today /var/log/maillog
$ sudo pflogsumm -d yesterday /var/log/maillog
```

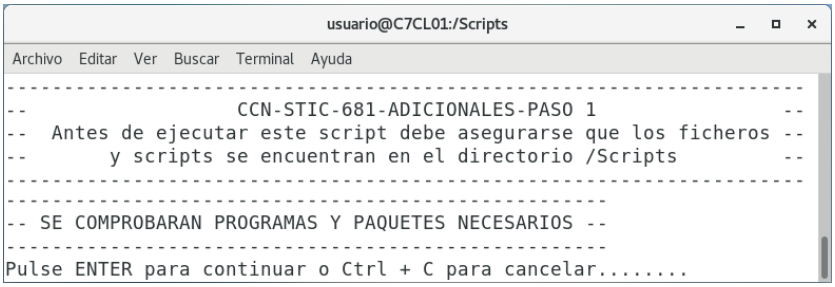
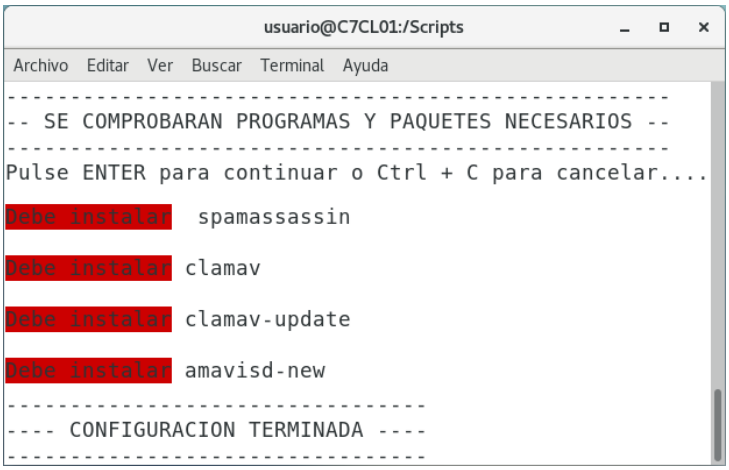
Paso	Descripción
1.	Inicie sesión en el equipo CentOS 7 Linux en el que se van a aplicar tareas adicionales, con una cuenta de usuario administrador.  **Nota:** Deberá iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".
2.	Diríjase a la barra de tareas superior, pulse sobre "Aplicaciones" y en el apartado "Favoritos" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "ENTER".
3.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. **$ sudo sh CCN-STIC-681_Adicional_Log.sh**
4.	Se desplegará un menu que le facilitara la tarea de visualizado de logs. 
5.	Para finalizar cualquier proceso pulse "CTRL+C".

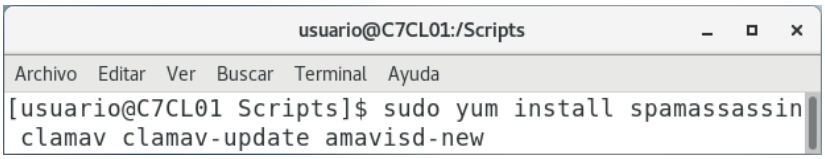
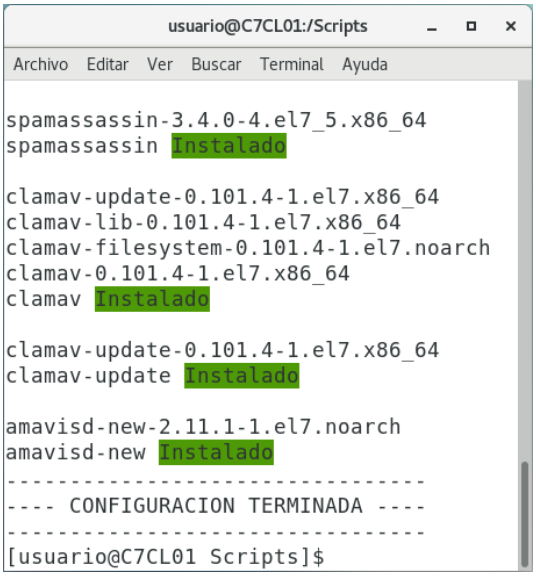
ANEXO A.5.2. TAREAS DE SEGURIDAD

Antes de comenzar con los puntos correspondientes a tareas adicionales de seguridad, debe conocer que la implementación de la funcionalidad "Amavis" engloba las soluciones de "SpamAssassin" y "ClamAv", por lo que si decide instalar ambas deberá dirigirse directamente al punto "4 AMAVIS".

1. PAQUETES ADICIONALES

Paso	Descripción
1.	Inicie sesión en el equipo CentOS 7 Linux en el que se van a instalar tareas adicionales, con una cuenta de usuario administrador.
2.	Diríjase a la barra de tareas superior, pulse sobre "Aplicaciones" y en el apartado "Favoritos" seleccione "Terminal". 
3.	Cree la carpeta "**Scripts**". Para ello, en el terminal, ejecute el comando siguiente. **$ cd /** Para crear la carpeta en la ubicación ejecute el siguiente comando. **$ sudo mkdir Scripts** **Nota:** Puede comprobar que la carpeta ha sido creada ejecutando **ls /**.
4.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía "CCN-STIC-681- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE CENTOS 7 LINUX". Introduzca las credenciales si se lo solicita.
5.	Copie el contenido de la carpeta con los scripts de "TAREAS ADICIONALES" correspondiente al directorio "Scripts/ENS_ADICIONALES" asociado a esta guía en la ruta "**/Scripts**". Pare ello, ejecute el comando siguiente. **$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_ADICIONALES/* /Scripts/** **Nota:** Se considera que los scripts están disponibles en un disco óptico que es sistema reconoce como ISO Label, en caso contrario adapte la ruta al medio de almacenamiento escogido. Los scripts asumen que su ubicación en el sistema será bajo "/Scripts". Si se desea modificar la ubicación deberá editar los scripts para reflejar la nueva ubicación.

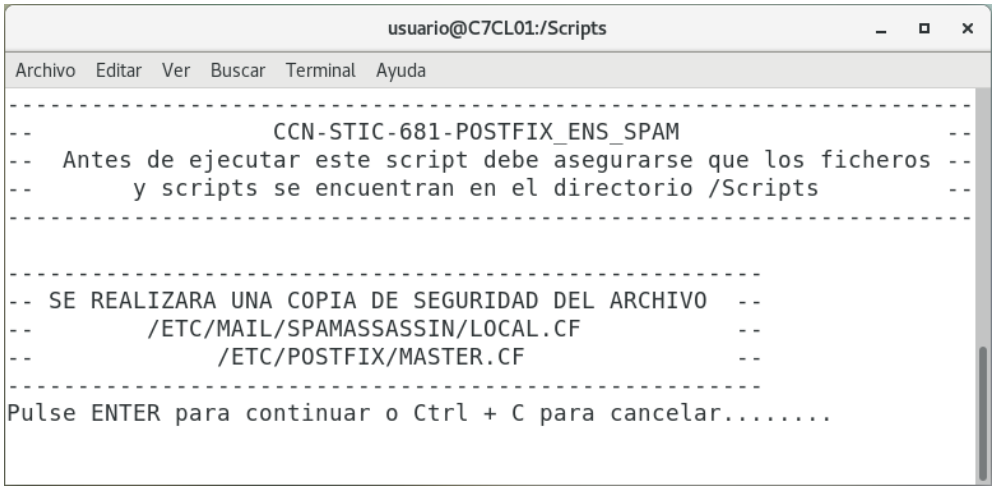
Paso	Descripción
6.	Expulse el CD/DVD de la unidad y diríjase a la carpeta “Scripts” .Para ello ejecute el comando siguiente. **$ cd /Scripts**
7.	Se va a comprobar los paquetes necesarios para la instalación de las diversas soluciones descritas durante el desarrollo de este punto (ANEXO A.5.2 TAREAS DE SEGURIDAD). Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_Paso1_ADICIONALES_comprobacion_paquetes_necesarios.sh**
8.	Pulse “ENTER” para continuar. 
9.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar.  **Nota:** Los resultados mostrados en pantalla pueden variar dependiendo de las configuraciones específicas de su organización.

