

Guía de Seguridad de las TIC CCN-STIC 681A21

IMPLEMENTACIÓN DEL ENS EN POSTFIX SOBRE RED HAT 8



SEPTIEMBRE 2021



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2021
NIPO: 083-21-163-3

Fecha de Edición: septiembre de 2021

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

septiembre de 2021

A handwritten signature in blue ink, belonging to Paz Esteban López, is positioned above her name and title.

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE POSTFIX SOBRE RED HAT 8	6
ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE POSTFIX SOBRE red hat 8.....	6
1. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN POSTFIX 3.3.1-12.el8_3.1.....	6
1.1. MARCO OPERACIONAL	7
1.1.1. CONTROL DE ACCESO	7
1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN	8
1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS	8
1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO.....	8
1.1.1.4. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN	9
1.1.1.5. OP. ACC. 7. ACCESO REMOTO	9
1.1.2. EXPLOTACIÓN.....	10
1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD.....	10
1.1.2.2. OP. EXP. 4 MANTENIMIENTO.....	11
1.1.2.3. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS.....	11
1.1.2.4. OP. EXP. 9. REGISTRO DE LA GESTION DE INCIDENTES.....	11
1.1.2.5. OP. EXP. 10. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	12
1.2. MEDIDAS DE PROTECCIÓN.....	12
1.2.1. PROTECCIÓN DE LAS COMUNICACIONES.....	12
1.2.1.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD	12
1.2.1.2. MP. COM. 9. MEDIOS ALTERNATIVOS	13
1.2.1.3. MP. SI. 5. BORRADO Y DESTRUCCION	13
1.2.1.4. MP. INFO. 4. FIRMA ELECTRONICA	14
1.2.1.5. MP. S. 1. PROTECCIÓN DEL CORREO ELECTRONICO	15
1.2.1.6. MP. S. 2. PROTECCIÓN DE SERVICIOS	15
1.2.1.7. MP. S. 9. MEDIOS ALTERNATIVOS.....	16
2. RESUMEN Y APLICACIÓN DE MEDIDAS DE POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8.3.....	16
ANEXO A.2. CATEGORÍA BÁSICA.....	18
ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS	18
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR RED HAT 8 ENS CATEGORÍA BÁSICA.....	37
ANEXO A.3. CATEGORÍA MEDIA	44

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS	44
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR RED HAT 8 ENS CATEGORÍA MEDIA	69
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA.....	76
ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	76
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR REDHAT 8 ENS CATEGORÍA ALTA	106
ANEXO A.5. TAREAS ADICIONALES.....	114
ANEXO A.5.1. TAREAS DE SEGURIDAD	114
1. PAQUETES ADICIONALES	114
2. SPAMASSASSIN	118
3. AMAVIS Y CLAMAV.....	121
4. FIREWALLD.....	127
ANEXO A.5.2. TAREAS DE MANTENIMIENTO	129
1. AUTOMATIZACIÓN DE ACTUALIZACIONES	130
2. PFLOGSUMM.....	131

ANEXO A. CONFIGURACIÓN SEGURA DE POSTFIX SOBRE RED HAT 8

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE POSTFIX SOBRE RED HAT 8

1. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN POSTFIX 3.3.1-12.el8_3.1

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 uso 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 Red Hat 8 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 Red Hat 8 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 Red Hat 8.

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 Red Hat 8, 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 ilegítima 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 RED HAT 8.3, 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 Red Hat 8, 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 interceptación 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 3.3.1-12.el8_3.1, 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 3.3.1-12.el8_3.1 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 3.3.1-12.el8_3.1, 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 3.3.1-12.el8_3.1 SOBRE RED HAT 8.3

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-681A21, adaptándolos a la organización.
OP. ACC. 3	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
OP. ACC. 5	Mecanismos de autenticación	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación de guía CCN-STIC-681A21, 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-681A21, adaptándolos a la organización.
OP. EXP. 4	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-681A21, 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-681A21, adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación y de la integridad	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. COM. 9	Medios alternativos	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. SI. 5	Borrado y destrucción de la información	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. INFO. 3	Cifrado de la información	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. INFO. 4	Firma electrónica de la información	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. S. 1	Protección del correo electrónico	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. S. 2	Protección de servicios	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.
MP. S. 9	Medios alternativos	Revisión e implementación de guía CCN-STIC-681A21, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8 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 3.3.1-12.el8_3.1 sobre un servidor Red Hat 8, 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 3.3.1-12.el8_3.1 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.

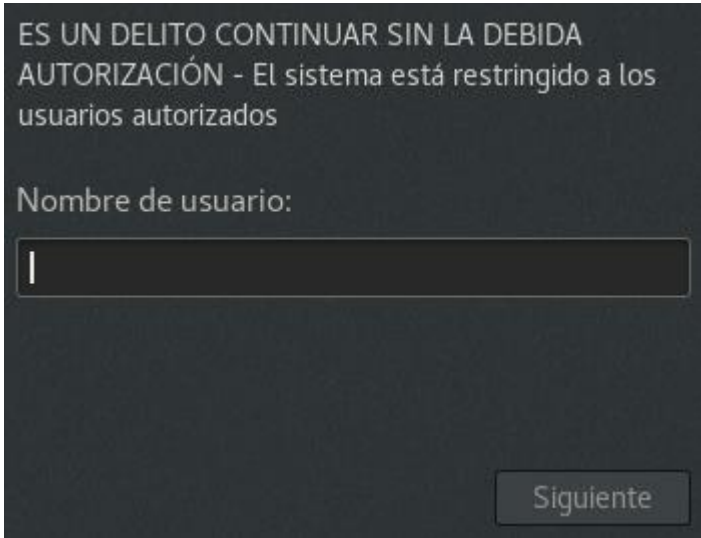
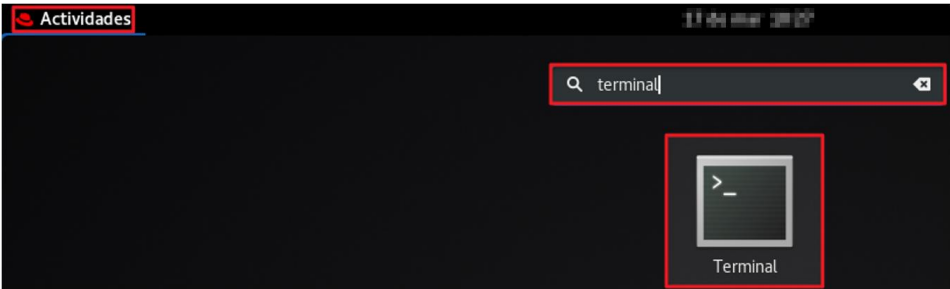
<http://www.postfix.org/features.html#fs-requirements>

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 las guías "CCN-STIC".

Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando.

- **\$ sudo setenforce 0**

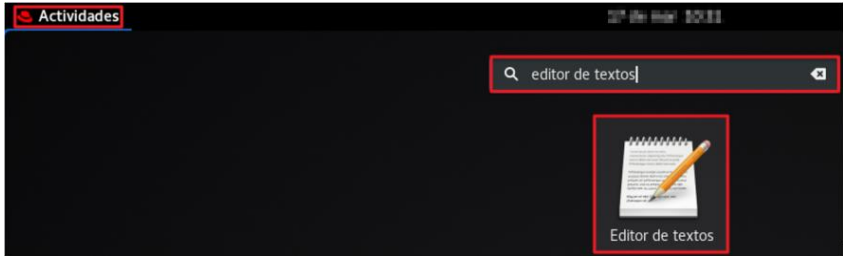
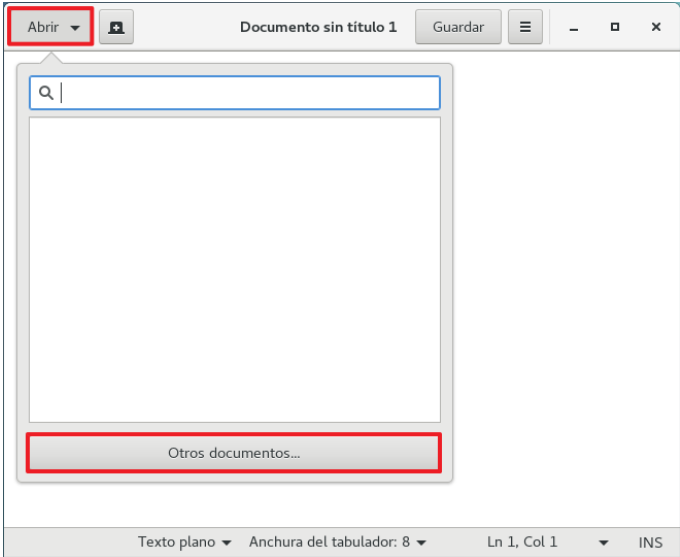
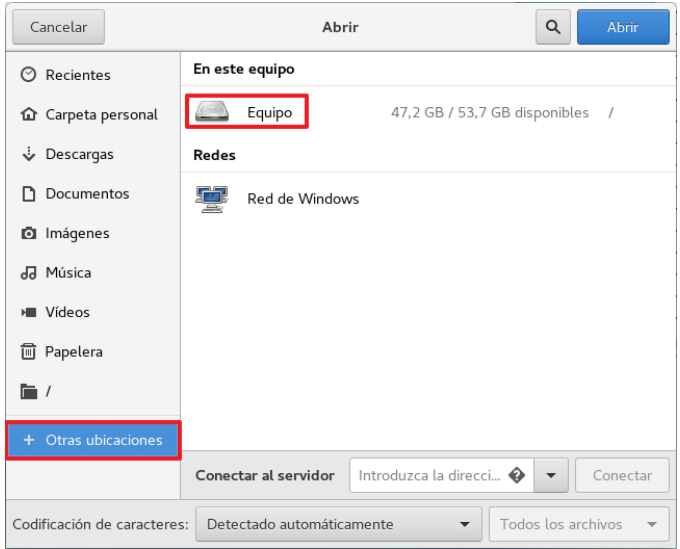
Deberá adaptar los parámetros de configuración de firewalld acorde a su organización. Tenga en cuenta que en esta guía se utilizan, a modo de ejemplo, varios puertos, que es necesario que estén abiertos para el correcto funcionamiento de los productos descritos.

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 "Actividades", escriba y seleccione "Terminal". 
3.	Cree la carpeta "Scripts". Para ello, en el terminal, ejecute el comando siguiente. <pre>\$ cd /</pre> Para crear la carpeta en la ubicación ejecute el siguiente comando. <pre>\$ sudo mkdir Scripts</pre> Nota: Puede comprobar que la carpeta ha sido creada ejecutando <code>ls /</code>.
4.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía "CCN-STIC-681- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE RED HAT 8 LINUX". Introduzca las credenciales si se lo solicita.

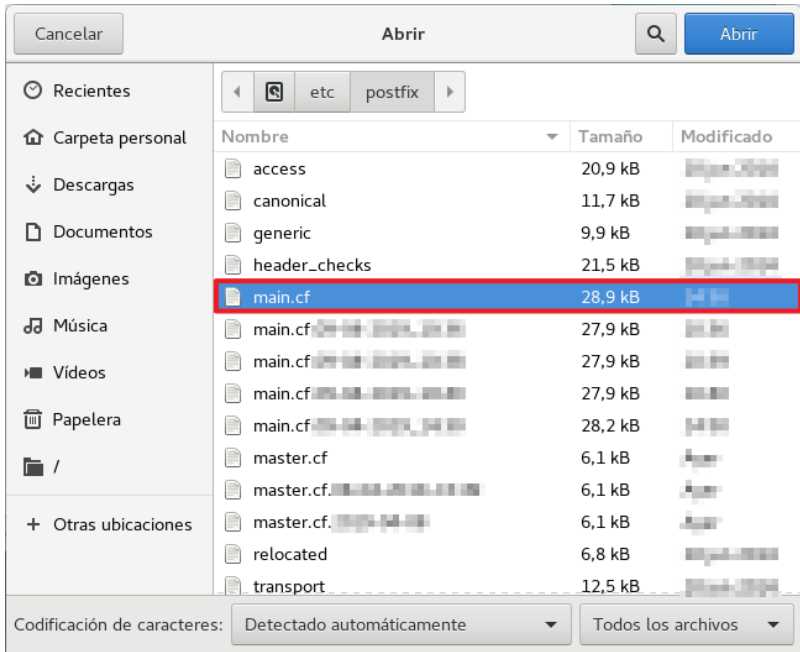
Paso	Descripción
5.	Copie el contenido de la carpeta con la categoría de seguridad “CATEGORIA_BASICA” correspondiente al directorio “Scripts/ENS_BASICA” asociado a esta guía en la ruta “/Scripts”. Para ello, ejecute el comando siguiente. <pre>\$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_BASICA/* /Scripts/</pre> 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.
6.	Expulse el CD/DVD de la unidad y diríjase a la carpeta “Scripts”. Para ello ejecute el comando siguiente. <pre>cd /Scripts</pre>
7.	Ejecute el siguiente comando. Introduzca la contraseña del usuario para continuar. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso1_comprobacion_paquetes_necesarios.sh</pre> 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.
8.	Pulse “ENTER” para continuar. <pre>----- -- CCN-STIC-681A21-POSTFIX-PASO 1 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>

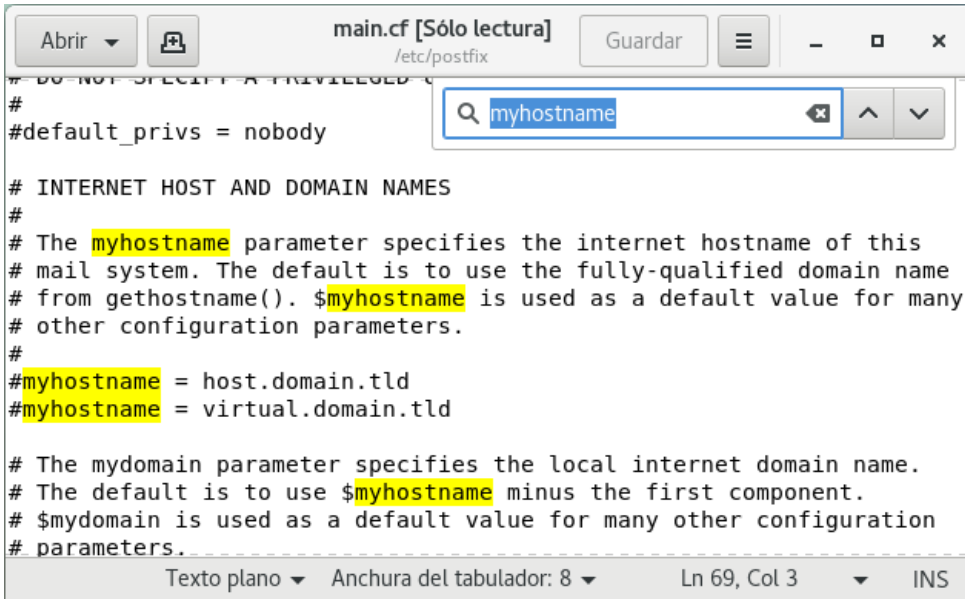
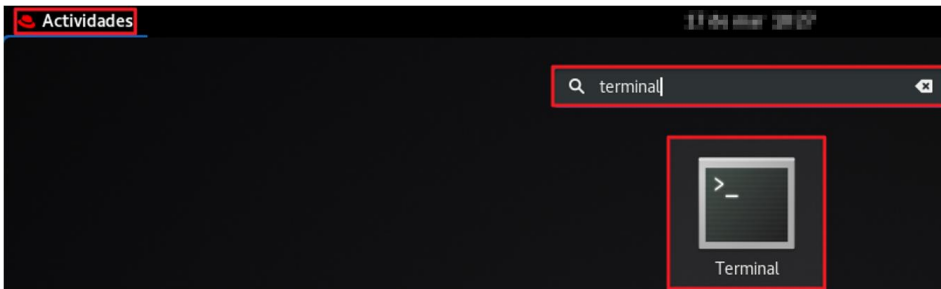
Paso	Descripción
9.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar. <pre> ----- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... postfix-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix Instalado gnupg2-2.2.20-2.el8.x86_64 gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2 Instalado Debe instalar gnupg2-smime </pre> Nota: Los resultados mostrados en pantalla pueden variar dependiendo de las configuraciones específicas de su organización.
10.	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”. <pre> ----- SE COMPROBARAN PROGRAMAS INNECESARIOS ----- Pulse ENTER para continuar o Ctrl + C para cancelar... NO HAY PROGRAMAS INNECESARIOS ----- ---- CONFIGURACION TERMINADA ---- ----- </pre>
11.	Instale o actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. <pre> \$ sudo yum install <Paquete1 Paquete2 Paquete 3 ...> \$ sudo yum update <Paquete1 Paquete2 Paquete 3 ...> \$ sudo yum remove <Paquete1 Paquete2 Paquete 3 ...> </pre> <pre> [usuario@RHEL8-SI01 ENS_BASICA]\$ sudo yum install gnupg2-smime </pre>

Paso	Descripción
12.	Ejecute el script de nuevo para comprobar que la configuración es correcta. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso1_comprobacion_paquetes_necesarios.sh</pre> <pre>python3-pyOpenSSL-18.0.0-1.el8.noarch perl-Crypt-OpenSSL-Random-0.15-3.el8.x86_64 openssl Instalado postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts Instalado epel-release-8-10.el8.noarch epel-release-7-11.noarch Instalado pypolicyd-spf-2.0.2-7.el8.noarch pypolicyd-spf Instalado ----- ----- SE COMPROBARAN PROGRAMAS INNECESARIOS ----- ----- Pulse ENTER para continuar o Ctrl + C para cancelar. .. NO HAY PROGRAMAS INNECESARIOS ----- ---- CONFIGURACION TERMINADA ---- -----</pre>
13.	Por motivos de seguridad preservando los datos y configuraciones de su organización, se 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. <pre>\$ 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</pre> 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.

Paso	Descripción
14.	Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “editor de textos”. 
15.	Diríjase a la esquina superior izquierda del editor de textos y pulse sobre “Abrir” y en “Otros documentos...”. 
16.	Deberá pulsar sobre “+ Otras Ubicaciones” y posteriormente sobre “Equipo”. 