Paso	Descripción
10.	Instale o actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. **$ sudo yum install <Paquete1 Paquete2 Paquete 3 …>** **$ sudo yum update <Paquete1 Paquete2 Paquete 3 …>** 
11.	Ejecute el script de nuevo para comprobar que la configuración es correcta. **$ sudo sh CCN-STIC-681_ENS_Paso1_ADICIONALES_comprobacion_paquetes_necesarios.sh** 
12.	Por motivos de seguridad preservando los datos y configuraciones de su organización, se va a proceder a realizar una copia de seguridad de las configuraciones originales de todos los archivos de configuración susceptibles de ser cambiados por esta guía. Para dicho proceso, escriba los siguientes comandos. **$ sudo cp -f /etc/mail/spamassassin/local.cf /home/usuario/BACKUP** **$ sudo cp -f /etc/freshclam.conf /home/usuario/BACKUP** **$ sudo cp -f /usr/share/doc/[Versión de Clamav que posea] /clamd.sysconfig "/home/usuario/BACKUP"** **$ sudo cp -f /etc/sysconfig/clamd.amavisd /home/usuario/BACKUP** **$ sudo cp -f /etc/tmpfiles.d/clamd.amavisd.conf /home/usuario/BACKUP** **$ sudo cp -f /usr/lib/systemd/system/clamd@.service /home/usuario/BACKUP** **Nota:** Debe elegir una ruta o medio extraíble donde ubicar dichas configuraciones para una posible restauración a un punto anterior. La ubicación "/home/BACKUP/" es la ubicación elegida por esta guía a modo de ejemplo. Adapte la configuración según requisitos específicos de su organización.

2. SPAMASSASSIN

SpamAssassin es una herramienta de filtrado de spam en los servidores de correo electrónico. Spamassassin analiza los mensajes de correo determinando la probabilidad de que sean spam.

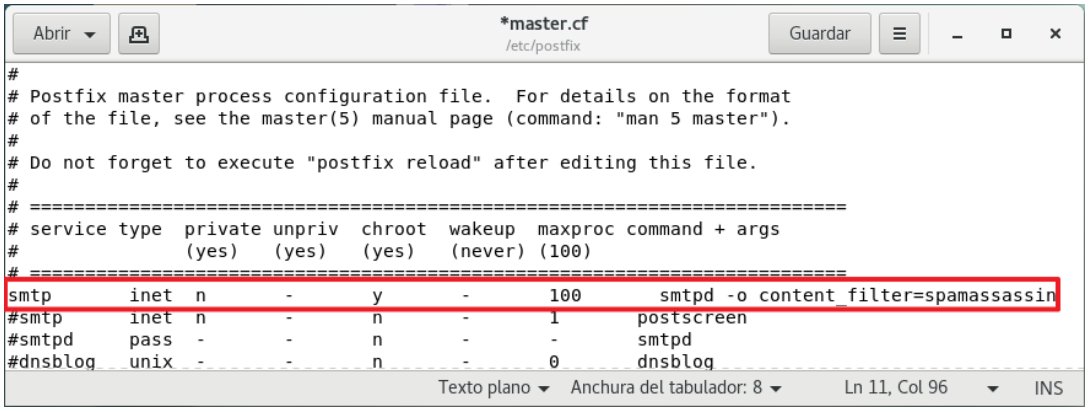
Nota: En esta guía, en modo de ejemplo, se realizará una instalación y configuración consistente en Postfix como MTA y filtrado Spam por Spamassassin.
En caso de que Amavis esté previamente configurado mediante la presente guía, los pasos siguientes no serán necesarios ya que las configuraciones relativas a Spamassassin se aplican en el punto "4 AMAVIS" de la presente guía.

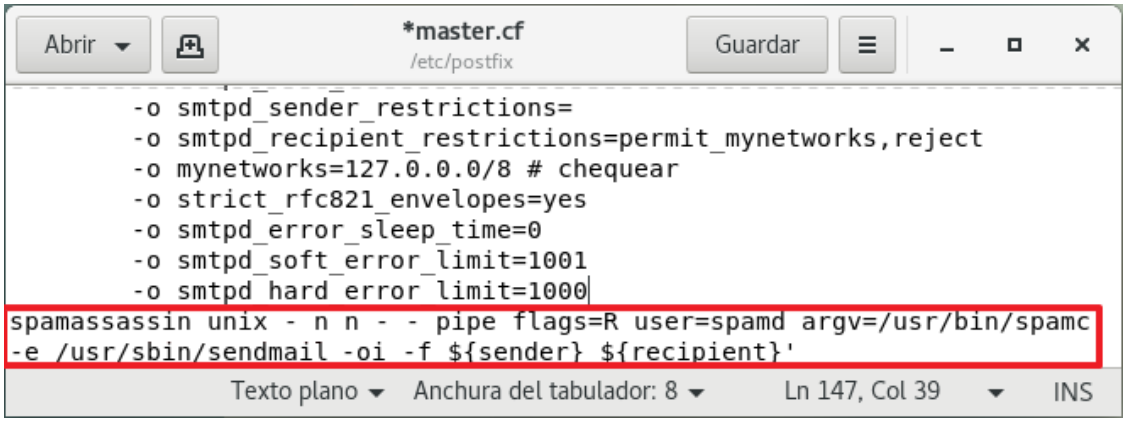
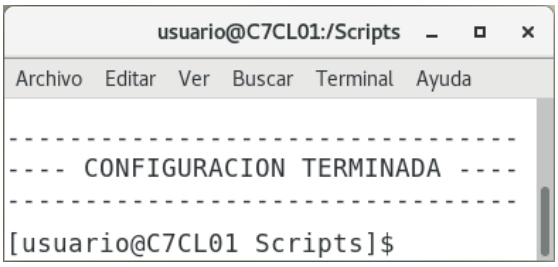
Paso	Descripción
1.	Inicie sesión en el equipo CentOS 7 Linux que está asegurando, con una cuenta administrador o sudoer.
2.	Diríjase al directorio "/Scripts". **$ cd /Scripts**
3.	Se procede a crear el usuario y el grupo "spamd", encargados del mantenimiento del programa. Para ello ejecute en el terminal los siguientes comandos. **$ sudo groupadd spamd** **$ sudo useradd -g spamd -s /bin/false -d /var/log/spamassassin spamd** **$ sudo chown spamd:spamd /var/log/spamassassin**
4.	Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_Adicional_Spam.sh**
5.	Se inicia la configuración de Apache SpamAssassin como solución antispam del correo. Para ello, se configura el archivo principal ubicado en /etc/mail/spamassassin/local.cf realizando una copia de seguridad en el mismo directorio con una terminación de fecha y hora. Pulse "ENTER" para continuar. 

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>6.</td><td>El script comenta toda configuración incluida en el fichero “local.cf”, a continuación, se edita el archivo de configuración “local.cf” ubicado en el directorio /etc/mail/spamassassin con el editor de textos. Se muestra una tabla con configuraciones de seguridad de los parámetros del fichero. Adapte éstos a los que más se adapten con su organización.

Nota: El parámetro “rewrite_header Subject” es el “mensaje” que mostrará el sistema al detectar un correo como spam

<table>
<tr><th>Parámetro</th><th>Valor</th></tr>
<tr><td>required_hits</td><td>5</td></tr>
<tr><td>rewrite_header Subject</td><td>['$mensaje']</td></tr>
<tr><td>report_safe</td><td>1</td></tr>
<tr><td>use_bayes</td><td>1</td></tr>
<tr><td>bayes_auto_learn</td><td>1</td></tr>
<tr><td>skip_rbl_checks</td><td>0</td></tr>
<tr><td>use_razor2</td><td>1</td></tr>
<tr><td>use_pyzor</td><td>1</td></tr>
</table></td></tr>
<tr><td>7.</td><td>Pulse sobre “Guardar” y cierre el editor de textos pulsando sobre la “x” en la esquina superior derecha de la ventana.