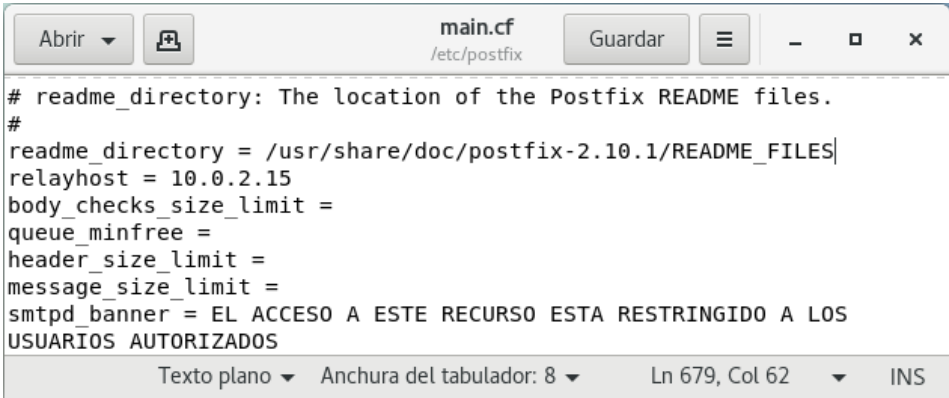
Paso	Descripción
17.	Ingrese a la carpeta “etc”.
	The screenshot shows a file manager window titled "Abrir". On the left sidebar, there are various locations like "Recientes", "Carpeta personal", "Descargas", etc., and the "/" (root) location is selected. The main pane displays a list of files and folders in the root directory. The folders listed include bin, boot, dev, etc, home, lib, lib64, media, mnt, opt, proc, root, run, and/sbin. The "etc" folder is highlighted with a red rectangle.
18.	Ingrese en la carpeta “postfix”.
	This screenshot shows the same file manager window after navigating into the "etc" directory. The breadcrumb at the top indicates the current path is "etc". The main pane now lists the contents of the "/etc" directory, which includes several configuration files and folders. The "postfix" folder is highlighted with a red rectangle.

Paso	Descripción
19.	Ejecute el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón. 
20.	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.

Paso	Descripción
21.	Por ser un archivo de configuración muy extenso, se recomienda pulsar “CTRL + f” y buscar el término deseado. 
22.	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. 
23.	Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “Terminal”. 

Paso	Descripción
24.	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. <pre>\$ 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</pre> 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.
25.	Diríjase a la carpeta “Scripts”. Para ello ejecute el comando siguiente. <pre>\$ cd /Scripts</pre>
26.	Se procede a configurar el fichero “main.cf” para ello, ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso2_configuracion_main.cf.sh</pre>
27.	Para continuar con la ejecución del script, pulse “ENTER”. <pre>----- -- CCN-STIC-681A21-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.....</pre>

Paso	Descripción
28.	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. <pre> ----- -- 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 AL SISTEMA ESTA RESTRINGIDO A USUARIOS AUTORIZADOS </pre> 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.
29.	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 AL SISTEMA ESTA RESTRINGIDO A USUARIOS AUTORIZADOS banner Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>

Paso	Descripción																		
30.	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.  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>	Parámetro	Valor	body_checks_size_limit =	65536	queue_minfree =	20971520	header_size_limit =	1024	message_size_limit =	65536	Parámetro	Valor	Mydomain =	<Su dominio>	Myhostname =	<El nombre del servidor>	Myorigin =	<Su dominio>
Parámetro	Valor																		
body_checks_size_limit =	65536																		
queue_minfree =	20971520																		
header_size_limit =	1024																		
message_size_limit =	65536																		
Parámetro	Valor																		
Mydomain =	<Su dominio>																		
Myhostname =	<El nombre del servidor>																		
Myorigin =	<Su dominio>																		
31.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 																		
32.	La configuración termina con la salida del proceso de configuración y el mensaje de finalización del mismo.																		
33.	Se procede a comprobar la configuración de Postfix. Para ello ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso3_comprobacion_configuracion.sh</pre>																		

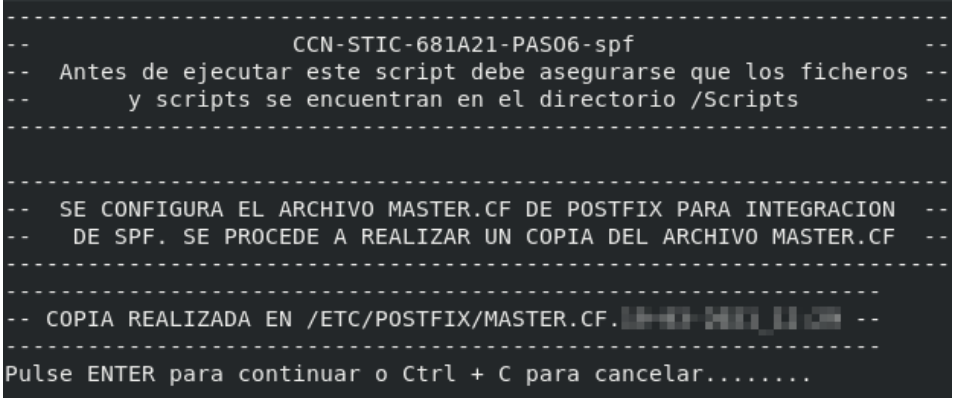
Paso	Descripción
34.	El script iniciará el proceso de verificación de acceso y pertenencia de los archivos y carpetas necesarias para el correcto funcionamiento seguro de Postfix. Pulse “ENTER” para continuar. <pre> ----- -- CCN-STIC-681A21-POSTFIX-PASO 3 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE COMPROBARA LA INTEGRIDAD DE LOS FICHEROS Y CARPETAS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre> Nota: No pulse ningún botón ni cierre la ventana hasta que finalice el script.
35.	En la salida del script, mostrará los archivos y carpetas necesarios para el correcto funcionamiento de Postfix y las recomendaciones pertinentes. <pre> -rw-r--r--. 1 root root 3961 mar 10 17:42 /etc/postfix/main.cf main.cf SI pertenece a root Correcto -rw-r--r--. 1 root root 3961 mar 10 17:42 /etc/postfix/main.cf main.cf Permisos de acceso CORRECTOS Correcto -rw-r--r--. 1 root root 640 mar 9 14:40 /etc/postfix/master.cf master.cf SI pertenece a root Correcto -rw-r--r--. 1 root root 640 mar 9 14:40 /etc/postfix/master.cf master.cf Permisos de acceso CORRECTOS Correcto drwxr-xr-x. 20 root root 347 mar 8 10:34 postfix /var/spool/postfix SI pertenece a root Correcto drwxr-xr-x. 20 root root 347 mar 8 10:34 postfix /var/spool/postfix Permisos de acceso CORRECTOS Correcto -rw-rw----. 1 root monitorizacion 5,1K mar 10 17:05 /var/log/maillog /var/log/maillog SI pertenece a root Correcto /var/log/maillog Permisos de acceso CORRECTOS Correcto </pre> 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.

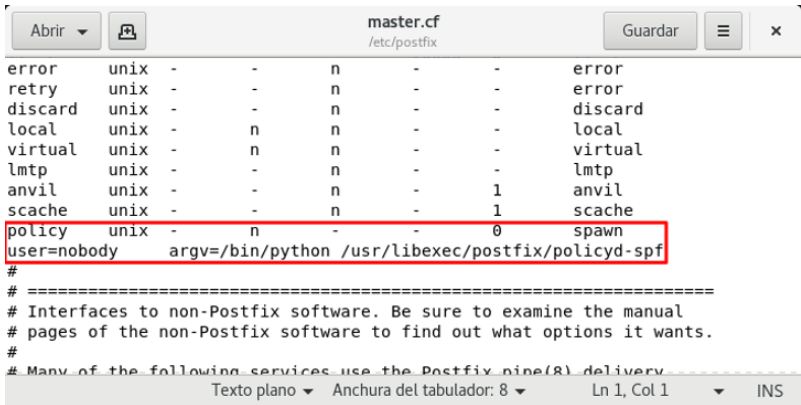
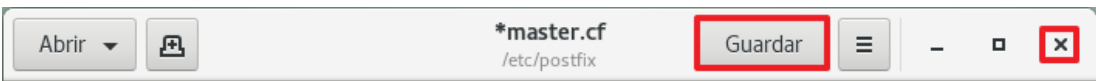
Paso	Descripción
36.	El Script continua con la comprobación de los usuarios y grupos necesarios para el correcto funcionamiento de Postfix de forma segura. Deberá pulsar “ENTER” para continuar. <pre> -- SE VA A PROCEDER A LA COMPROBACION DE USUARIOS Y GRUPOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... mail:x:12:postfix postdrop:x:90: postfix:x:89: Grupos existentes Correcto vboxadd:x:976:1::/var/run/vboxadd:/bin/false postfix:x:89:89::/var/spool/postfix:/bin/false spamd:x:1001:1002::/var/log/spamassassin:/bin/false Usuario existente y configurado correctamente Correcto </pre> 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.
37.	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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso4_certificados_openSSL.sh</pre> 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.
38.	Se procederá a crear la clave privada RSA. Deberá dar un nombre al fichero “.key” y pulsar “ENTER” para continuar. <pre> ----- -- CCN-STIC-681A21-POSTFIX-PASO 4 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE PROCEDE A CREAR UN CERTIFICADO AUTO-FIRMADO SSL -- ----- Nombre de llave privada: CLAVEPRIVADA </pre>

Paso	Descripción
39.	Posteriormente introduzca un nombre para el fichero CSR (solicitud de firma de certificado) que se generará posteriormente. Pulse “Enter” para continuar. <pre>-- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE PROCEDE A CREAR UN CERTIFICADO AUTO-FIRMADO SSL -- ----- Nombre de llave privada: CLAVEPRIVADA Nombre Certificado de firma: NOMBREFIRMA</pre>
40.	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. <pre>Generating RSA private key, 2096 bit long modulus (2 primes) .++++++++++ e is 65537 (0x010001) Enter pass phrase for CLAVEPRIVADA.key: Verifying - Enter pass phrase for CLAVEPRIVADA.key: Enter pass phrase for CLAVEPRIVADA.key:</pre>
41.	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. <pre>What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country Name (2 letter code) [XX]:ES State or Province Name (full name) []:Madrid Locality Name (eg, city) [Default City]:Madrid Organization Name (eg, company) [Default Company Ltd]:Organizacion Organizational Unit Name (eg, section) []:opcional Organizacion Common Name (eg, your name or your server's hostname) []:RHEL8-SI01 Email Address []:correo@organizacion.es Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:password An optional company name []:Organizacion</pre> Nota: Deberá pulsar “ENTER” para que los datos queden introducidos en la información del certificado.

Paso	Descripción
42.	Continúe con el proceso nombrando el certificado. Cuando finalice pulse “ENTER”. <pre>Nombre de certificado auto-firmado: RHEL08</pre>
43.	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. <pre>Signature ok subject=C = ES, ST = Madrid, L = Madrid, O = Organizacion, OU = opcional Organizacion, CN = RHEL8-SI01, emailAddress = correo@organizacion.es Getting Private key Enter pass phrase for CLAVEPRIVADA.key: ----- ---- CONFIGURACION TERMINADA ---- -----</pre>
44.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso5_Seguridad.sh</pre>
45.	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”. <pre>----- -- CCN-STIC-681A21-POSTFIX-PASO 5 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE REALIZARA UNA COPIA DE SEGURIDAD DEL ARCHIVO MAIN.CF -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>
46.	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. <pre>----- -- SE REALIZARA UNA COPIA DE SEGURIDAD DEL ARCHIVO MAIN.CF -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... - COPIA DE SEGURIDAD REALIZADA EN /ETC/POSTFIX/MAIN.CF.13-03-2021_13:50 - ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... -- SE PROCEDERA A CONFIGURAR EL ARCHIVO MAIN.CF -- -- PARA EL USO DE SSL Y TLS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>

Paso	Descripción																																		
47.	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.  <pre> ##### ### VALORES DE SEGURIDAD ### ##### CCN-STIC-681A21 ##### ##### smtpd_sasl_auth_enable = yes broken_sasl_auth_clients = yes #smtpd_sasl_type = smtpd_sasl_path = private/auth smtpd_sasl_security_options = noanonymous smtpd_recipient_restrictions = permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination,reject_unauth_destination,permit_auth_destination smtp_use_tls = yes smtp_tls_mandatory_protocols = !SSLv2,!SSLv3, !TLSv1 smtpd_tls_cert_file = /etc/ssl/certs/RHEL08SI01.organizacion.es.crt smtpd_tls_key_file = /etc/ssl/certs/organizacion.key 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 </pre>	Parámetro	Valor	smtpd_sasl_auth_enable =	yes	broken_sasl_auth_clients =	yes	#smtpd_sasl_type =		smtpd_sasl_path =	private/auth	smtpd_sasl_security_options =	noanonymous	smtpd_recipient_restrictions =	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, reject_unauth_destination, permit_auth_destination	smtp_use_tls =	yes	smtp_tls_mandatory_protocols =	!SSLv2, !SSLv3, !TLSv1	smtpd_tls_cert_file =	/etc/ssl/certs/<certificado>	smtpd_tls_key_file =	/etc/ssl/certs/<certificado>	smtpd_tls_session_cache_database =	btree:/etc/postfix/smtpd_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
Parámetro	Valor																																		
smtpd_sasl_auth_enable =	yes																																		
broken_sasl_auth_clients =	yes																																		
#smtpd_sasl_type =																																			
smtpd_sasl_path =	private/auth																																		
smtpd_sasl_security_options =	noanonymous																																		
smtpd_recipient_restrictions =	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, reject_unauth_destination, permit_auth_destination																																		
smtp_use_tls =	yes																																		
smtp_tls_mandatory_protocols =	!SSLv2, !SSLv3, !TLSv1																																		
smtpd_tls_cert_file =	/etc/ssl/certs/<certificado>																																		
smtpd_tls_key_file =	/etc/ssl/certs/<certificado>																																		
smtpd_tls_session_cache_database =	btree:/etc/postfix/smtpd_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																																		

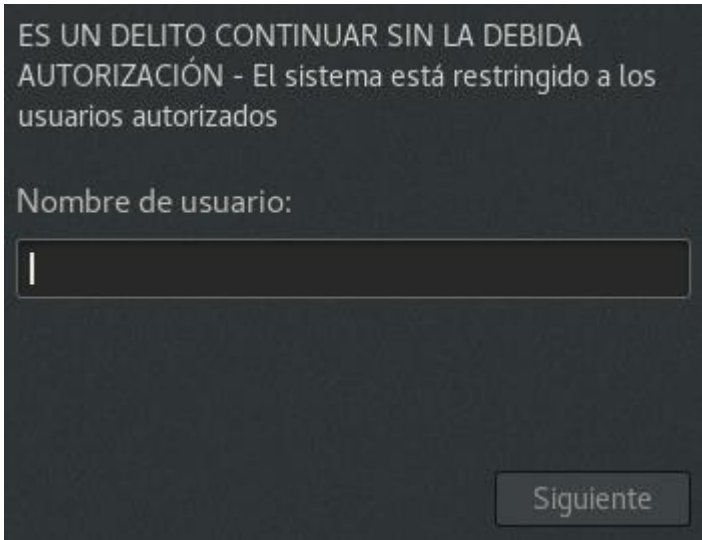
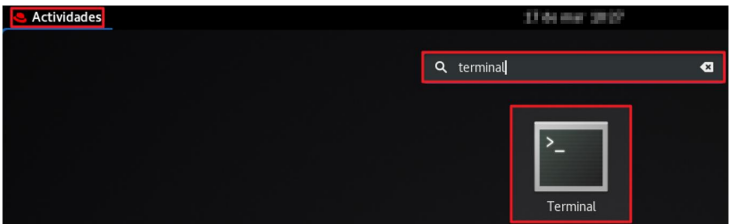
Paso	Descripción
48.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
49.	El script finalizará mostrando el mensaje “CONFIGURACION TERMINADA”. 
50.	Se procede a realizar una la integración de SPF sobre Postfix. Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. <pre>\$ sudo sh CCN-STIC-681A21_ENS_BASICA_Paso6_spf.sh</pre> 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.
51.	Para ello, primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar “ENTER” para continuar. 

Paso	Descripción
52.	El script editará el fichero master.cf. Inserte la siguiente línea en “master.cf” para configurar SPF. <pre>policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf</pre>  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.
53.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
54.	El proceso finaliza con el siguiente mensaje, realizándose una comprobación de sintaxis de Postfix. <pre>configuracion de postfix Correcta ----- ---- CONFIGURACION TERMINADA ---- -----</pre>
55.	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. <pre>\$ sudo systemctl unmask postfix.service \$ sudo systemctl start postfix.service \$ sudo systemctl enable postfix.service</pre>
56.	Elimine la carpeta “/Scripts” y todo su contenido.
57.	Guarde las aplicaciones que se encuentren abiertas y reinicie el servidor. <pre>\$ sudo shutdown -r</pre>

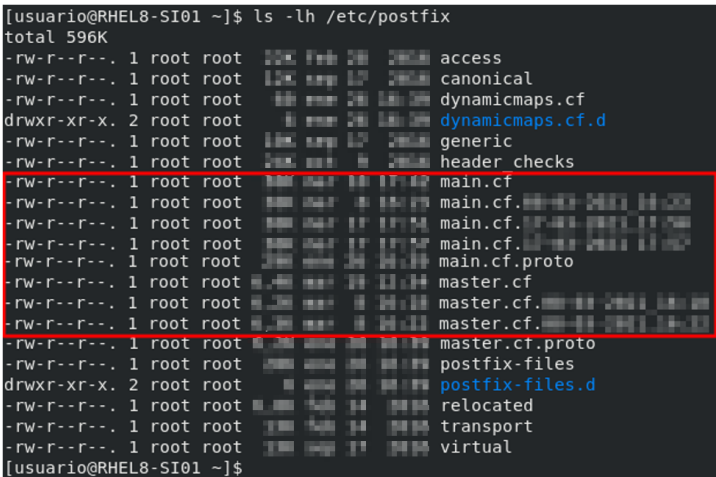
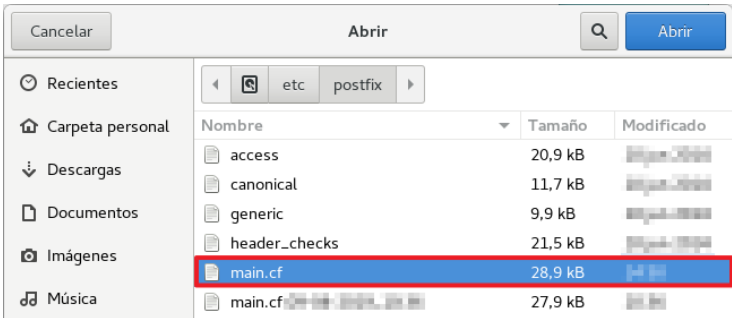
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR RED HAT 8 ENS CATEGORÍA BÁSICA

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.

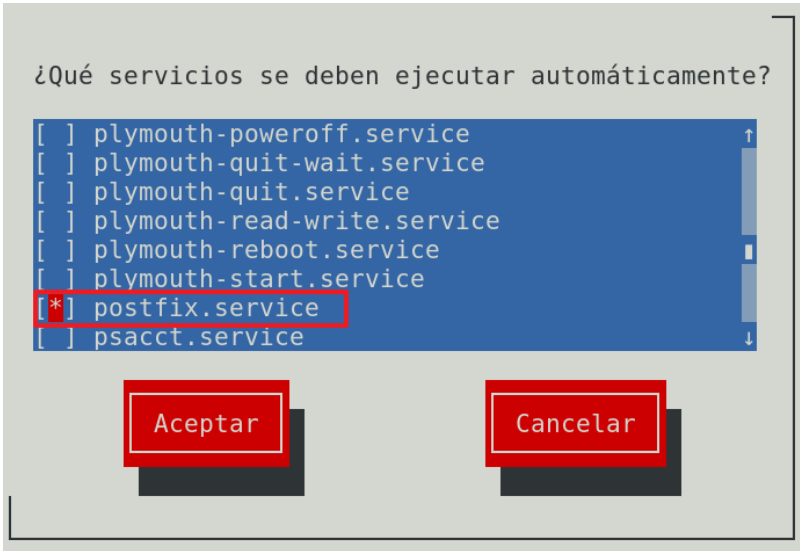
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En uno de los servidores Red Hat 8, inicie sesión con una cuenta que tenga privilegios de administración. 
2. Inicie la Terminal de Linux.		Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “Terminal”. 

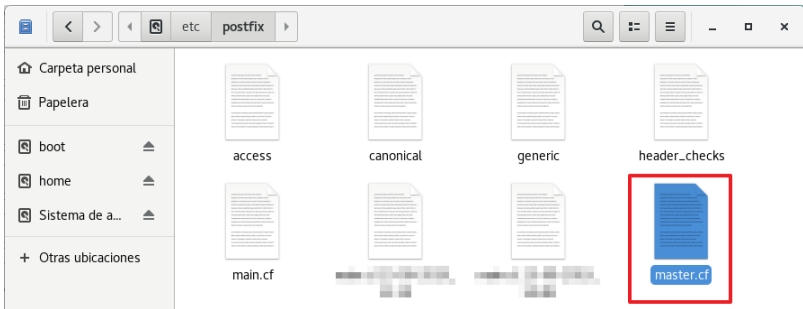
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que se encuentren instalados los paquetes necesarios.		En la “terminal” ejecute el siguiente comando. <pre>\$ sudo rpm -aq egrep 'gnupg2 gnupg2-smime openssl pypolicyd-spf postfix'</pre> <pre>[usuario@RHEL8-SI01 ~]\$ sudo rpm -aq egrep 'gnupg2 gnupg2-smime openssl pypolicyd-spf postfix'</pre> <pre>postfix-3.3.1-12.el8_3.1.x86_64 gnupg2-2.2.20-2.el8.x86_64 gnupg2-smime-2.2.20-2.el8.x86_64 openssl-pkcs11-0.4.10-2.el8.x86_64 openssl-libs-1.1.1g-12.el8_3.x86_64 pypolicyd-spf-2.0.2-7.el8.noarch xmlsec1-openssl-1.2.25-4.el8.x86_64 openssl-1.1.1g-12.el8_3.x86_64 postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 [usuario@RHEL8-SI01 ~]\$</pre> Nota: Deberá comprobar que las versiones de los paquetes que aquí se comprueban, se encuentran en sus últimas versiones.
		Parámetros
		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]
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
		ls /home/usuario/BACKUP/ egrep "main.cf"
		ls /home/usuario/BACKUP/ egrep "master.cf"

Comprobación	OK/NOK	Cómo hacerlo
5. Copias de seguridad de la organización		En un terminal ejecute el siguiente comando. <pre>\$ ls -lh /etc/postfix</pre> Revise que se han realizado las correspondientes copias de seguridad de los archivos según la ejecución de los scripts correspondientes.  <pre>[usuario@RHEL8-SI01 ~]\$ ls -lh /etc/postfix total 596K -rw-r--r--. 1 root root 12K Feb 28 20:08 access -rw-r--r--. 1 root root 12K May 27 20:08 canonical -rw-r--r--. 1 root root 8K May 28 20:08 dynamicmaps.cf drwxr-xr-x. 2 root root 8K May 28 20:08 dynamicmaps.cf.d -rw-r--r--. 1 root root 8K May 27 20:08 generic -rw-r--r--. 1 root root 20K May 28 20:08 header_checks -rw-r--r--. 1 root root 8K May 28 20:08 main.cf -rw-r--r--. 1 root root 8K May 28 20:08 main.cf.[FECHA] -rw-r--r--. 1 root root 8K May 28 20:08 main.cf.[FECHA] -rw-r--r--. 1 root root 8K May 28 20:08 main.cf.[FECHA] -rw-r--r--. 1 root root 20K May 28 20:08 main.cf.proto -rw-r--r--. 1 root root 8K May 28 20:08 master.cf -rw-r--r--. 1 root root 8K May 28 20:08 master.cf.[FECHA] -rw-r--r--. 1 root root 8K May 28 20:08 master.cf.[FECHA] -rw-r--r--. 1 root root 8K May 28 20:08 master.cf.proto -rw-r--r--. 1 root root 8K May 28 20:08 postfix-files drwxr-xr-x. 2 root root 8K May 28 20:08 postfix-files.d -rw-r--r--. 1 root root 8K May 28 20:08 relocated -rw-r--r--. 1 root root 8K May 28 20:08 transport -rw-r--r--. 1 root root 8K May 28 20:08 virtual [usuario@RHEL8-SI01 ~]\$</pre> 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.

Comprobación	OK/NOK	Cómo hacerlo	
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	
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		btrees:/etc/postfix/smttd_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	

Comprobación	OK/NOK	Cómo hacerlo		
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. <pre>\$ 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</pre>		
		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. <pre>\$ 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\-----'</pre>		
		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. <pre>\$ cat /etc/passwd egrep "postfix /bin/false" \$ cat /etc/group egrep "postfix postdrop"</pre>		
		Configuración	Valor	OK/NOK
		Usuario: postfix	Existe	
		Shell: postfix	/bin/false	
		Grupo: postfix	Existe	
		Grupo: postdrop	Existe	

Comprobación	OK/NOK	Cómo hacerlo		
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	
11.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	

Comprobación	OK/NOK	Cómo hacerlo
12. Configuración del archivo master.cf		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". 
	Parámetros	
		policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8 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 3.3.1-12.el8_3.1 sobre Red Hat 8, 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 3.3.1-12.el8_3.1 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.

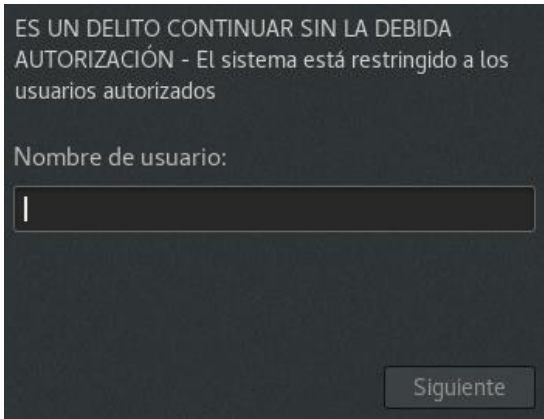
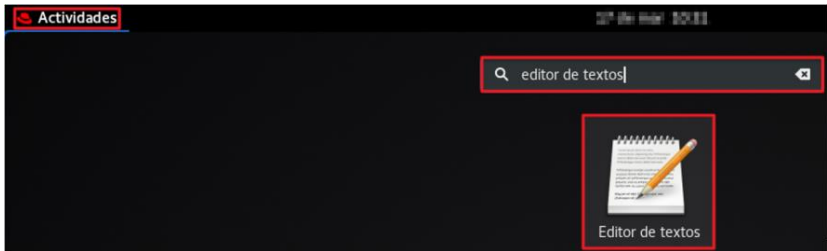
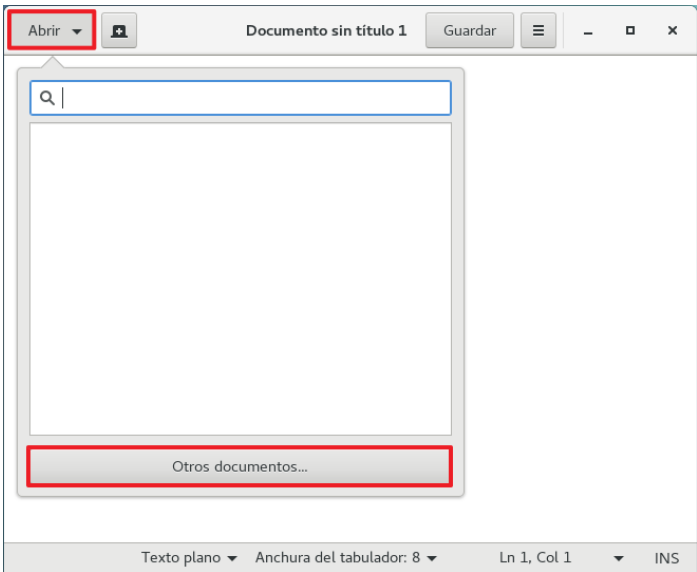
<http://www.postfix.org/features.html#fs-requirements>

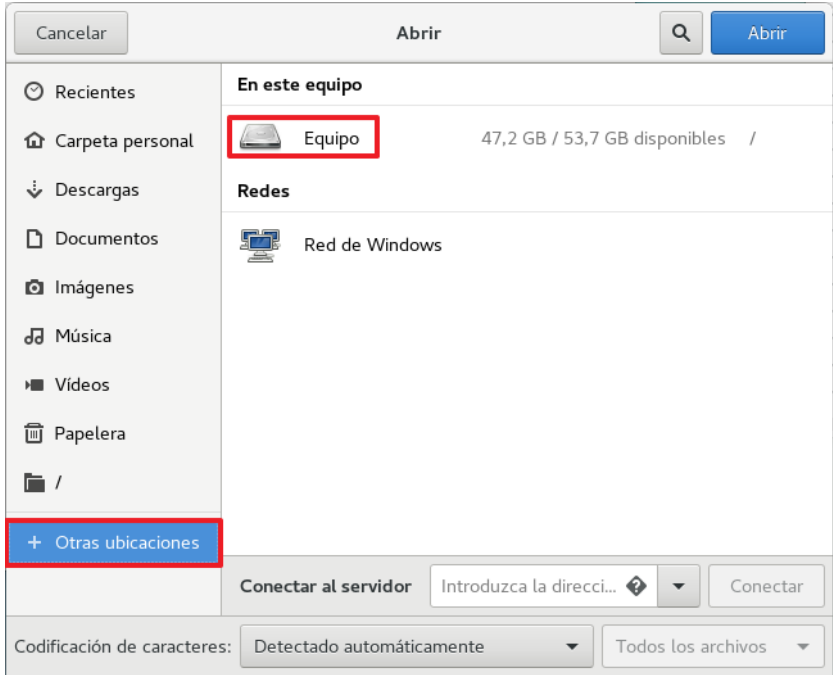
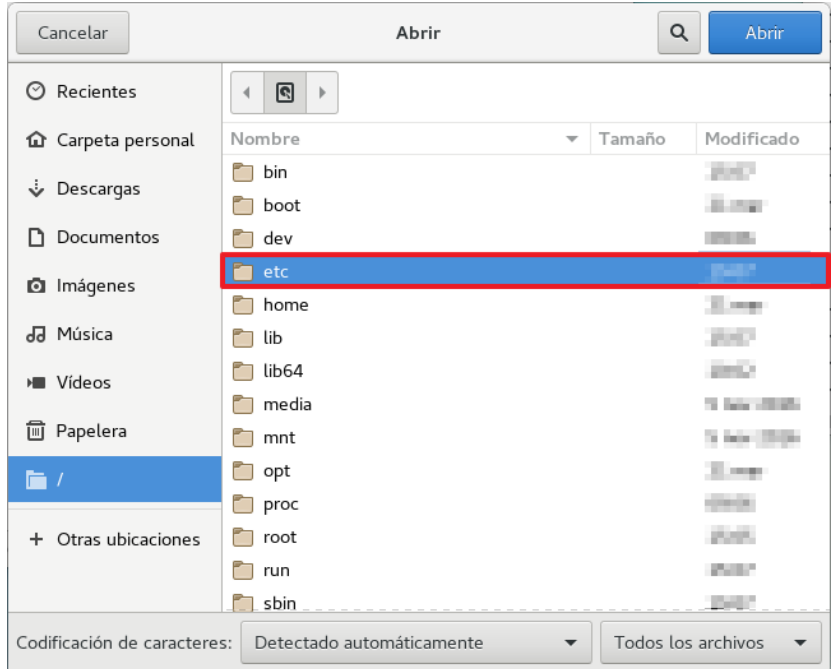
Nota: La instalación de Postfix se debe realizar en un volumen que debe haber sido formateado previamente con el formato XFS, formato que permite la aplicación de ACL's. Así mismo, antes de proceder a instalar las diferentes funcionalidades y complementos de Postfix, se debe haber reiniciado el servidor 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 las guías "CCN-STIC".

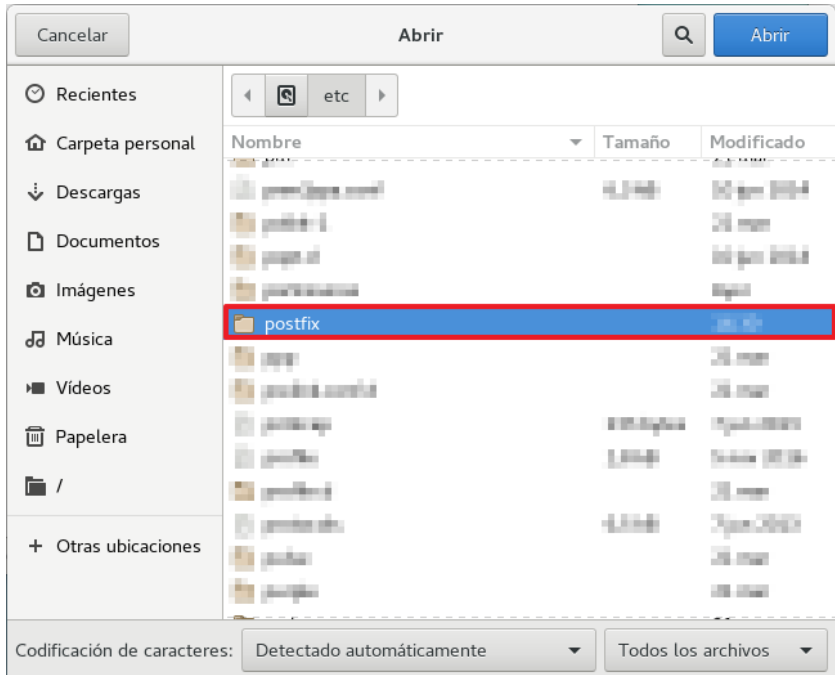
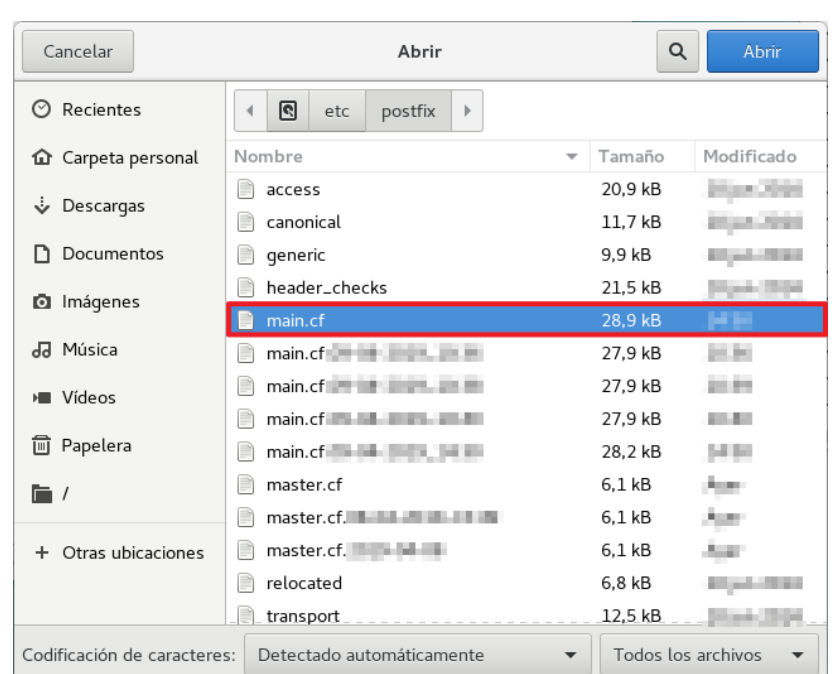
Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando.