 
</td></tr>
<tr><td>8.</td><td>Seguidamente se abrirá el archivo de configuración “/etc/postfix/master.cf” en el cual se deberá añadir la siguiente configuración para el escaneo por parte de la solución de “SpamAssassin” de los mensajes de correo entrantes.

<table>
<tr><th>Valor inicial</th><th>Valor final</th></tr>
<tr><td>smtp inet n - yes - 100 smtpd</td><td>smtp inet n - y - 100 smtpd -o content_filter=spamassassin</td></tr>
</table>

</td></tr>
</table>

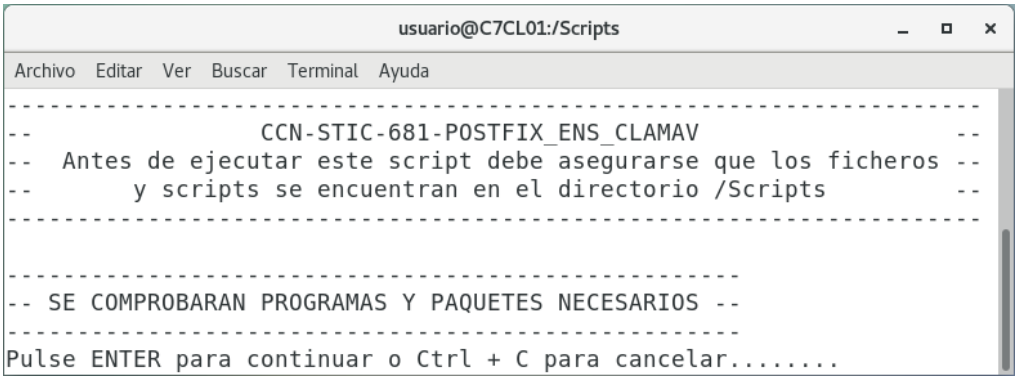
Paso	Descripción
9.	Añada la siguiente línea al final del archivo de configuración. **spamassassin unix - n n - - pipe flags=R user=spamd argv=/usr/bin/spamc -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}'** 
10.	Una vez definidos los parámetros indicados, pulse "**Guardar**" y cierre el Editor de textos pulsando la **"x"** situada en la zona superior derecha de la ventana. 
11.	El script finalizará con el siguiente mensaje. 
12.	SpamAssassin posee un comando para poder comprobar la sintaxis de sus archivos de configuración. Ejecute el siguiente comando. Si la sintaxis fuera correcta no se mostrará ningún mensaje por pantalla. **$ sudo spamassassin --lint** **Nota:** Si en la salida del comando hubiese alguna discrepancia a solucionar, restaure el archivo de respaldo de configuración "local.cf.[fecha]" y vuelva a ejecutar el script "CCN-STIC-681-ENS_Adicional_Spam.sh".

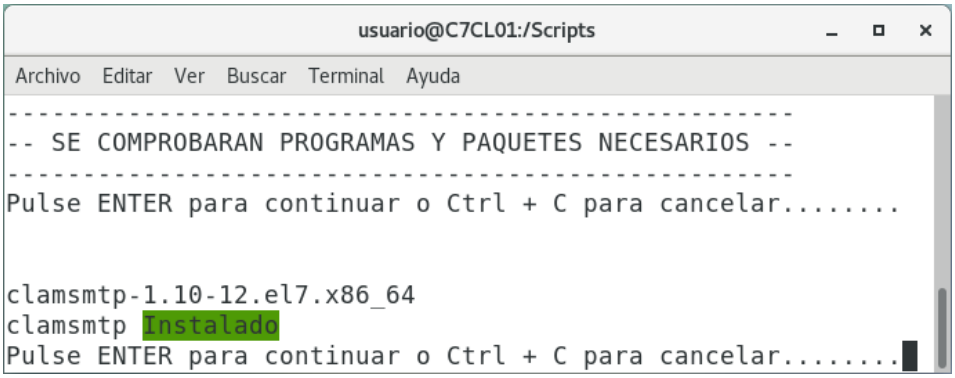
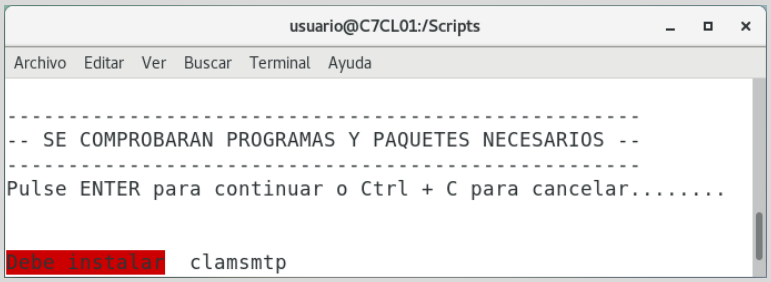
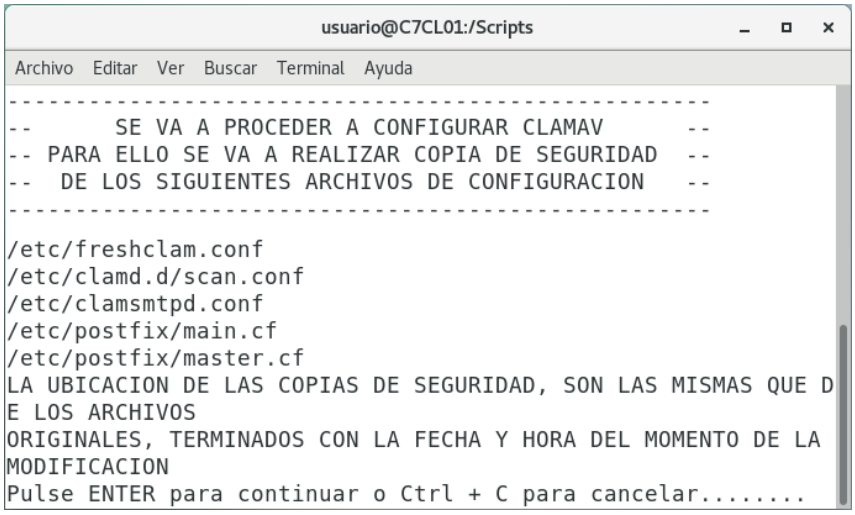
3. CLAMAV

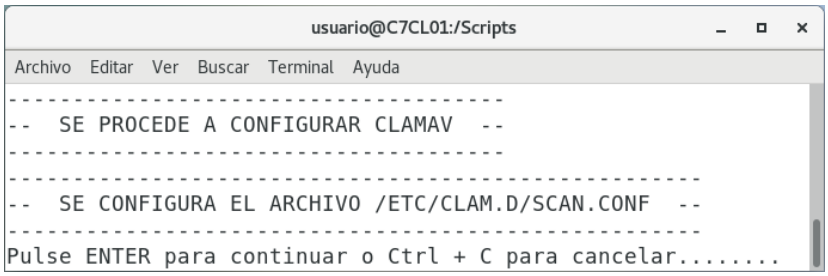
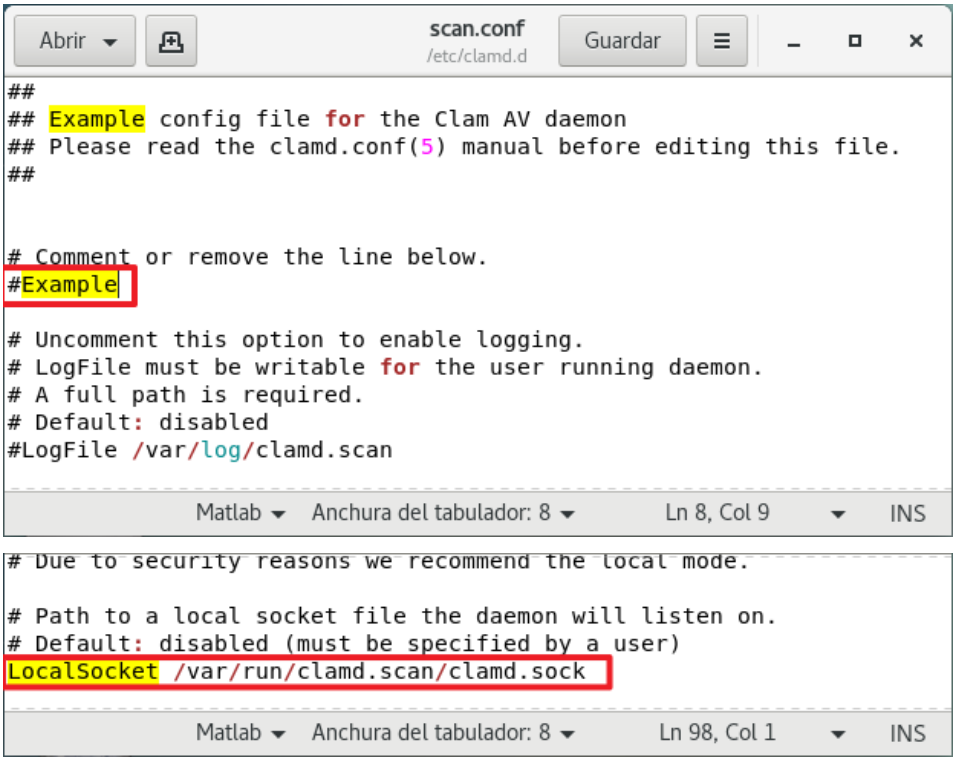
Clamav es un software antivirus de código abierto, Open Source y licencia GPL.