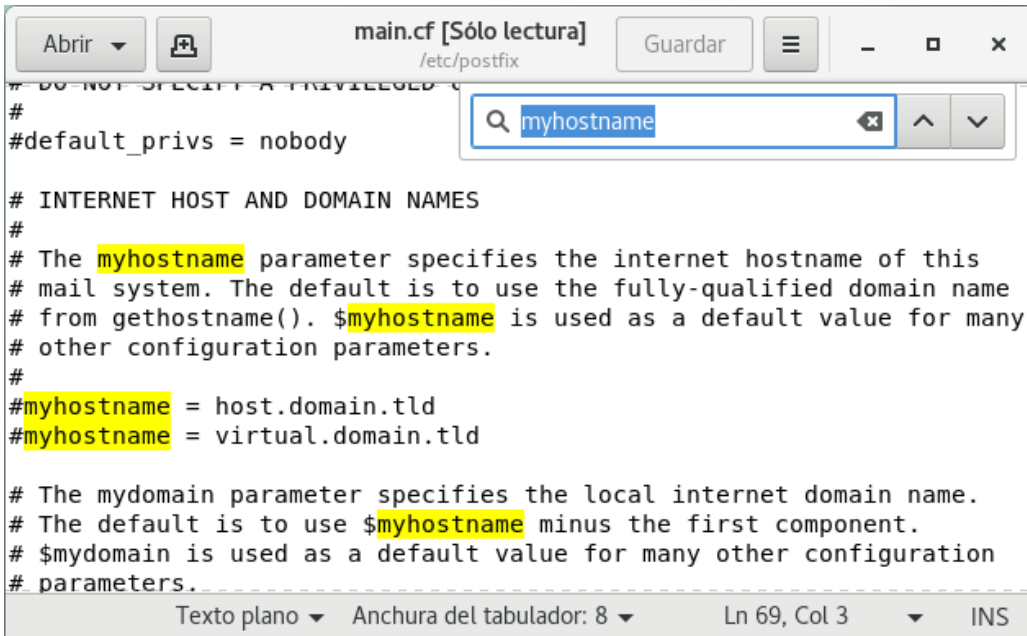
- **\$ sudo setenforce 0**

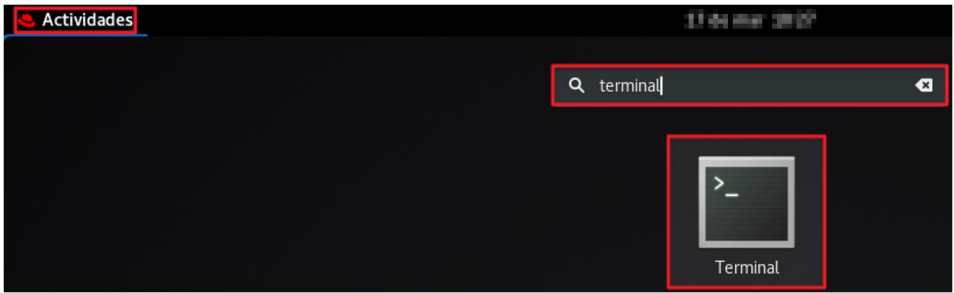
Deberá adaptar los parámetros de configuración de firewalld acorde a su organización. Tenga en cuenta que en esta guía se utilizan, a modo de ejemplo, varios puertos, que es necesario que estén abiertos para el correcto funcionamiento de los productos descritos.

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 “Actividades”, escriba y 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.	Ingresa a la carpeta “etc”. 

Paso	Descripción
6.	Ingrese en la carpeta “postfix”.  The screenshot shows a file manager window with the title 'Abrir'. On the left sidebar, the 'postfix' directory is selected. The main pane displays a list of files and directories. The 'postfix' directory is highlighted with a red box. The list includes files like 'access', 'canonical', 'generic', 'header_checks', 'main.cf', 'master.cf', 'relocated', and 'transport'.
7.	Ejecute el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón.  The screenshot shows the same file manager window, but now the 'main.cf' file is selected and highlighted with a red box. The left sidebar remains the same, and the main pane shows the contents of the 'postfix' directory.

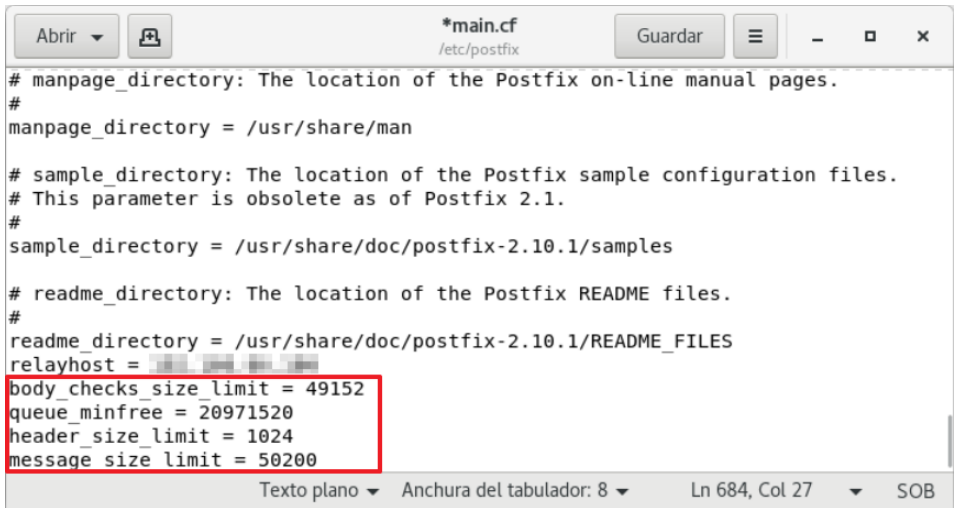
Paso	Descripción
8.	A continuación, se muestran los parámetros a modificar. Estos parámetros responden a una configuración de tipo “parámetro=valor”, utilizando el símbolo “dólar” (\$) para exportarlo globalmente en todo el fichero. – Myhostname = Nombre del servidor MTA Postfix. – Mydomain = Nombre 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.  <pre> # DO NOT SPECIFY A PRIVILEGED USER OR GROUP # #default_privs = nobody # INTERNET HOST AND DOMAIN NAMES # # The myhostname parameter specifies the internet hostname of this # mail system. The default is to use the fully-qualified domain name # from gethostname(). \$myhostname is used as a default value for many # other configuration parameters. # #myhostname = host.domain.tld #myhostname = virtual.domain.tld # The mydomain parameter specifies the local internet domain name. # The default is to use \$myhostname minus the first component. # \$mydomain is used as a default value for many other configuration # parameters. </pre>
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. 

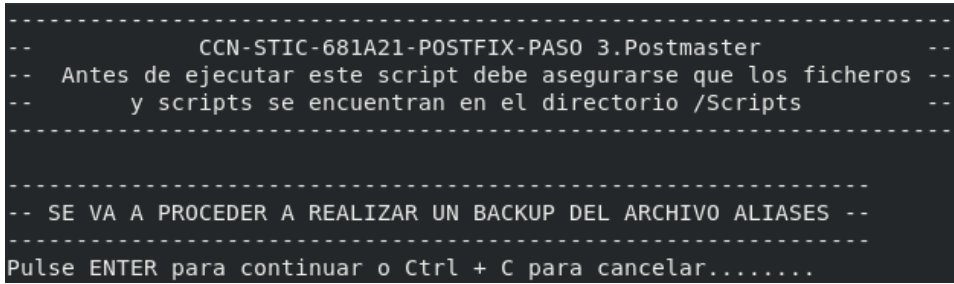
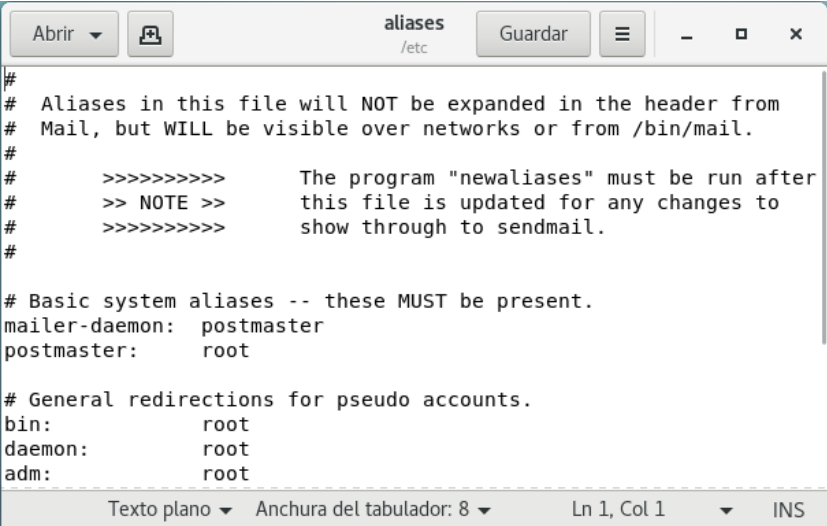
Paso	Descripción
11.	Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “Terminal”. 
12.	Cree la carpeta “Scripts”. Para ello, en el terminal, ejecute el comando siguiente. <pre>\$ cd /</pre> Para crear la carpeta en la ubicación ejecute el siguiente comando. <pre>\$ sudo mkdir Scripts</pre> Nota: Puede comprobar que la carpeta ha sido creada ejecutando <code>ls /</code>.
13.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía “CCN-STIC-681A21- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE RED HAT 8 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”. Para ello, ejecute el comando siguiente. <pre>\$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_MEDIA/* /Scripts/</pre> 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. <pre>\$ cd /Scripts</pre>
16.	Ejecute el siguiente comando. Introduzca la contraseña del usuario para continuar. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso1_comprobacion_paquetes_necesarios.sh</pre> 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.

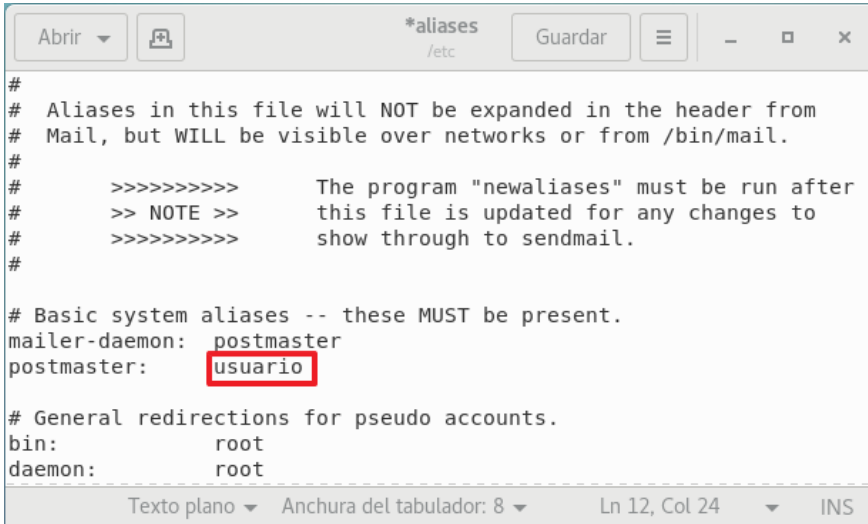
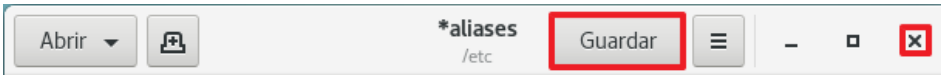
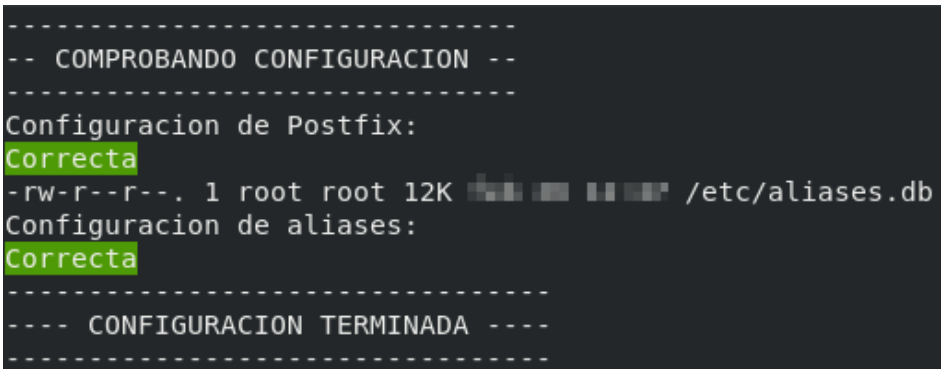
Paso	Descripción
17.	Pulse “ENTER” para continuar. <pre> ----- -- CCN-STIC-681A21-POSTFIX-PASO 1 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
18.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar. <pre> ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... postfix-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix Instalado gnupg2-2.2.20-2.el8.x86_64 gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2 Instalado Debe instalar gnupg2-smime </pre> 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”. <pre> ----- -- SE COMPROBARAN PROGRAMAS INNECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar... NO HAY PROGRAMAS INNECESARIOS ----- -- CONFIGURACION TERMINADA -- ----- </pre>
20.	Instale, actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. <pre> \$ sudo yum install <Paquete1 Paquete2 Paquete 3 ...> \$ sudo yum update <Paquete1 Paquete2 Paquete 3 ...> </pre> <pre> [usuario@RHEL8-SI01 Scripts]\$ sudo yum install postfix-perl-scripts gnupg2-smime pypolicyd-spf </pre>

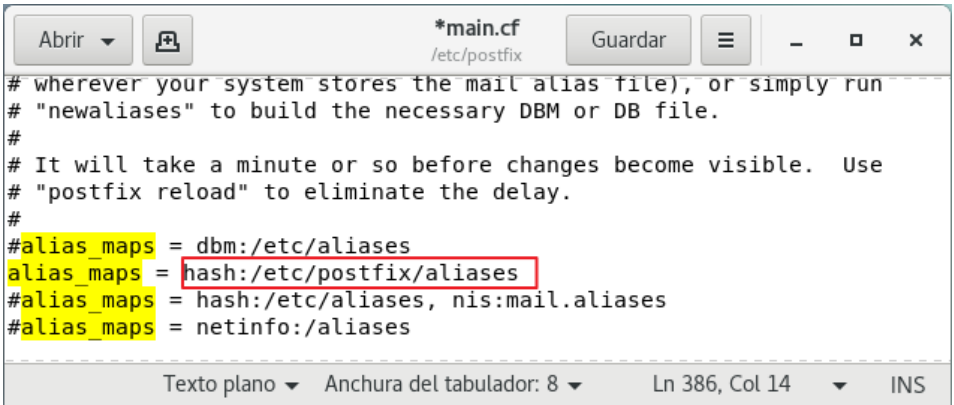
Paso	Descripción
21.	Ejecute el script de nuevo para comprobar que la configuración es correcta. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso1_comprobacion_paquetes_necesarios.sh</pre> <pre> ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... postfix-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix Instalado gnupg2-2.2.20-2.el8.x86_64 gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2 Instalado gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2-smime Instalado perl-Crypt-OpenSSL-Bignum-0.09-5.el8.x86_64 openssl-pkcs11-0.4.10-2.el8.x86_64 openssl-libs-1.1.1g-12.el8_3.x86_64 xmlsec1-openssl-1.2.25-4.el8.x86_64 openssl-1.1.1g-12.el8_3.x86_64 perl-Crypt-OpenSSL-RSA-0.31-1.el8.x86_64 python3-pyOpenSSL-18.0.0-1.el8.noarch perl-Crypt-OpenSSL-Random-0.15-3.el8.x86_64 openssl Instalado postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts Instalado epel-release-8-10.el8.noarch epel-release-7-11.noarch Instalado pypolicyd-spf-2.0.2-7.el8.noarch pypolicyd-spf Instalado libopendkim-2.11.0-0.17.el8.x86_64 opendkim-2.11.0-0.17.el8.x86_64 opendkim Instalado </pre> 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 <pre> ----- ----- SE COMPROBARAN PROGRAMAS INNECESARIOS ----- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... sendmail-milter-8.15.2-32.el8.x86_64 Deberá enmascar los servicios y demonios asociados limitando exposición en caso de NO SER NECESARIO PARA SU SISTEMA ----- ---- CONFIGURACION TERMINADA ---- ----- </pre>

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. <pre>\$ 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</pre> 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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso2_configuracion_main.cf.sh</pre>
24.	Para continuar con la ejecución del script, pulse “ENTER”. <pre>----- -- CCN-STIC-681A21-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.....</pre>
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. <pre>----- -- 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 AL SISTEMA ESTA RESTRINGIDO A USUARIOS AUTORIZADOS</pre> 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.

Paso	Descripción																		
26.	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 AL SISTEMA ESTA RESTRINGIDO A USUARIOS AUTORIZADOS banner Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>																		
27.	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 border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </table> Nota: Deberá adaptar los valores a los requeridos por su organización.  Además, deberá añadir la siguiente información en el fichero. <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </table>	Parámetro	Valor	body_checks_size_limit =	49152	queue_minfree =	20971520	header_size_limit =	1024	message_size_limit =	50200	Parámetro	Valor	Mydomain =	<Su dominio>	Myhostname =	<El nombre del servidor>	Myorigin =	<Su dominio>
Parámetro	Valor																		
body_checks_size_limit =	49152																		
queue_minfree =	20971520																		
header_size_limit =	1024																		
message_size_limit =	50200																		
Parámetro	Valor																		
Mydomain =	<Su dominio>																		
Myhostname =	<El nombre del servidor>																		
Myorigin =	<Su dominio>																		

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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso3_Postmaster.sh</pre> 
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.

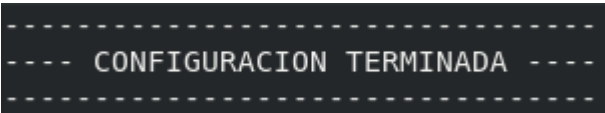
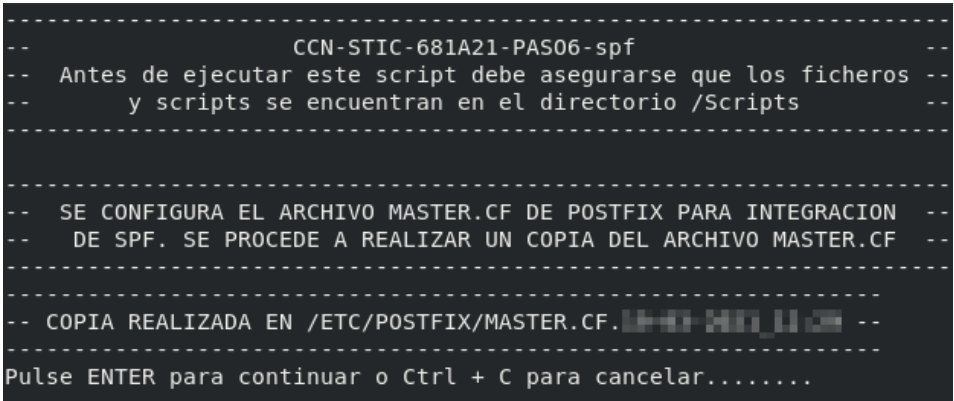
Paso	Descripción				
36.	Deberá editar el archivo de configuración main.cf de Postfix, para que el servidor postfix pueda detectar la nueva configuración. Introduzca la contraseña si se le solicita. <pre>\$ sudo gnome-text-editor /etc/postfix/main.cf &>/dev/null</pre> <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <tr> <td>alias_maps =</td><td>hash:/etc/postfix/alias</td></tr> </tbody> </table> 	Parámetro	Valor	alias_maps =	hash:/etc/postfix/alias
Parámetro	Valor				
alias_maps =	hash:/etc/postfix/alias				
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 Red Hat 8 Linux, ejecute el siguiente comando. Si ejecuta sin errores, no mostrará resultado por pantalla. <pre>\$ sudo newaliases</pre>				
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 Red Hat 8 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. <pre>\$ sudo groupadd “monitorización” \$ sudo chgrp -R “monitorización” /var/log/maillog \$ sudo usermod -a -G “monitorización” “usuarios designados”</pre> 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.				

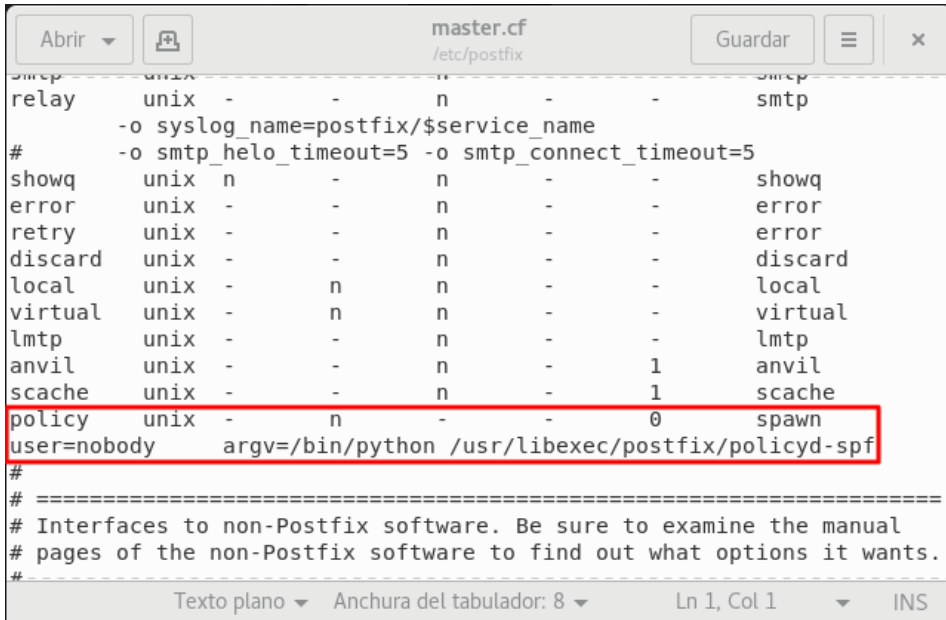
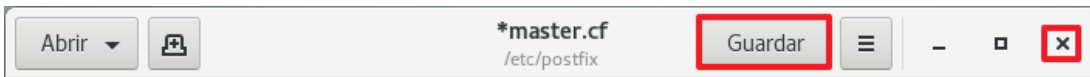
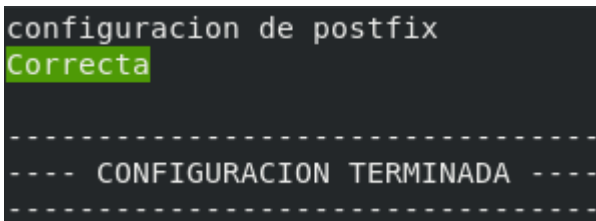
Paso	Descripción
40.	La modificación de permisos sobre la carpeta de logs de los correos electrónicos se realiza desde la línea de comandos, otorgando los permisos de escritura y lectura al usuario y al grupo designados. El usuario del sistema “root” será el poseedor de la carpeta para el correcto funcionamiento del sistema y poseerá los permisos equivalentes a “660”. <pre>\$ sudo chmod -660 /var/log/maillog</pre>
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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso4_certificados_openSSL.sh</pre> 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. <pre> ----- -- CCN-STIC-681A21-POSTFIX-PASO 4 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE PROCEDE A CREAR UN CERTIFICADO AUTO-FIRMADO SSL -- ----- Nombre de llave privada: CLAVEPRIVADA </pre>
43.	Posteriormente introduzca un nombre para el fichero CSR (solicitud de firma de certificado) que se generará posteriormente. Pulse “Enter” para continuar. <pre> -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE PROCEDE A CREAR UN CERTIFICADO AUTO-FIRMADO SSL -- ----- Nombre de llave privada: CLAVEPRIVADA Nombre Certificado de firma: NOMBREFIRMA </pre>

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. <pre> Generating RSA private key, 2096 bit long modulus (2 primes) .++++++++++ e is 65537 (0x010001) Enter pass phrase for CLAVEPRIVADA.key: Verifying - Enter pass phrase for CLAVEPRIVADA.key: Enter pass phrase for CLAVEPRIVADA.key: </pre>
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. <pre> What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country Name (2 letter code) [XX]:ES State or Province Name (full name) []:Madrid Locality Name (eg, city) [Default City]:Madrid Organization Name (eg, company) [Default Company Ltd]:Organizacion Organizational Unit Name (eg, section) []:opcional Organizacion Common Name (eg, your name or your server's hostname) []:RHEL8-SI01 Email Address []:correo@organizacion.es Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:password An optional company name []:Organizacion </pre> 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”. <pre> Nombre de certificado auto-firmado: RHEL08 </pre>

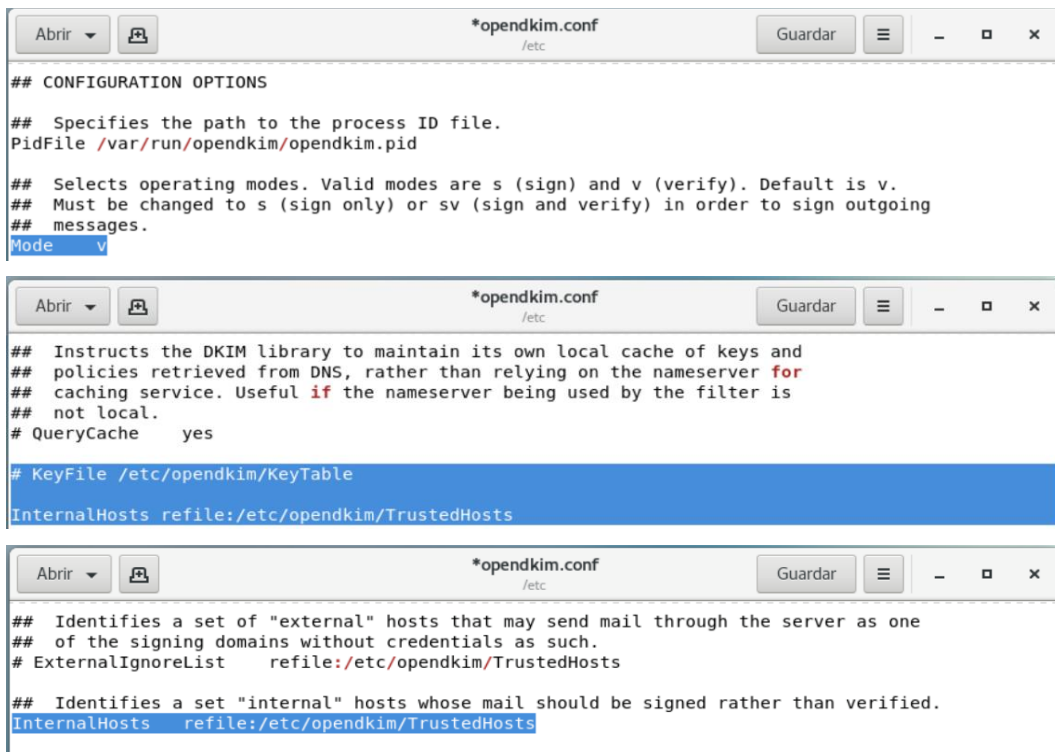
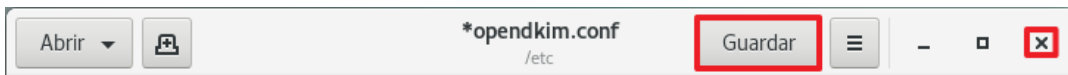
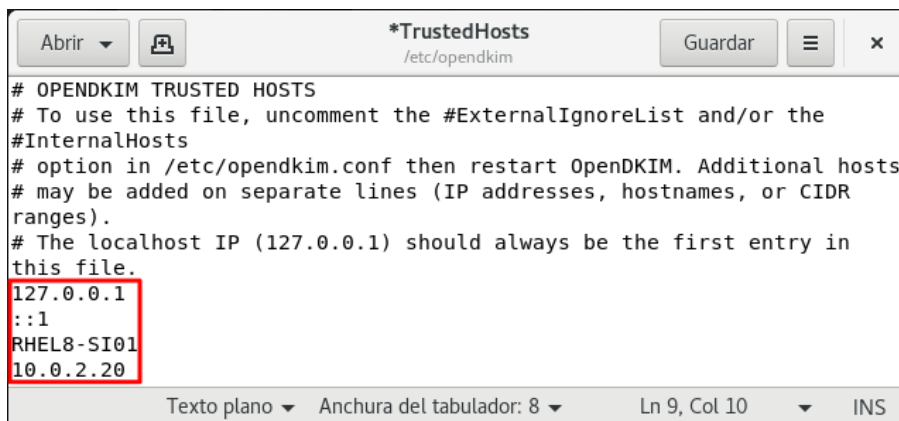
Paso	Descripción
47.	El proceso finaliza con el mensaje “Signature ok” y mostrando las configuraciones elegidas. Para finalizar el proceso de generación de firma “auto-firmada”, se solicita que ingrese la contraseña de su clave privada. <pre>Signature ok subject=C = ES, ST = Madrid, L = Madrid, O = Organizacion, OU = opcional Organizacion, CN = RHEL8-SI01, emailAddress = correo@organizacion.es Getting Private key Enter pass phrase for CLAVEPRIVADA.key: ----- ---- CONFIGURACION TERMINADA ---- -----</pre>
48.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso5_Seguridad.sh</pre>
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”. <pre>----- -- CCN-STIC-681A21-POSTFIX-PASO 5 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE REALIZARA UNA COPIA DE SEGURIDAD DEL ARCHIVO MAIN.CF -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>
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. <pre>----- - COPIA DE SEGURIDAD REALIZADA EN /ETC/POSTFIX/MAIN.CF. 11-11-2021 - ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... ----- -- SE PROCEDERA A CONFIGURAR EL ARCHIVO MAIN.CF -- -- PARA EL USO DE SSL Y TLS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>

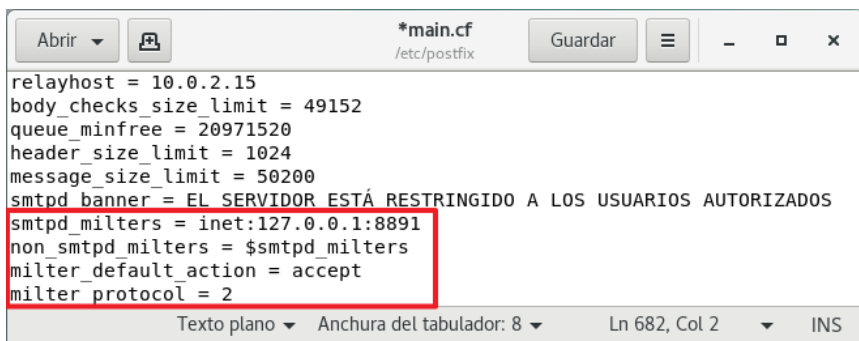
Paso	Descripción																																		
51.	A continuación, se muestra una tabla con los valores recomendados que se deberán aplicar en el archivo de configuración main.cf de Postfix. <table> <tr> <th>Parámetro</th><th>Valor</th></tr> <tr> <td>smtpd_sasl_auth_enable =</td><td>yes</td></tr> <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.  <pre> smtpd_sasl_auth_enable = yes broken_sasl_auth_clients = yes #smtpd_sasl_type = smtpd_sasl_path = private/auth smtpd_sasl_security_options = noanonymous smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, reject_unauth_destination, per smtp_use_tls = yes smtp_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1 smtpd_tls_session_cache_database = btree:/etc/postfix/smtpd_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 </pre>	Parámetro	Valor	smtpd_sasl_auth_enable =	yes	broken_sasl_auth_clients =	yes	#smtpd_sasl_type =		smtpd_sasl_path =	private/auth	smtpd_sasl_security_options =	noanonymous	smtpd_recipient_restrictions =	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, reject_unauth_destination, permit_auth_destination	smtp_use_tls =	yes	smtp_tls_mandatory_protocols =	!SSLv2, !SSLv3, !TLSv1	smtpd_tls_cert_file =	/etc/ssl/certs/<certificado>	smtpd_tls_key_file =	/etc/ssl/certs/<certificado>	smtpd_tls_session_cache_database =	btree:/etc/postfix/smtpd_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
Parámetro	Valor																																		
smtpd_sasl_auth_enable =	yes																																		
broken_sasl_auth_clients =	yes																																		
#smtpd_sasl_type =																																			
smtpd_sasl_path =	private/auth																																		
smtpd_sasl_security_options =	noanonymous																																		
smtpd_recipient_restrictions =	permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, reject_unauth_destination, permit_auth_destination																																		
smtp_use_tls =	yes																																		
smtp_tls_mandatory_protocols =	!SSLv2, !SSLv3, !TLSv1																																		
smtpd_tls_cert_file =	/etc/ssl/certs/<certificado>																																		
smtpd_tls_key_file =	/etc/ssl/certs/<certificado>																																		
smtpd_tls_session_cache_database =	btree:/etc/postfix/smtpd_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																																		

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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso6_spf.sh</pre> 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. <pre>policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf</pre>  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.
57.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
58.	El proceso finaliza con el siguiente mensaje, realizándose una comprobación de sintaxis. 

Paso	Descripción										
59.	Ejecute el siguiente comando para continuar con la configuración. Ingrese la contraseña si se le solicita. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIO_Paso7_Dkim.sh</pre> 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 Opendkim sobre Postfix. Para ello primero se realiza una copia de seguridad de los archivos. Deberá pulsar “ENTER” para continuar. <pre> ----- -- CCN-STIC-681A21_PASO 7 DKim -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE PROCEDE A CONFIGURAR EL ARCHIVO /ETC/OPENDKIM.CONF, -- -- /ETC/POSTFIX/MAIN.CF Y /ETC/OPENDKIM/TRUSTEDHOSTS -- -- SE REALIZARA UNA COPIA DE SEGURIDAD DE LOS ARCHIVOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>										
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. <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>	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
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/openssl/TrustedHosts. 

Paso	Descripción										
66.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.										
67.	Con la inserción de valores en el archivo /etc/postfix/main.cf se concluirá la integración de OpenDkim con Postfix. Pulse “ENTER” para continuar. <pre> ----- -- INTEGRANDO DKIM A POSTFIX -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>										
68.	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 border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </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.	Parámetro	Valor	smtpd_milters =	inet:127.0.0.1:8891	non_smtpd_milters =	\$smtpd_milters	milter_default_action =	accept	milter_protocol =	2
Parámetro	Valor										
smtpd_milters =	inet:127.0.0.1:8891										
non_smtpd_milters =	\$smtpd_milters										
milter_default_action =	accept										
milter_protocol =	2										
69.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 										
70.	El script finaliza el proceso con una comprobación de sintaxis. <pre> Sintaxis de Integracion: Correcta ----- -- DKIM INTEGRADO EN EL SISTEMA -- ----- </pre>										

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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso8_comprobacion_configuracion.sh</pre> <pre>----- -- CCN-STIC-681A21-POSTFIX-PASO 8 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE COMPROBARA LA INTEGRIDAD DE LOS FICHEROS Y CARPETAS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>
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. <pre>----- -- SE COMPROBARA LA INTEGRIDAD DE LOS FICHEROS Y CARPETAS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... -rw-r--r--. 1 root root 30K mar 22 20:07 /etc/postfix/main.cf main.cf SI pertenece a root Correcto -rw-r--r--. 1 root root 30K mar 22 20:07 /etc/postfix/main.cf main.cf Permisos de acceso CORRECTOS Correcto -rw-r--r--. 1 root root 6,4K mar 22 19:07 /etc/postfix/master.cf master.cf SI pertenece a root Correcto -rw-r--r--. 1 root root 6,4K mar 22 19:07 /etc/postfix/master.cf master.cf Permisos de acceso CORRECTOS Correcto drwxr-xr-x. 20 root root 247 mar 8 16:34 postfix /var/spool/postfix SI pertenece a root Correcto drwxr-xr-x. 20 root root 247 mar 8 16:34 postfix /var/spool/postfix Permisos de acceso CORRECTOS Correcto -rw-rw----. 1 root monitorizacion 60K mar 22 20:07 /var/log/maillog /var/log/maillog SI pertenece a root Correcto -rw-rw----. 1 root monitorizacion 60K mar 22 20:07 /var/log/maillog /var/log/maillog Permisos de acceso CORRECTOS Correcto</pre> 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.