Clamav se integra en el sistema Postfix, para el chequeo de correo electrónico en busca de virus y otros malware, proporcionando una serie de herramientas diseñadas para este propósito específico.

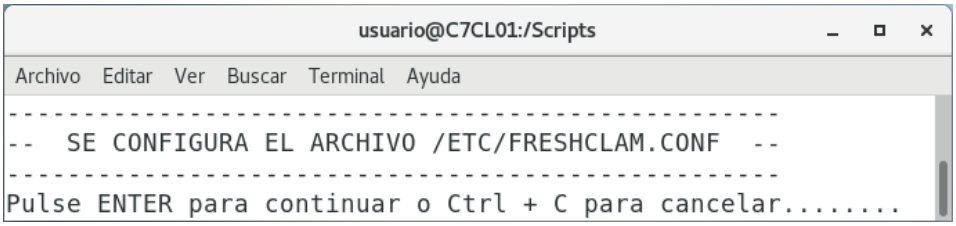
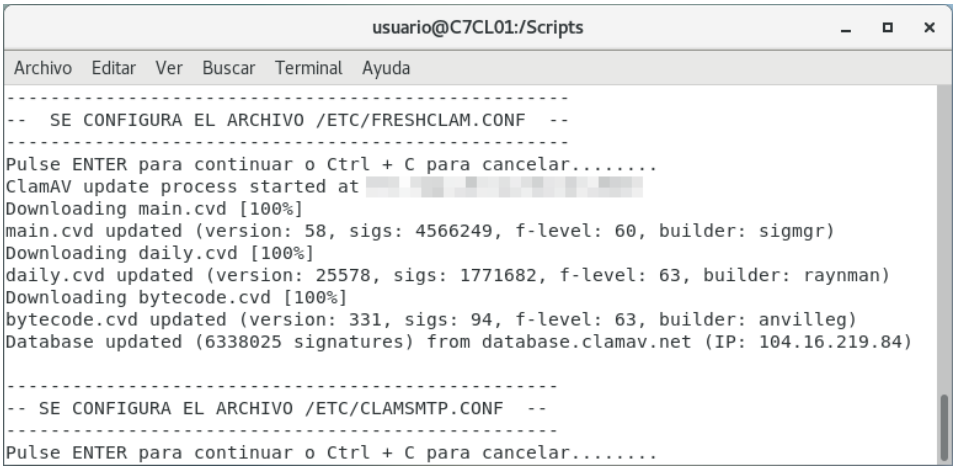
Nota: En esta guía, en modo de ejemplo, se realizará una instalación y configuración consistente en Postfix como MTA, con filtrado antivirus por Clamav.
En caso de que Amavis esté previamente configurado mediante la presente guía, los pasos siguientes no serán necesarios ya que las configuraciones relativas a Clamav se aplican en el punto "4 AMAVIS" de la presente guía.

Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS. Deberá iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers". 
2.	Diríjase al directorio "/Scripts". **$ cd /Scripts**
3.	Ejecute el siguiente comando y siga los pasos que le indica. Introduzca la contraseña si se le solicita. **$ sudo sh CCN-STIC-681_ENS_Adicional_Clamav.sh**
4.	Se comienza la configuración de la aplicación antivirus ClamAV, para ello se realiza una comprobación de paquetes necesarios. 

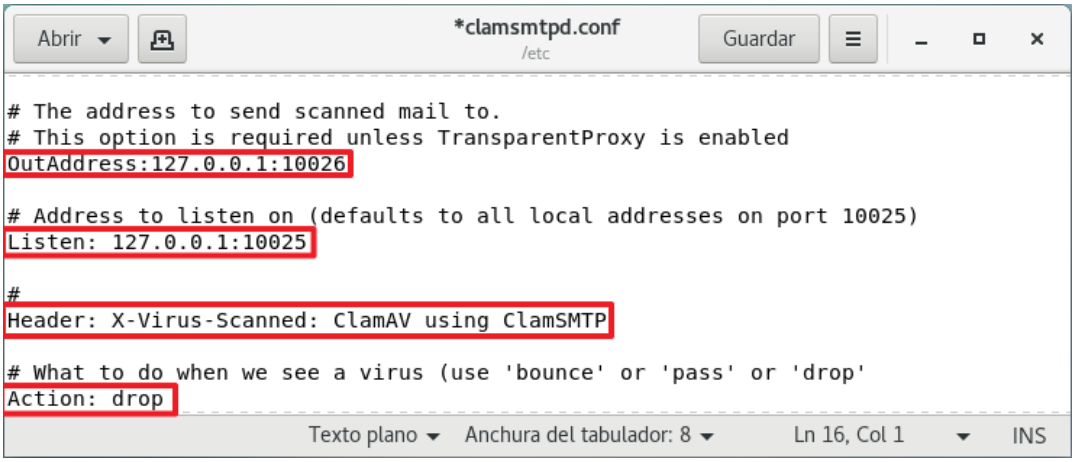
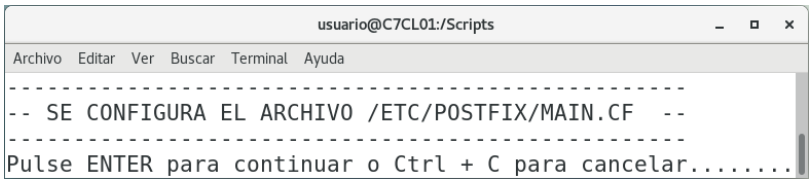
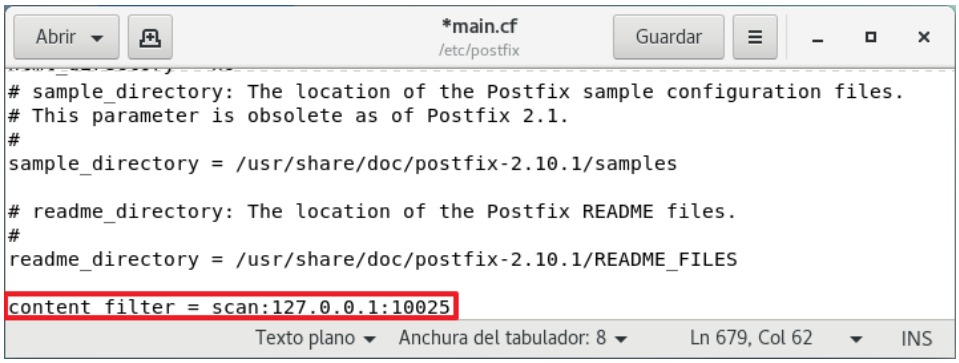
Paso	Descripción
5.	Para la continuación de la ejecución del script, deberá pulsar “ENTER”. Una vez finalice la ejecución y los paquetes necesarios se encuentran instalados, pulse ENTER para continuar.  **Nota:** Si la salida del comando da como resultado el mensaje “Debe instalar”, Pulse “Enter”. El script finalizará para que pueda instalar el paquete requerido.  Ejecute el siguiente comando para la instalación del paquete. **$ sudo yum install clamsmtp** Cuando la instalación haya finalizado, repita los pasos del 2 al 5 de este mismo punto antes de continuar.