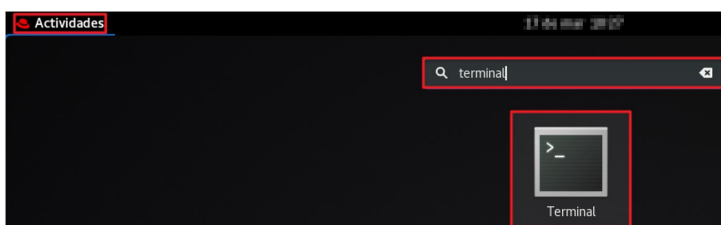
Paso	Descripción
73.	El Script continua con la comprobación de los usuarios y grupos y sus respectivas “shells”. Pulse “ENTER” para continuar. El script finalizará con el mensaje “CONFIGURACION TERMINADA”. <pre> ----- -- SE VA A PROCEDER A LA COMPROBACION DE USUARIOS Y GRUPOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... mail:x:12:postfix,opendkim postdrop:x:90: postfix:x:89: Grupos existentes Correcto Debera crear el usuario postfix con shell /bin/false Valor NO conforme opendkim:x:975:972:OpenDKIM Milter:/run/opendkim:/sbin/nologin USUARIO opendkim EXISTE Debera modificar al usuario opendkim con shell /bin/false Valor NO conforme ----- ---- CONFIGURACION TERMINADA ---- ----- </pre> 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. <pre> \$ sudo chsh -s /bin/false postfix \$ sudo chsh -s /bin/false opendkim </pre> <pre> [usuario@RHEL8-SI01 Scripts]\$ sudo chsh -s /bin/false postfix Cambiando intérprete de órdenes para postfix. chsh: No se ha cambiado el intérprete de órdenes. [usuario@RHEL8-SI01 Scripts]\$ sudo chsh -s /bin/false opendkim Cambiando intérprete de órdenes para opendkim. Se ha cambiado el intérprete de órdenes. [usuario@RHEL8-SI01 Scripts]\$ </pre>

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”. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso8_comprobacion_configuracion.sh</pre> <pre>----- -- SE VA A PROCEDER A LA COMPROBACION DE USUARIOS Y GRUPOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... mail:x:12:postfix,opendkim postdrop:x:90: postfix:x:89: Grupos existentes Correcto postfix:x:89:89:./var/spool/postfix:/bin/false Usuario existente y configurado correctamente Correcto opendkim:x:975:972:OpenDKIM Milter:/run/opendkim:/bin/false USUARIO opendkim EXISTE opendkim:x:975:972:OpenDKIM Milter:/run/opendkim:/bin/false USUARIO opendkim CONFIGURADO: CORRECTO ----- ---- CONFIGURACION TERMINADA ---- -----</pre>
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. <pre>\$ sudo systemctl unmask postfix.service \$ sudo systemctl start postfix.service \$ sudo systemctl enable postfix.service \$ sudo systemctl restart opendkim</pre>
77.	Elimine la carpeta /Scripts y todo su contenido.
78.	Guarde las aplicaciones que se encuentren abiertas y reinicie el servidor. <pre>\$ sudo shutdown -r</pre>

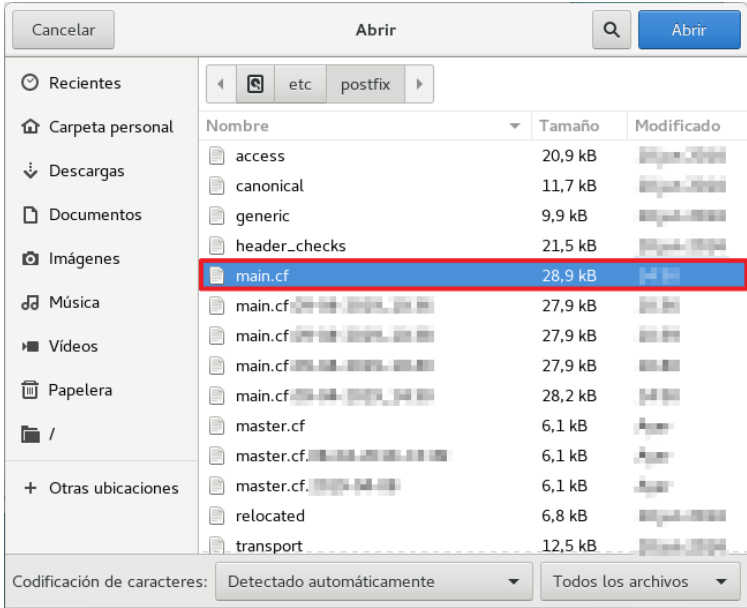
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR RED HAT 8 ENS CATEGORÍA MEDIA

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.

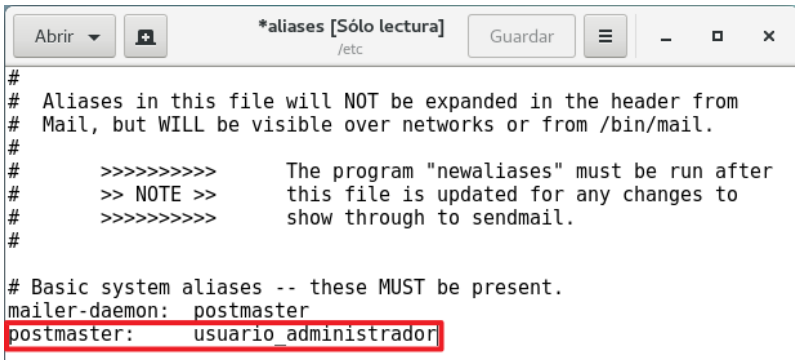
- a) Terminal.
- b) Editor de textos.

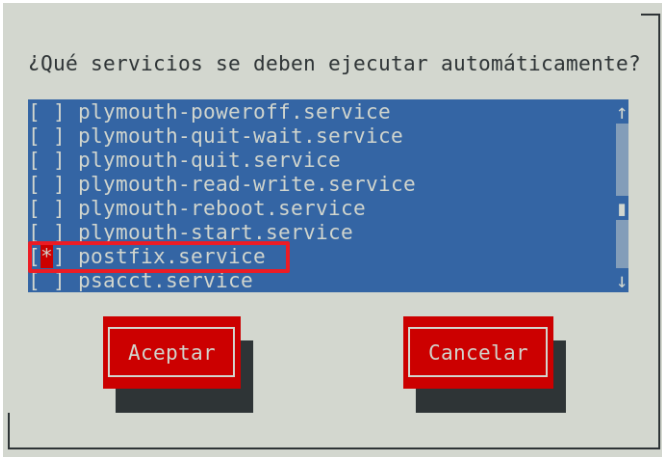
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En uno de los equipos Red Hat 8, inicie sesión con una cuenta que tenga privilegios de administración.
2. Inicie la Terminal de Linux.		Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “Terminal”. 
3. Verifique que se encuentren instalados los paquetes necesarios.		En la “terminal” ejecute el siguiente comando. <pre>\$ sudo rpm -aq egrep 'gnupg2 gnupg2-smime openssl postfix opendkim pypolicyd-spf'</pre> <pre>[usuario@RHEL8-SI01 Scripts]\$ sudo rpm -aq egrep 'gnupg2 gnupg2-smime openssl postfix opendkim pypolicyd-spf'</pre><pre>libopendkim-2.11.0-0.17.el8.x86_64</pre><pre>postfix-3.3.1-12.el8_3.1.x86_64</pre><pre>gnupg2-2.2.20-2.el8.x86_64</pre><pre>gnupg2-smime-2.2.20-2.el8.x86_64</pre><pre>openssl-pkcs11-0.4.10-2.el8.x86_64</pre><pre>openssl-libs-1.1.1g-12.el8_3.x86_64</pre><pre>pypolicyd-spf-2.0.2-7.el8.noarch</pre><pre>xmlsec1-openssl-1.2.25-4.el8.x86_64</pre><pre>openssl-1.1.1g-12.el8_3.x86_64</pre><pre>postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64</pre><pre>opendkim-2.11.0-0.17.el8.x86_64</pre> Nota: Deberá comprobar que las versiones de los paquetes que aquí se comprueban, se encuentran en sus últimas versiones.
Parámetros		OK/NOK
gnupg2-smime-[versión actualizada]		
openssl-[versión actualizada]		
postfix-[versión actualizada]		
pypolicyd-spf-[versión actualizada]		
gnupg2-[versión actualizada]		
openssl-libs-[versión actualizada]		

Comprobación	OK/NOK	Cómo hacerlo
	Parámetros	
	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	
	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. <pre>\$ ls -lh /etc/postfix \$ ls -lh /etc grep aliases</pre> Revise que se han realizado las correspondientes copias de seguridad de los archivos según la ejecución de los scripts correspondientes. <pre>[usuario@RHEL8-SI01 ~]\$ ls -lh /etc/postfix total 596K -rw-r--r--. 1 root root 12K Feb 28 2023 access -rw-r--r--. 1 root root 12K Feb 28 2023 canonical -rw-r--r--. 1 root root 12K Feb 28 2023 dynamicmaps.cf drwxr-xr-x. 2 root root 12K Feb 28 2023 dynamicmaps.cf.d -rw-r--r--. 1 root root 12K Feb 28 2023 generic -rw-r--r--. 1 root root 12K Feb 28 2023 header_checks -rw-r--r--. 1 root root 12K Feb 28 2023 main.cf -rw-r--r--. 1 root root 12K Feb 28 2023 main.cf.backup -rw-r--r--. 1 root root 12K Feb 28 2023 main.cf.proto -rw-r--r--. 1 root root 12K Feb 28 2023 master.cf -rw-r--r--. 1 root root 12K Feb 28 2023 master.cf.backup -rw-r--r--. 1 root root 12K Feb 28 2023 master.cf.proto -rw-r--r--. 1 root root 12K Feb 28 2023 postfix-files drwxr-xr-x. 2 root root 12K Feb 28 2023 postfix-files.d -rw-r--r--. 1 root root 12K Feb 28 2023 relocated -rw-r--r--. 1 root root 12K Feb 28 2023 transport -rw-r--r--. 1 root root 12K Feb 28 2023 virtual [usuario@RHEL8-SI01 ~]\$</pre> Nota: Tenga en consideración que poseerá tantas copias como veces haya ejecutado los scripts.
	Configuración	
	master.cf.[FECHA]	
	main.cf.[FECHA]	
	Aliases.[FECHA]	

Comprobación	OK/NOK	Cómo hacerlo
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	
smtp_tls_mandatory_protocols	!SSLv2,SSLv3, TLSv1	
smtpd_tls_cert_file	/etc/ssl/private/<certificado.extensión>	

Comprobación	OK/NOK	Cómo hacerlo	
Parámetros		Valor	OK/NOK
smtpd_tls_key_file		/etc/ssl/private/<clave.extensión>	
smtpd_tls_session_cache_database		btrees:/etc/postfix/smt_d_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.	
		<pre>\$ 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</pre>	
		Ruta	Propietario
		/etc/postfix/main.cf	root
		/etc/postfix/master.cf	root
		/var/spool/	root
8. Comprobación de permisos de archivos			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.	
		<pre>\$ 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\-----'</pre>	

Comprobación	OK/NOK	Cómo hacerlo		
		Configuración	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.		
		<pre>\$ cat /etc/passwd egrep "postfix /bin/false "</pre> <pre>\$ cat /etc/group egrep "postfix postdrop"</pre> <pre>\$ cat /etc/passwd egrep "opendkim /bin/false "</pre> <pre>\$ cat /etc/group egrep " opendkim"</pre>		
		Configuración	Valor	OK/NOK
		Usuario: postfix	Existe	
		Shell: postfix	/bin/false	
		Grupo: postfix	Existe	
		Grupo: postdrop	Existe	
		Usuario: opendkim	Existe	
		Shell: opendkim	/bin/false	
		Grupo: opendkim	Existe	
10.Cambio de usuario de Postmaster		Compruebe que se han modificado los siguientes parámetros dentro del archivo aliases. Para ello diríjase a la barra de tareas superior, pulse sobre "Actividades", escriba y 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.		
		 <pre># # Aliases in this file will NOT be expanded in the header from # Mail, but WILL be visible over networks or from /bin/mail. # # >>>>>>>> The program "newaliases" must be run after # >> NOTE >> this file is updated for any changes to # >>>>>>>> show through to sendmail. # # Basic system aliases -- these MUST be present. mailer-daemon: postmaster postmaster: usuario_administrador</pre>		

Comprobación	OK/NOK	Cómo hacerlo		
11.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	
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	

Comprobación	OK/NOK	Cómo hacerlo
13. Configuración del archivo master.cf		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". 
	Parámetros	
		policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA POSTFIX 3.3.1-12.el8_3.1 SOBRE RED HAT 8 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 3.3.1-12.el8_3.1 sobre Red Hat 8, 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 uso 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 Red Hat 8 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.

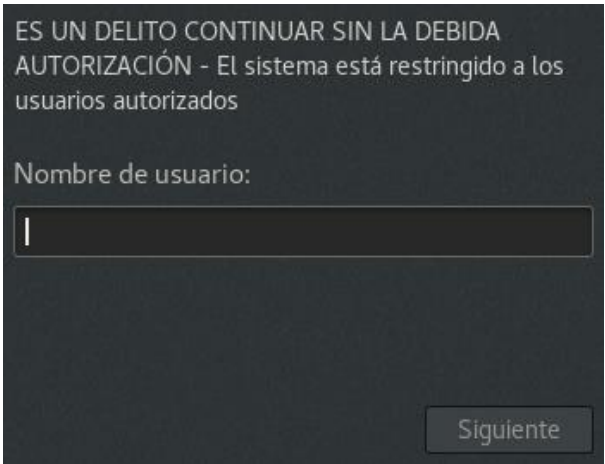
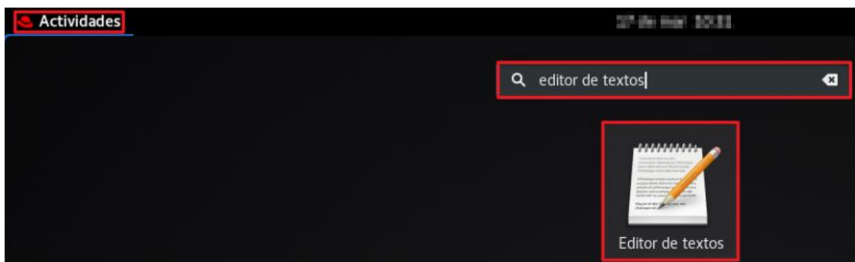
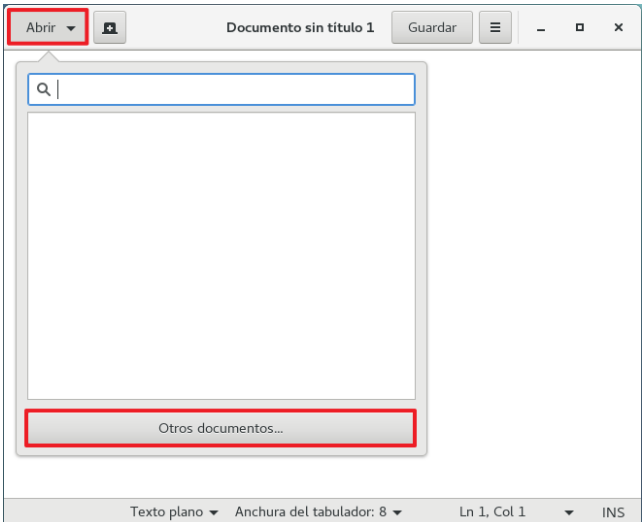
Postfix 3.3.1-12.el8_3.1.x86_64 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Postfix, en caso de necesitar información sobre los requisitos previos de instalación de Postfix visite el enlace <http://www.postfix.org/features.html#fs-requirements>

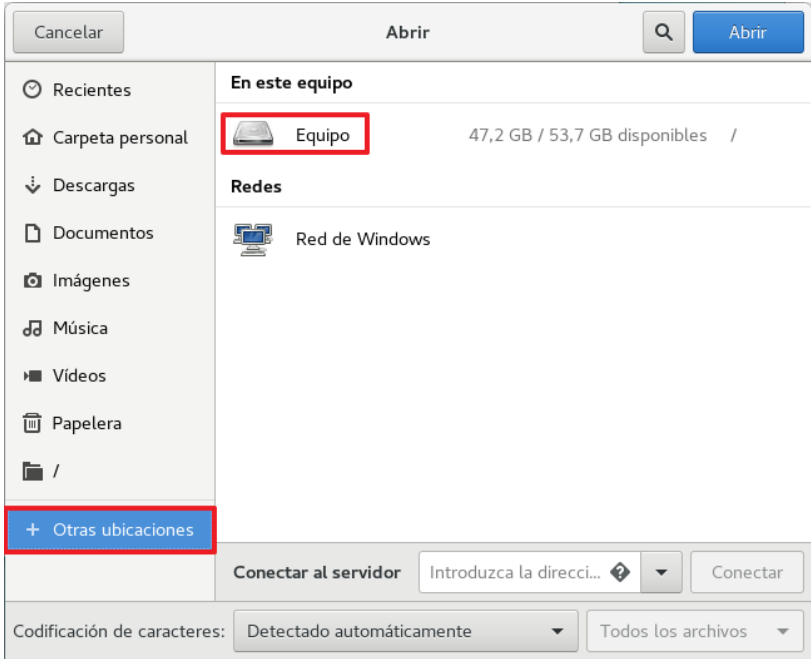
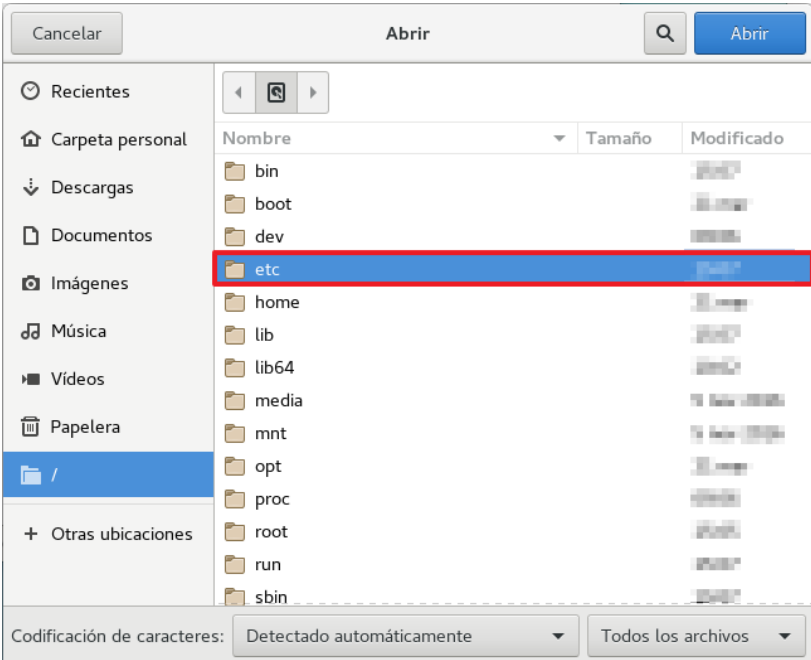
Nota: La instalación de Postfix se debe realizar en un volumen que debe haber sido formateado previamente con el formato XFS, formato que permite la aplicación de ACL's. Así mismo, antes de proceder a instalar las diferentes funcionalidades y complementos de Postfix, se debe haber reiniciado el servidor 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 "CCN-STIC".