6.	Una vez comprobados los archivos y librerías necesarias para continuar, se realizará una copia de los ficheros de configuración a modificar. Pulse “ENTER”, para continuar. 

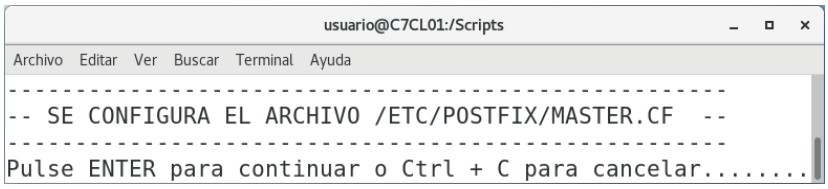
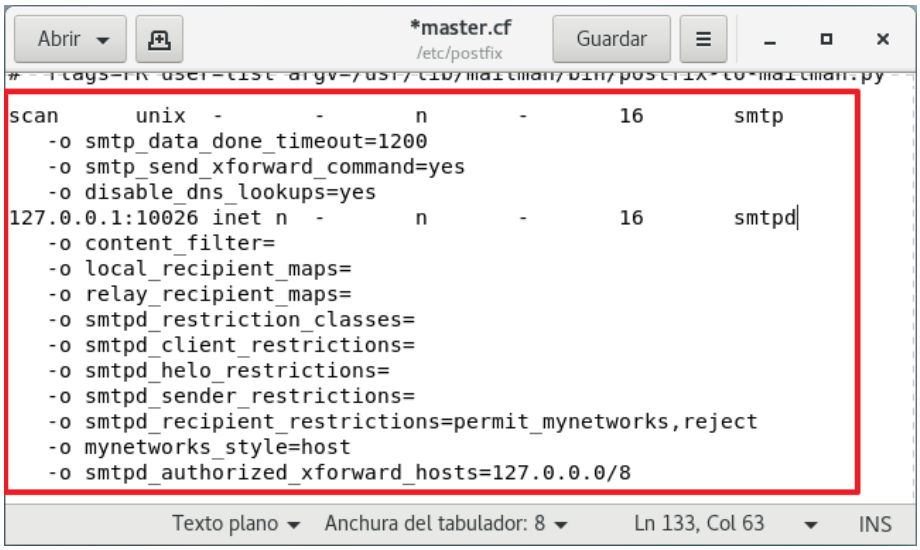
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>7.</td><td>Realizadas, las copias de seguridad de los archivos necesarios, se comienza con la configuración. Pulse “ENTER” para continuar.

</td></tr>
<tr><td>8.</td><td>El script editará el fichero “/etc/clam.d/scan.conf”. Deberá modificar los valores acordes a la siguiente tabla.
<table>
<tr><th>Valor Original</th><th>Valor Final</th></tr>
<tr><td>Example</td><td>#Example</td></tr>
<tr><td>#LocalSocket
/var/run/clam.scan/clamd.sock</td><td>LocalSocket
/var/run/clam.scan/clamd.sock</td></tr>
</table></td></tr>
<tr><td>9.</td><td>Los valores quedarán configurados como se muestra en la siguiente imagen. Guarde el documento y cierre el editor de texto.

</td></tr>
<tr><td>10.</td><td>Pulse “Guardar” y, acto seguido, pulse “x” para cerrar el editor de texto.

</td></tr>
</table>

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>11.</td><td>Se va a configurar el archivo “freshclam.conf”. Para continuar con el proceso debe pulsar “ENTER”.
 
</td></tr>
<tr><td>12.</td><td>Deberá modificar los valores acordes a la siguiente tabla.
<table>
<tr><th>Valor Original</th><th>Valor Final</th></tr>
<tr><td>Example</td><td>#Example</td></tr>
</table></td></tr>
<tr><td>13.</td><td>Los valores quedarán configurados, como se muestra en la siguiente imagen.
 
</td></tr>
<tr><td>14.</td><td>Pulse sobre “Guardar” y cierre el editor de textos pulsando sobre la “x” en la esquina superior derecha de la ventana.
 
</td></tr>
<tr><td>15.</td><td>Posteriormente, el equipo conectará con los servidores de ClamAV para descargar las firmas de virus. Cuando finalice pulse “Enter” para editar el fichero “clamsmtp.conf”.
 

Nota: Este proceso puede durar varios minutos. El sistema intentará conectar con los servidores de ClamAV, si no puede conectar automáticamente probará en una réplica suya. Ignore los mensajes de error.</td></tr>
</table>

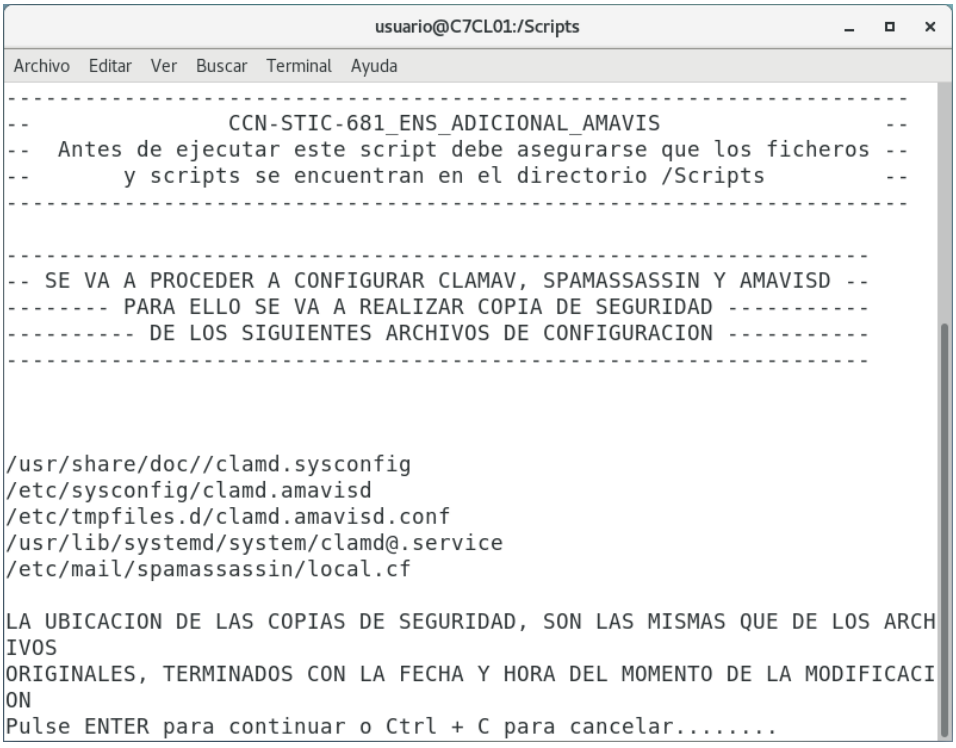
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>16.</td><td>Deberá modificar los valores acordes a la siguiente tabla.
<table>
<tr><th>Valor Original</th><th>Valor Final</th></tr>
<tr><td>OutAddress: 10026</td><td>OutAddress: 127.0.0.1:10026</td></tr>
<tr><td>#Listen: 0.0.0.0:10025</td><td>Listen: 127.0.0.1:10025</td></tr>
<tr><td>#Header: X-Virus-Scanned: ClamAV using ClamSMTP</td><td>Header: X-Virus-Scanned: ClamAV using ClamSMTP</td></tr>
<tr><td>#Action: drop</td><td>Action: drop</td></tr>
</table>

</td></tr>
<tr><td>17.</td><td>Pulse sobre “Guardar” y cierre el editor de textos pulsando sobre la “x” en la esquina superior derecha de la ventana.</td></tr>
<tr><td>18.</td><td>El script procederá a configurar el archivo /etc/postfix/main.cf. Pulse ENTER para continuar.

</td></tr>
<tr><td>19.</td><td>Inserte la siguiente línea al final del texto.
content_filter = scan:127.0.0.1:10025

</td></tr>
<tr><td>20.</td><td>Pulse sobre “Guardar” y cierre el editor de textos pulsando sobre la “x” en la esquina superior derecha de la ventana.</td></tr>
</table>

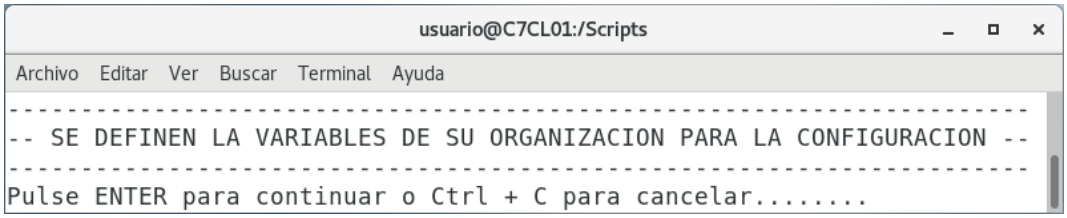
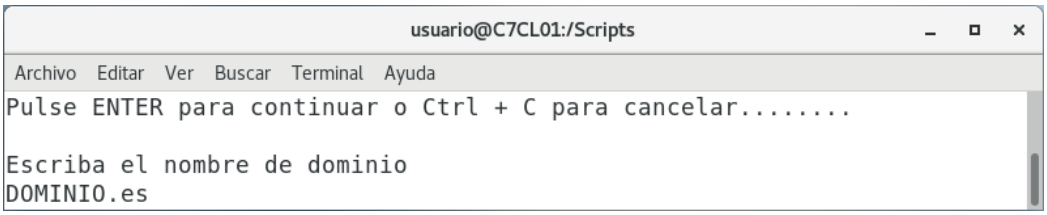
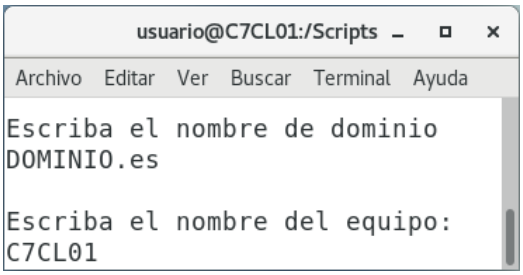
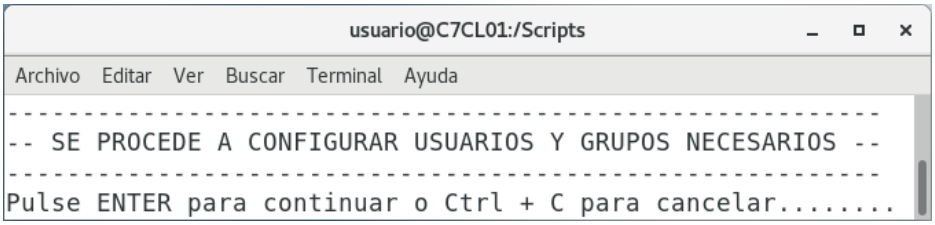
Paso	Descripción
21.	Finalmente se procederá a configurar el archivo /etc/postfix/master.cf con los valores de seguridad recomendados. Pulse “ENTER” para continuar. 
22.	Se muestran valores recomendados de configuración de seguridad que deberá adaptar a las necesidades de su organización. **scan unix - - n - 16 smtp** **-o smtp_data_done_timeout=1200** **-o smtp_send_xforward_command=yes** **-o disable_dns_lookups=yes** **127.0.0.1:10026 inet n - n - 16 smtpd** **-o content_filter=** **-o local_recipient_maps=** **-o relay_recipient_maps=** **-o smtpd_restriction_classes=** **-o smtpd_client_restrictions=** **-o smtpd_helo_restrictions=** **-o smtpd_sender_restrictions=** **-o smtpd_recipient_restrictions=permit_mynetworks,reject** **-o mynetworks_style=host** **-o smtpd_authorized_xforward_hosts=127.0.0.0/8** 
23.	Pulse sobre “Guardar” y cierre el editor de textos pulsando sobre la **“x”** en la esquina superior derecha de la ventana. **Nota:** Cuando cierre el documento se iniciará un proceso que puede tardar varios minutos.
24.	El proceso termina con el mensaje “CONFIGURACION TERMINADA”.

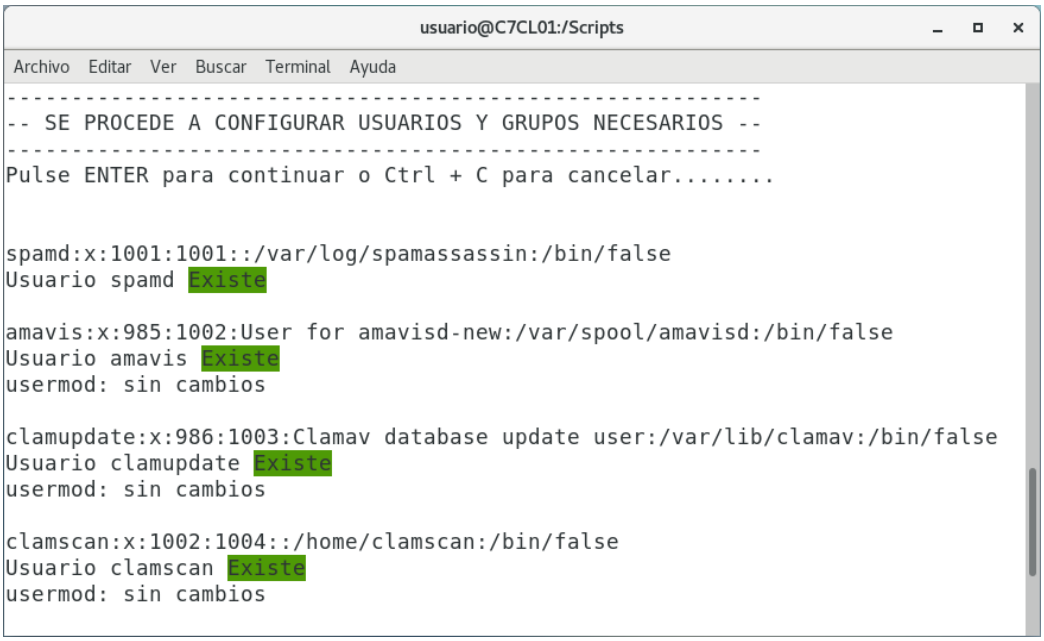
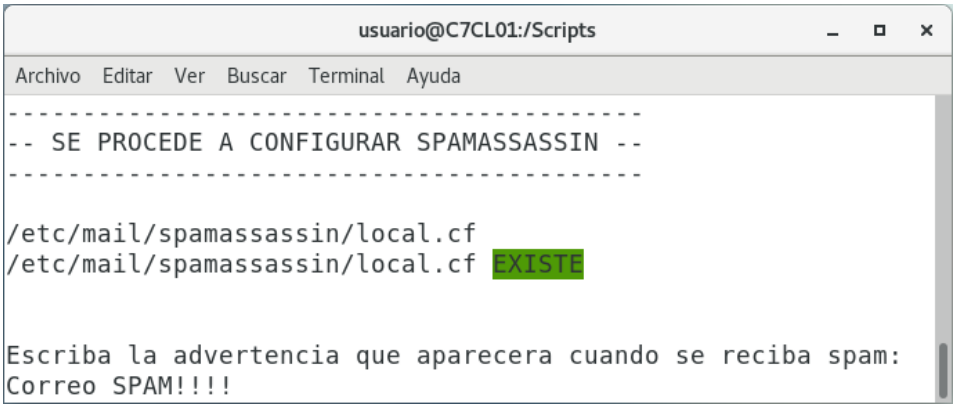