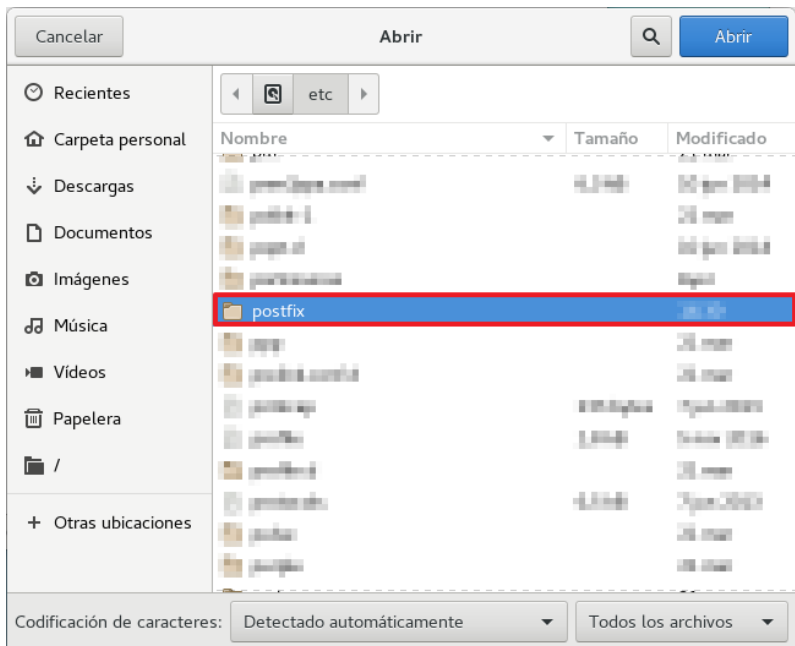
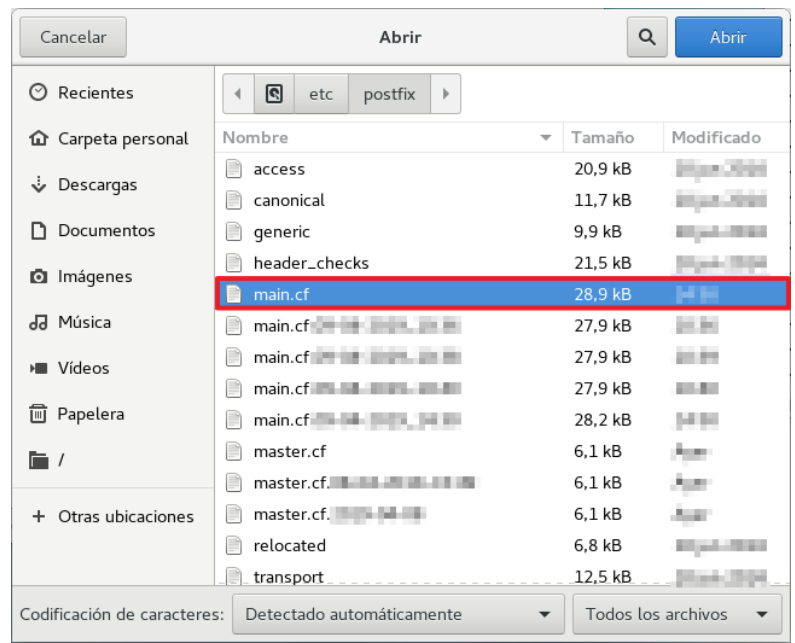
Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando.

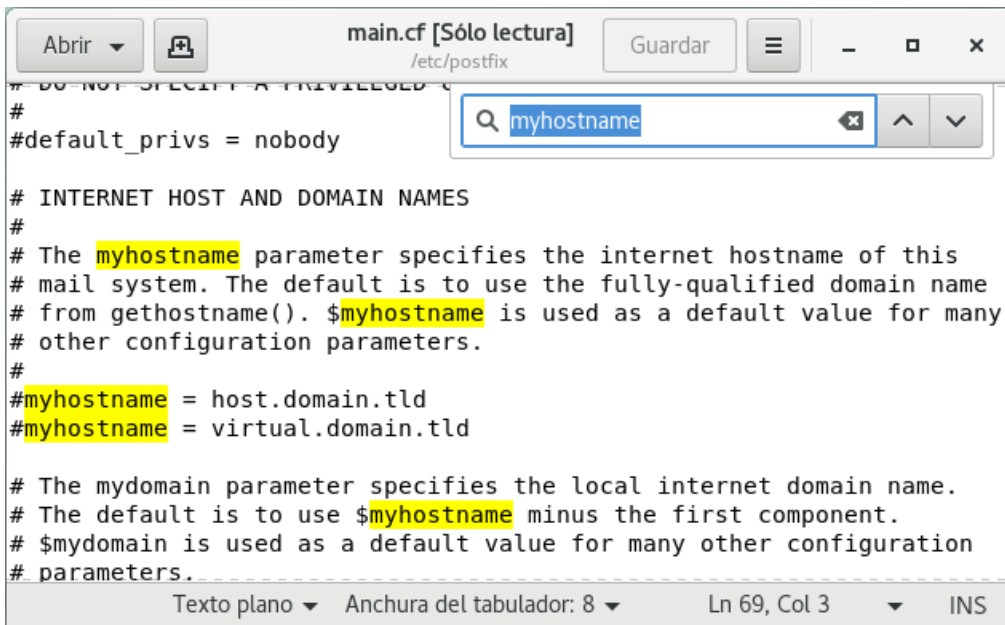
- **\$ sudo setenforce 0**

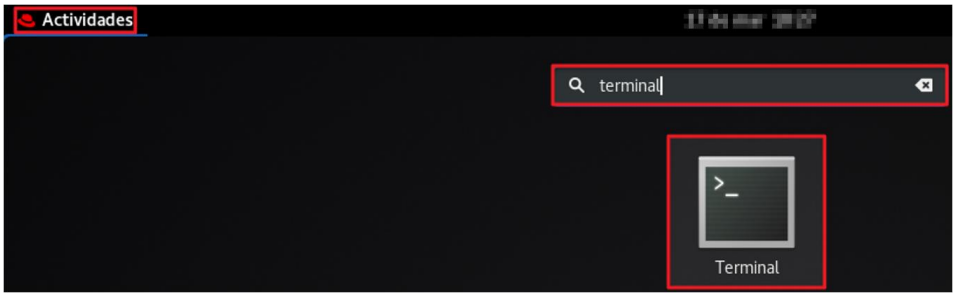
Deberá adaptar los parámetros de configuración de firewalld acorde a su organización. Tenga en cuenta que en esta guía se utilizan, a modo de ejemplo, varios puertos, que es necesario que estén abiertos para el correcto funcionamiento de los productos descritos.

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 "Actividades", escriba y 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.	Ingresa a la carpeta “etc”. 

Paso	Descripción																																													
6.	Ingrese en la carpeta “postfix”.  The screenshot shows a file manager window titled "Abrir" (Open). The left sidebar lists various locations like "Recientes", "Carpeta personal", "Descargas", etc. The main pane shows a list of files and folders. The "postfix" folder is highlighted with a red box. The table below represents the data shown in the file manager window. <table><tr><th>Nombre</th><th>Tamaño</th><th>Modificado</th></tr><tr><td>access</td><td>20,9 kB</td><td>10/04/2024</td></tr><tr><td>canonical</td><td>11,7 kB</td><td>10/04/2024</td></tr><tr><td>generic</td><td>9,9 kB</td><td>10/04/2024</td></tr><tr><td>header_checks</td><td>21,5 kB</td><td>10/04/2024</td></tr><tr><td>main.cf</td><td>28,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup</td><td>27,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup.1</td><td>27,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup.2</td><td>27,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup.3</td><td>28,2 kB</td><td>10/04/2024</td></tr><tr><td>master.cf</td><td>6,1 kB</td><td>10/04/2024</td></tr><tr><td>master.cf.backup</td><td>6,1 kB</td><td>10/04/2024</td></tr><tr><td>master.cf.backup.1</td><td>6,1 kB</td><td>10/04/2024</td></tr><tr><td>relocated</td><td>6,8 kB</td><td>10/04/2024</td></tr><tr><td>transport</td><td>12,5 kB</td><td>10/04/2024</td></tr></table>	Nombre	Tamaño	Modificado	access	20,9 kB	10/04/2024	canonical	11,7 kB	10/04/2024	generic	9,9 kB	10/04/2024	header_checks	21,5 kB	10/04/2024	main.cf	28,9 kB	10/04/2024	main.cf.backup	27,9 kB	10/04/2024	main.cf.backup.1	27,9 kB	10/04/2024	main.cf.backup.2	27,9 kB	10/04/2024	main.cf.backup.3	28,2 kB	10/04/2024	master.cf	6,1 kB	10/04/2024	master.cf.backup	6,1 kB	10/04/2024	master.cf.backup.1	6,1 kB	10/04/2024	relocated	6,8 kB	10/04/2024	transport	12,5 kB	10/04/2024
Nombre	Tamaño	Modificado																																												
access	20,9 kB	10/04/2024																																												
canonical	11,7 kB	10/04/2024																																												
generic	9,9 kB	10/04/2024																																												
header_checks	21,5 kB	10/04/2024																																												
main.cf	28,9 kB	10/04/2024																																												
main.cf.backup	27,9 kB	10/04/2024																																												
main.cf.backup.1	27,9 kB	10/04/2024																																												
main.cf.backup.2	27,9 kB	10/04/2024																																												
main.cf.backup.3	28,2 kB	10/04/2024																																												
master.cf	6,1 kB	10/04/2024																																												
master.cf.backup	6,1 kB	10/04/2024																																												
master.cf.backup.1	6,1 kB	10/04/2024																																												
relocated	6,8 kB	10/04/2024																																												
transport	12,5 kB	10/04/2024																																												
7.	Ejecute el archivo “main.cf” pulsando sobre el botón “Abrir” o haciendo doble clic izquierdo con el ratón.  The screenshot shows the same file manager window, but now the "main.cf" file is highlighted with a red box. The table below represents the data shown in the file manager window. <table><tr><th>Nombre</th><th>Tamaño</th><th>Modificado</th></tr><tr><td>access</td><td>20,9 kB</td><td>10/04/2024</td></tr><tr><td>canonical</td><td>11,7 kB</td><td>10/04/2024</td></tr><tr><td>generic</td><td>9,9 kB</td><td>10/04/2024</td></tr><tr><td>header_checks</td><td>21,5 kB</td><td>10/04/2024</td></tr><tr><td>main.cf</td><td>28,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup</td><td>27,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup.1</td><td>27,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup.2</td><td>27,9 kB</td><td>10/04/2024</td></tr><tr><td>main.cf.backup.3</td><td>28,2 kB</td><td>10/04/2024</td></tr><tr><td>master.cf</td><td>6,1 kB</td><td>10/04/2024</td></tr><tr><td>master.cf.backup</td><td>6,1 kB</td><td>10/04/2024</td></tr><tr><td>master.cf.backup.1</td><td>6,1 kB</td><td>10/04/2024</td></tr><tr><td>relocated</td><td>6,8 kB</td><td>10/04/2024</td></tr><tr><td>transport</td><td>12,5 kB</td><td>10/04/2024</td></tr></table>	Nombre	Tamaño	Modificado	access	20,9 kB	10/04/2024	canonical	11,7 kB	10/04/2024	generic	9,9 kB	10/04/2024	header_checks	21,5 kB	10/04/2024	main.cf	28,9 kB	10/04/2024	main.cf.backup	27,9 kB	10/04/2024	main.cf.backup.1	27,9 kB	10/04/2024	main.cf.backup.2	27,9 kB	10/04/2024	main.cf.backup.3	28,2 kB	10/04/2024	master.cf	6,1 kB	10/04/2024	master.cf.backup	6,1 kB	10/04/2024	master.cf.backup.1	6,1 kB	10/04/2024	relocated	6,8 kB	10/04/2024	transport	12,5 kB	10/04/2024
Nombre	Tamaño	Modificado																																												
access	20,9 kB	10/04/2024																																												
canonical	11,7 kB	10/04/2024																																												
generic	9,9 kB	10/04/2024																																												
header_checks	21,5 kB	10/04/2024																																												
main.cf	28,9 kB	10/04/2024																																												
main.cf.backup	27,9 kB	10/04/2024																																												
main.cf.backup.1	27,9 kB	10/04/2024																																												
main.cf.backup.2	27,9 kB	10/04/2024																																												
main.cf.backup.3	28,2 kB	10/04/2024																																												
master.cf	6,1 kB	10/04/2024																																												
master.cf.backup	6,1 kB	10/04/2024																																												
master.cf.backup.1	6,1 kB	10/04/2024																																												
relocated	6,8 kB	10/04/2024																																												
transport	12,5 kB	10/04/2024																																												

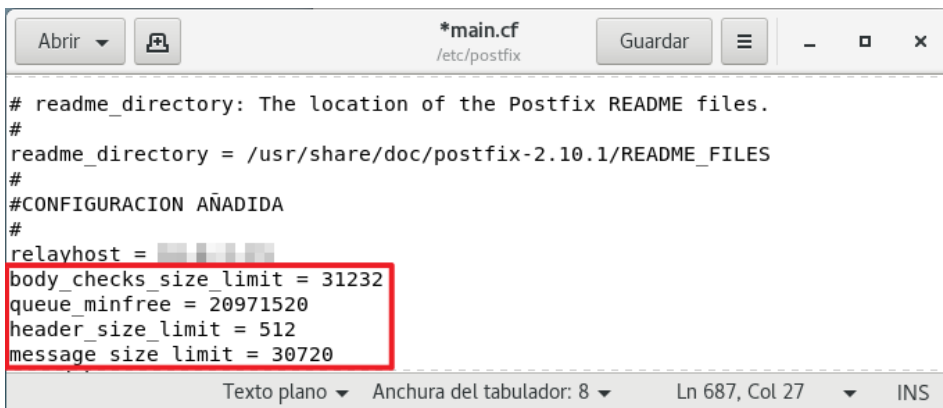
Paso	Descripción
8.	A continuación, se muestran los parámetros a modificar. Estos parámetros responden a una configuración de tipo “parámetro=valor”, utilizando el símbolo “dólar” (\$) para exportarlo globalmente en todo el fichero. – Myhostname = Nombre del servidor MTA Postfix. – Mydomain = Nombre 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.  The screenshot shows a text editor window titled 'main.cf [Sólo lectura]' with the path '/etc/postfix'. A search bar at the top right contains the text 'myhostname'. The main text area shows the configuration file content with several lines highlighted in yellow, including '#myhostname = host.domain.tld' and '#myhostname = virtual.domain.tld'. The status bar at the bottom indicates 'Texto plano', 'Anchura del tabulador: 8', 'Ln 69, Col 3', and 'INS'.
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.  The screenshot shows the bottom part of the text editor window. The 'Guardar' button is highlighted with a red box, and the close button (represented by an 'x' icon) is also highlighted with a red box.

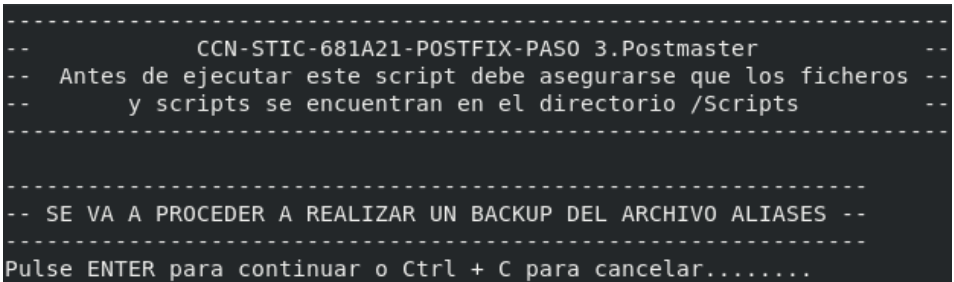
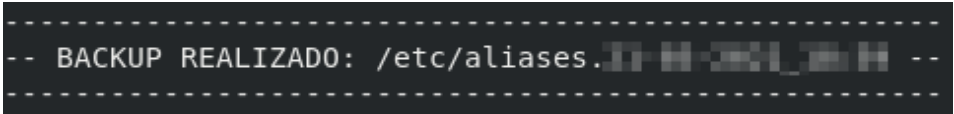
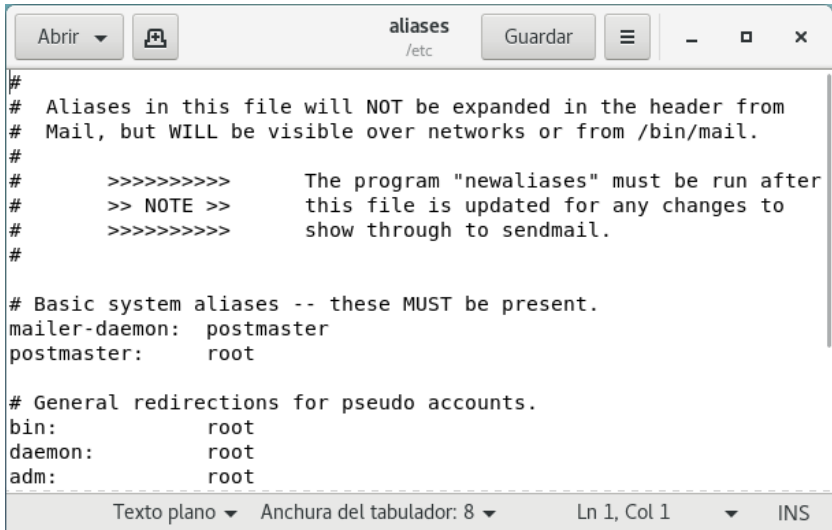
Paso	Descripción
11.	Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “Terminal”. 
12.	Cree la carpeta “Scripts”. Para ello, en el terminal, ejecute el comando siguiente. <pre>\$ cd /</pre> Para crear la carpeta en la ubicación ejecute el siguiente comando. <pre>\$ sudo mkdir Scripts</pre> Nota: Puede comprobar que la carpeta ha sido creada ejecutando <code>ls /</code>.
13.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía CCN-STIC-681A21- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE RED HAT 8 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”. Para ello, ejecute el comando siguiente. <pre>\$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_ALTA/* /Scripts/</pre> 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. <pre>\$ cd /Scripts</pre>
16.	Ejecute el siguiente comando. Introduzca la contraseña del usuario para continuar. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso1_comprobacion_paquetes_necesarios.sh</pre> 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.