4. AMAVIS

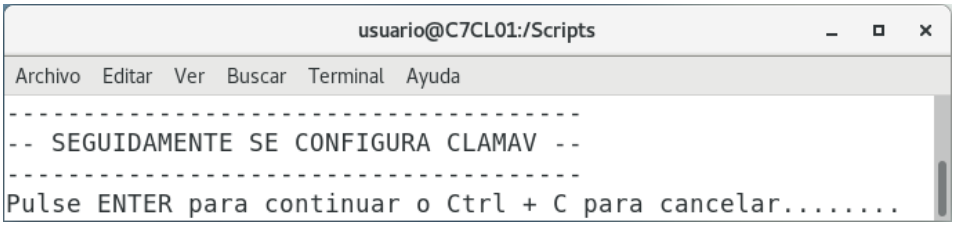
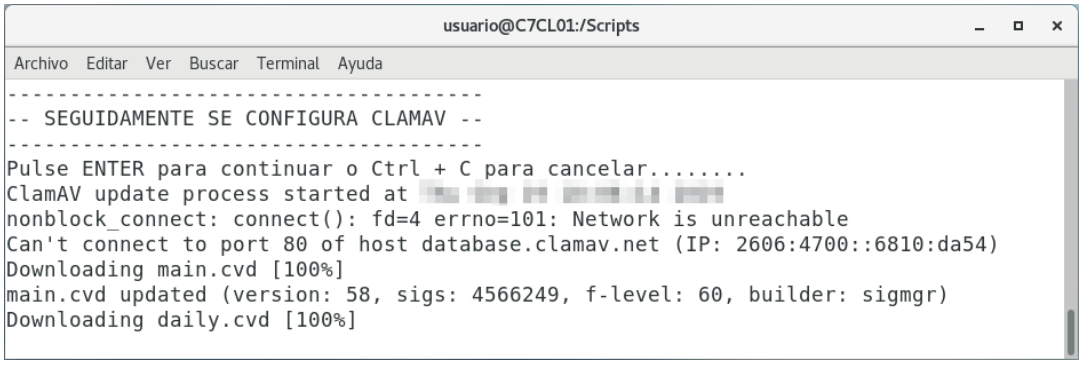
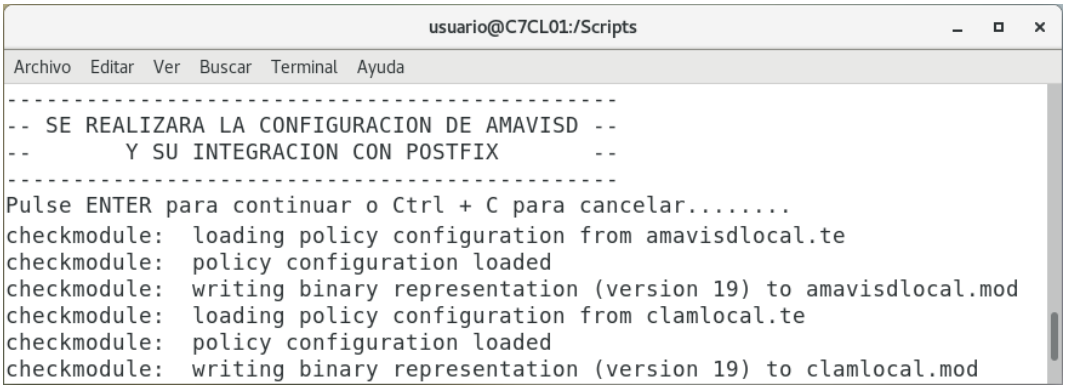
Amavis es una solución de código abierto para el correo electrónico que se ocupa del filtrado de mensajes, protegiendo el sistema de correo electrónico de mensajes no deseados, de virus y de otros programas maliciosos. Actúa como una interfaz entre el MTA y los filtros de contenido antivirus, filtro de contenido antispam.

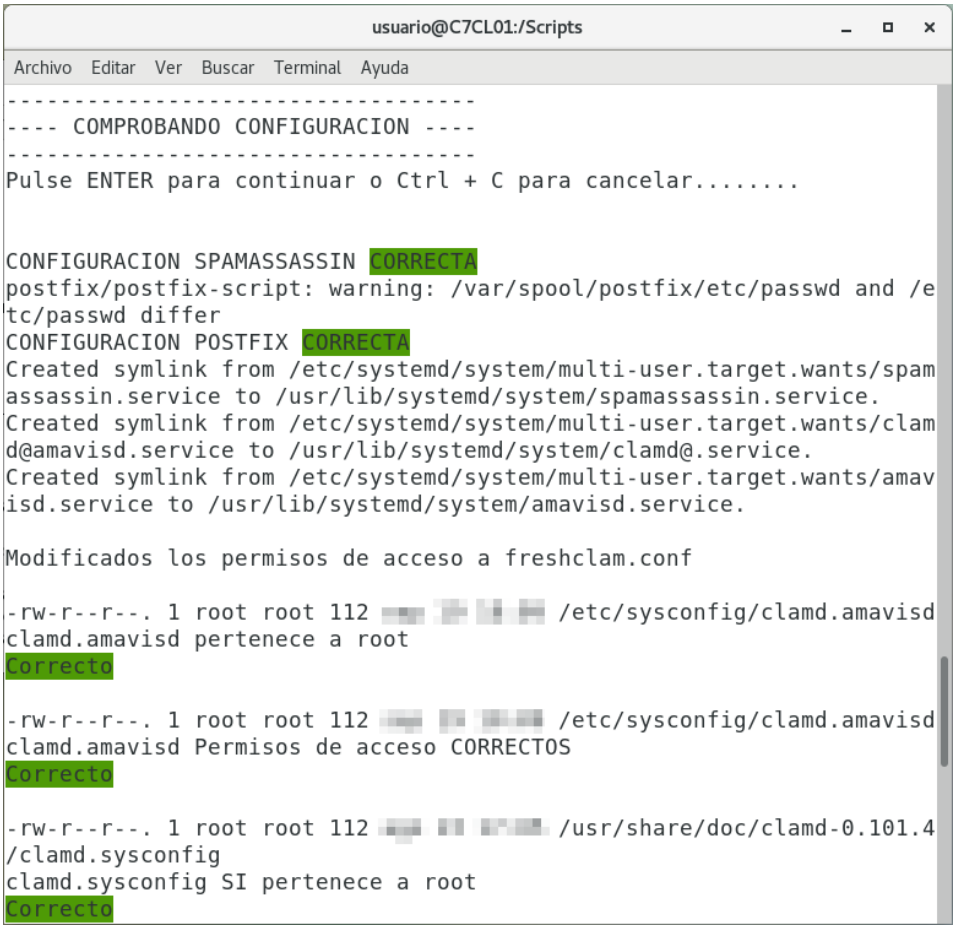
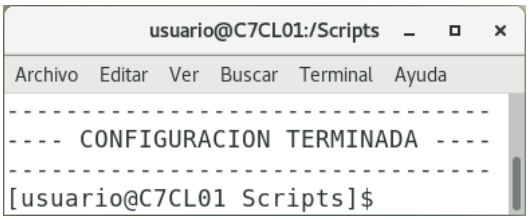
Nota: En esta guía, a modo de ejemplo, se realizará una instalación y configuración consistente en Postfix como MTA, el uso de Amavis como filtro de los correos entrantes por SMTP, filtrado antivirus por Clamav y filtrado Spam por Spamassassin.

Paso	Descripción
1.	Inicie sesión en el equipo CentOS 7 Linux en el que se van a instalar tareas adicionales, con una cuenta de usuario administrador.
2.	Diríjase al directorio "/Scripts". **$ cd /Scripts**
3.	Ejecute el siguiente comando y siga los pasos que le indica. Si fuese necesario, inserte contraseña de usuario administrador. **$ sudo sh CCN-STIC-681_ENS_Adicional_Amavis.sh**
4.	La solución Amavis integra ClamAV y Spamassassin. Se procede a realizar los pasos necesarios para completar dicha integración en el sistema. Para ello, se realizan las copias de seguridad de los archivos de configuración. Para continuar con el proceso pulse "ENTER".  **Nota:** Los archivos de respaldo se guardan en el mismo directorio del archivo original, con una terminación de fecha y hora del momento en que se realiza la copia.

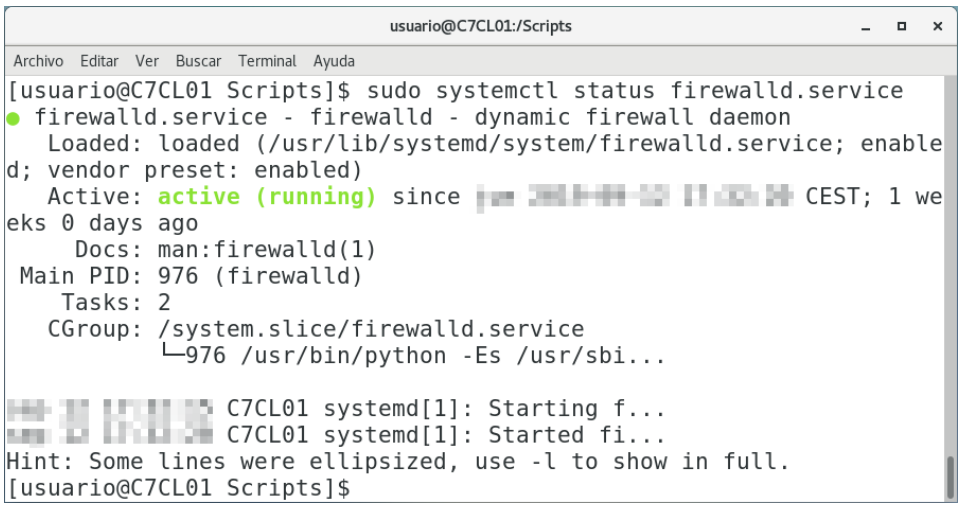
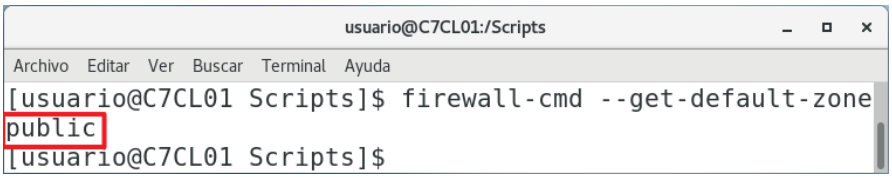
Paso	Descripción
5.	Se procede a definir las variables correspondientes con su organización. Para tal cometido presione “ENTER”. 
6.	Inserte el nombre de dominio de su organización y pulse “ENTER”. 
7.	Escriba el nombre del equipo donde se está implantando la solución de Amavis, y pulse “ENTER” para continuar.  **Nota:** Deberá adaptar los parámetros a la configuración de su organización
8.	Se continua con la configuración de los usuarios y grupos necesarios. Pulsando “ENTER” se continua con la ejecución del script. 

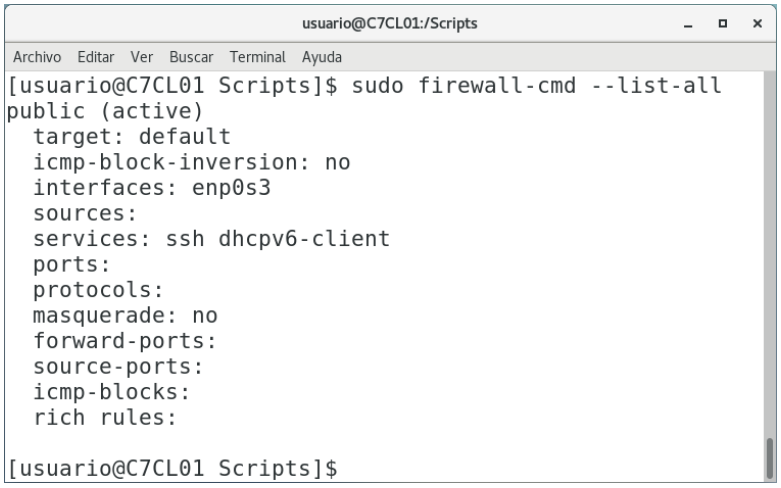
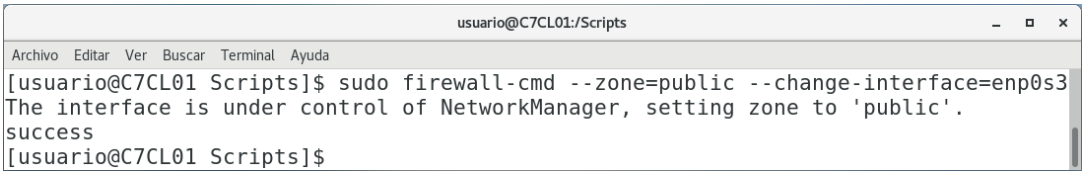
Paso	Descripción
9.	Acto seguido se comprueba la configuración.  **Nota:** El script está automatizado y la creación o modificación de los usuarios no requiere la interacción del usuario.
10.	A continuación, el script comprueba los ficheros de configuración de Spamassassin y posteriormente solicita mensaje a mostrar cuando detecte un correo de spam. Inserte el mensaje y pulse ENTER para continuar.  **Nota:** El script comentará toda configuración que posea el archivo /etc/mail/spamassasin/local.cf para su posterior configuración.

Paso	Descripción
11.	Para continuar con la configuración de la solución “ClamAV”, debe de presionar “ENTER”. 
12.	El equipo conectará con los servidores de la solución “ClamAV” para descargar las firmas de virus.  **Nota:** Este proceso puede durar varios minutos. El sistema intentará conectar con los servidores de ClamAV, si no puede conectar automáticamente probará en una réplica suya. Ignore los mensajes de error.
13.	Una vez actualizada la base de firmas de antivirus de ClamAV, pulse “ENTER” para proceder a la configuración de “Amavis”. Se añaden excepciones en los productos “Firewalld” y “Selinux”. 

Paso	Descripción
14.	Pulse “ENTER” para continuar con la comprobación de la configuración.  **Nota:** Es posible que al realizar modificaciones salga un mensaje “warning”. Éste es debido a la jaula chroot, ya que al modificar configuraciones de Postfix se advierte por pantalla en formato “warning”. `postfix/postfix-script: warning: /var/spool/postfix/etc/passwd and /etc/passwd differ`
15.	La finalización de la instalación e integración de Amavis, ClamAV y SpamAssassin en el sistema finalizará con el siguiente mensaje. 

5. FIREWALLD

Paso	Descripción
1.	Se va a proceder a revisar el estado de Firewalld, así como su configuración.
2.	Inicie sesión en el equipo CentOS 7 Linux que está asegurando, con la cuenta del grupo “wheel” creada en la instalación. 
3.	Diríjase al directorio “/Scripts”. **$ cd /Scripts**
4.	Revise el correcto estado de funcionamiento de “Firewall”, ejecutando los siguientes comandos. **$ sudo systemctl status firewalld.service** **$ sudo firewall-cmd --state** 
5.	Firewalld posee varias zonas diferenciadas de funcionamiento. Para poder comprobar en que zona se encuentra ejecute el siguiente comando. **$ firewall-cmd --get-default-zone** 

Paso	Descripción
6.	Para conocer que reglas están asociadas a dicha zona podemos usar el siguiente comando. **$ sudo firewall-cmd --list-all** 
7.	Para asignar una zona específica a una interfaz de red del equipo, deberá ejecutar el siguiente comando. **$ sudo firewall-cmd --zone=public --change-interface=enp0s3** 
8.	A continuación, se procede a realizar a modo de ejemplo la inserción del puerto 25 a la excepción de firewalld. **$ sudo firewall-cmd --zone=public --add-port=25/tcp** **$ sudo firewall-cmd --reload** **$ sudo firewall-cmd --list-services** **Nota:** Deberá adaptar los parámetros de configuración acorde a su organización. Tenga en cuenta que durante la ejecución de esta guía se utilizan en modo de ejemplo varios puertos que son necesarios para el correcto funcionamiento de los productos descritos. No es imprescindible usar los puertos específicos configurados de ejemplo, pudiendo adaptar dichos puertos a las necesidades de su organización.