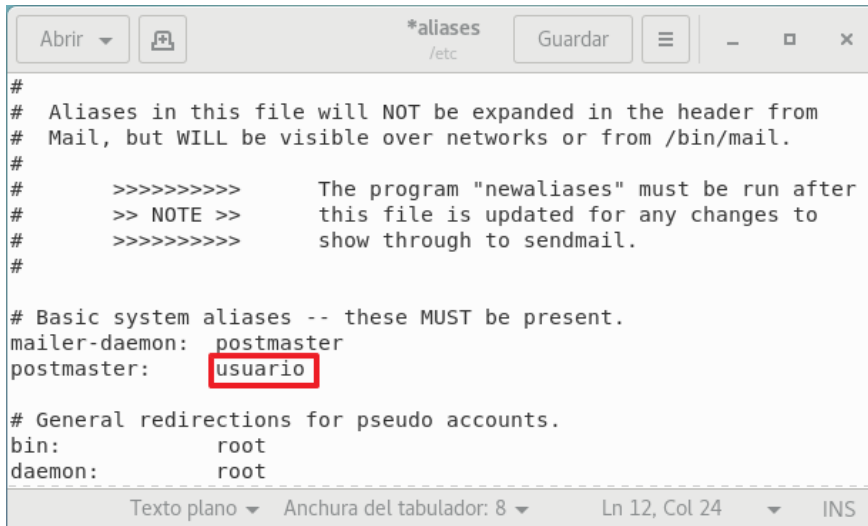
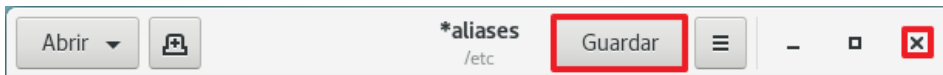
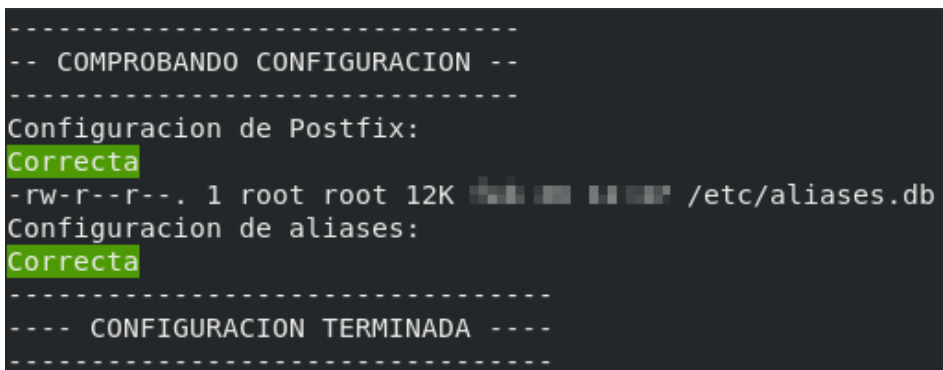
Paso	Descripción
17.	Pulse “ENTER” para continuar. <pre> ----- -- CCN-STIC-681A21-POSTFIX-PASO 1 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
18.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar. <pre> ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... postfix-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix Instalado gnupg2-2.2.20-2.el8.x86_64 gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2 Instalado Debe instalar gnupg2-smime </pre> 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”. <pre> ----- SE COMPROBARAN PROGRAMAS INNECESARIOS ----- ----- Pulse ENTER para continuar o Ctrl + C para cancelar... NO HAY PROGRAMAS INNECESARIOS ----- CONFIGURACION TERMINADA ----- ----- </pre>
20.	Instale, actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. <pre> \$ sudo yum install <Paquete1 Paquete2 Paquete 3 ...> \$ sudo yum update <Paquete1 Paquete2 Paquete 3 ...> </pre> <pre> [usuario@RHEL8-SI01 Scripts]\$ sudo yum install postfix-perl-scripts gnupg2-smime pypolicyd-spf </pre>

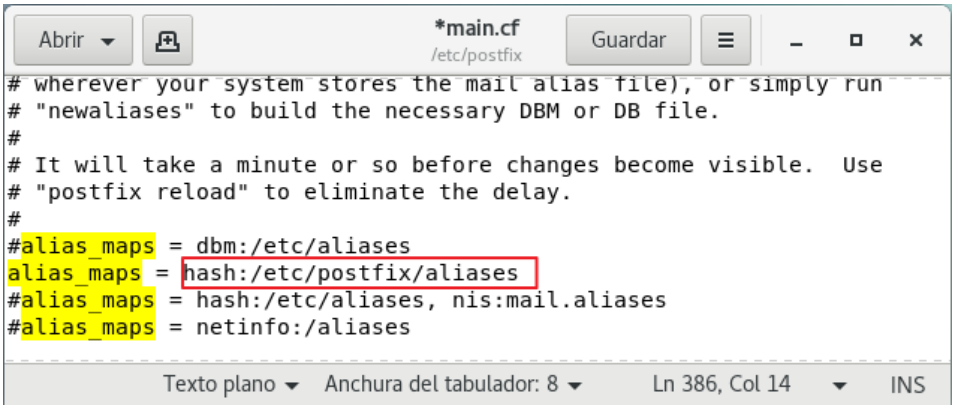
Paso	Descripción
21.	Ejecute el script de nuevo para comprobar que la configuración es correcta. <pre>\$ sudo sh CCN-STIC-681A21_ENS_MEDIA_Paso1_comprobacion_paquetes_necesarios.sh</pre> <pre> ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... postfix-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix Instalado gnupg2-2.2.20-2.el8.x86_64 gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2 Instalado gnupg2-smime-2.2.20-2.el8.x86_64 gnupg2-smime Instalado perl-Crypt-OpenSSL-Bignum-0.09-5.el8.x86_64 openssl-pkcs11-0.4.10-2.el8.x86_64 openssl-libs-1.1.1g-12.el8_3.x86_64 xmlsec1-openssl-1.2.25-4.el8.x86_64 openssl-1.1.1g-12.el8_3.x86_64 perl-Crypt-OpenSSL-RSA-0.31-1.el8.x86_64 python3-pyOpenSSL-18.0.0-1.el8.noarch perl-Crypt-OpenSSL-Random-0.15-3.el8.x86_64 openssl Instalado postfix-perl-scripts-3.3.1-12.el8_3.1.x86_64 postfix-perl-scripts Instalado epel-release-8-10.el8.noarch epel-release-7-11.noarch Instalado pypolicyd-spf-2.0.2-7.el8.noarch pypolicyd-spf Instalado libopendkim-2.11.0-0.17.el8.x86_64 opendkim-2.11.0-0.17.el8.x86_64 opendkim Instalado </pre> 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 <pre> ----- ----- SE COMPROBARAN PROGRAMAS INNECESARIOS ----- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... sendmail-milter-8.15.2-32.el8.x86_64 Deberá enmascar los servicios y demonios asociados limitando exposición en caso de NO SER NECESARIO PARA SU SISTEMA ----- ---- CONFIGURACION TERMINADA ---- ----- </pre>

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. <pre>\$ 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</pre> 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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso2_configuracion_main.cf.sh</pre>
24.	Para continuar con la ejecución del script, pulse “ENTER”. <pre>----- -- CCN-STIC-681A21-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.....</pre>
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. <pre>----- -- 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 AL SISTEMA ESTA RESTRINGIDO A USUARIOS AUTORIZADOS</pre> 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.

Paso	Descripción																		
26.	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 AL SISTEMA ESTA RESTRINGIDO A USUARIOS AUTORIZADOS banner Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>																		
27.	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 border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </table>	Parámetro	Valor	body_checks_size_limit =	31232	queue_minfree =	20971520	header_size_limit =	512	message_size_limit =	30720	Parámetro	Valor	Mydomain =	<Su dominio>	Myhostname =	<El nombre del servidor>	Myorigin =	<Su dominio>
Parámetro	Valor																		
body_checks_size_limit =	31232																		
queue_minfree =	20971520																		
header_size_limit =	512																		
message_size_limit =	30720																		
Parámetro	Valor																		
Mydomain =	<Su dominio>																		
Myhostname =	<El nombre del servidor>																		
Myorigin =	<Su dominio>																		

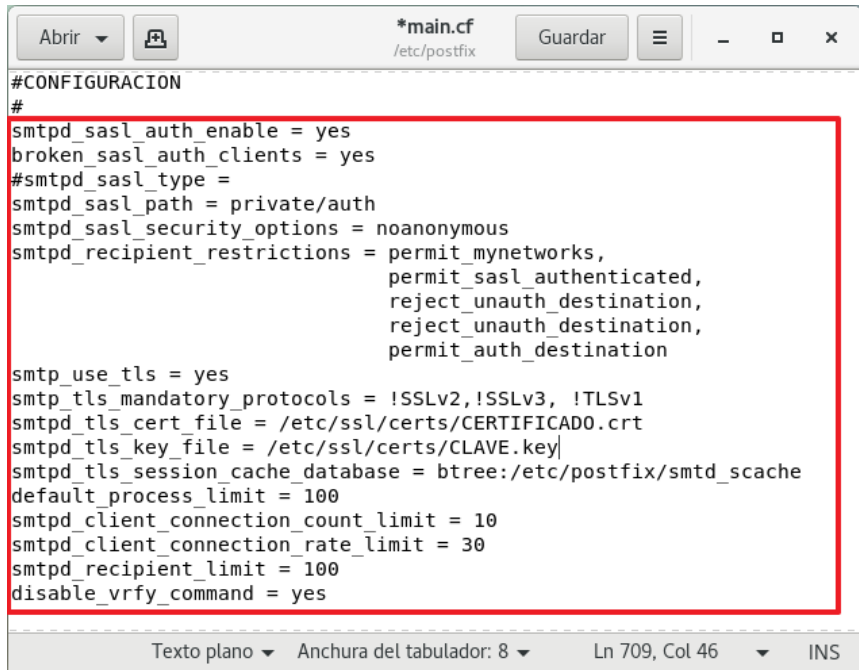
Paso	Descripción
28.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
29.	La configuración termina con la salida del proceso de configuración y el mensaje de finalización del mismo.
30.	Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso3_Postmaster.sh</pre> 
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.  <pre># # Aliases in this file will NOT be expanded in the header from # Mail, but WILL be visible over networks or from /bin/mail. # # >>>>>>>> The program "newaliases" must be run after # >> NOTE >> this file is updated for any changes to # >>>>>>>> show through to sendmail. # # Basic system aliases -- these MUST be present. mailer-daemon: postmaster postmaster: usuario # General redirections for pseudo accounts. bin: root daemon: root</pre> 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”.  <pre>-- COMPROBANDO CONFIGURACION -- Configuracion de Postfix: Correcta -rw-r--r--. 1 root root 12K /etc/aliases.db Configuracion de aliases: Correcta --- CONFIGURACION TERMINADA ---</pre> Nota: Si hubiera alguna discrepancia, restaure el archivo de copia de seguridad y ejecute de nuevo el script siguiendo los pasos de configuración.

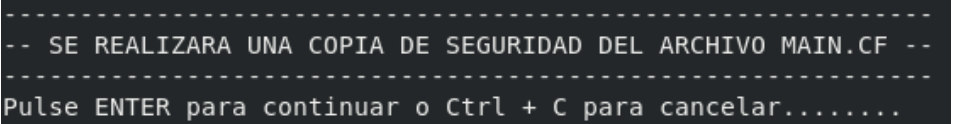
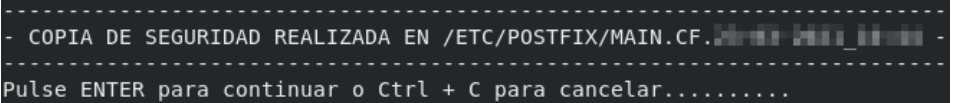
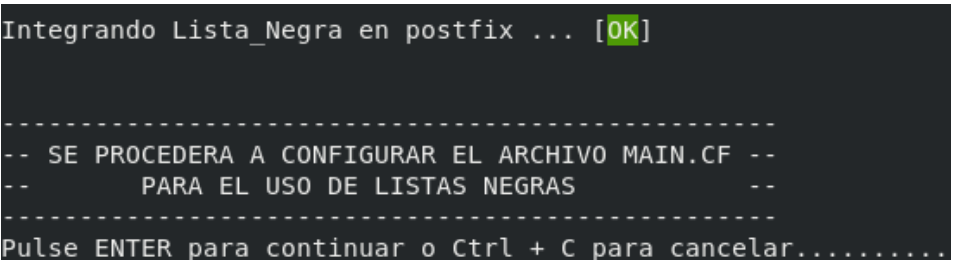
Paso	Descripción				
36.	Deberá editar el archivo de configuración main.cf de Postfix, para que el servidor postfix pueda detectar la nueva configuración. Introduzca la contraseña si se le solicita. <pre>\$ sudo gnome-text-editor /etc/postfix/main.cf &>/dev/null</pre> <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <tr> <td>alias_maps =</td><td>hash:/etc/postfix/alias</td></tr> </tbody> </table> 	Parámetro	Valor	alias_maps =	hash:/etc/postfix/alias
Parámetro	Valor				
alias_maps =	hash:/etc/postfix/alias				
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 Red Hat 8 Linux, ejecute el siguiente comando. Si ejecuta sin errores, no mostrará resultado por pantalla. <pre>\$ sudo newaliases</pre>				
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 Red Hat 8 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. <pre>\$ sudo groupadd "monitorización" \$ sudo chgrp -R "monitorización" /var/log/maillog \$ sudo usermod -a -G "monitorización" "usuarios designados"</pre> 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.				

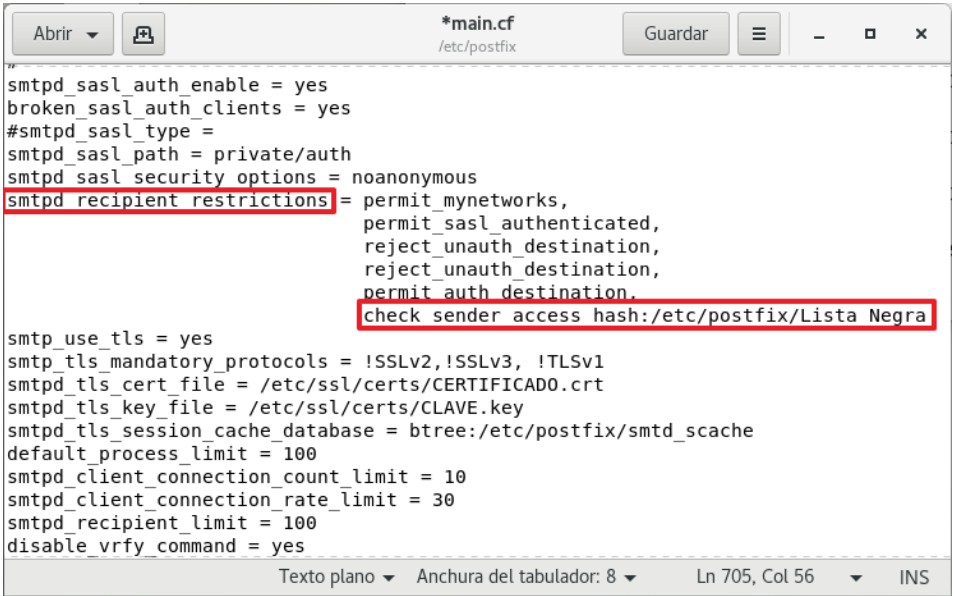
Paso	Descripción
40.	La modificación de permisos sobre la carpeta de logs de los correos electrónicos se realiza desde la línea de comandos, otorgando los permisos de escritura y lectura al usuario y al grupo designados. El usuario del sistema “root” será el poseedor de la carpeta para el correcto funcionamiento del sistema y poseerá los permisos equivalentes a “660”. <pre>\$ sudo chmod -660 /var/log/maillog</pre>
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”. <pre>\$ cd /Scripts</pre>
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 <u>entidades certificadoras autorizadas</u>. 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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso4_Seguridad.sh</pre> 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.
44.	El script iniciará realizando de una copia de seguridad del archivo a configurar, “/etc/postfix/main.cf”. Para continuar pulse la tecla “ENTER”. <pre> -- CCN-STIC-681A21-POSTFIX-PASO 4 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- -- SE REALIZARA UNA COPIA DE SEGURIDAD DEL ARCHIVO MAIN.CF -- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
45.	Se confirma la realización de la copia de seguridad. Deberá pulsar la tecla “ENTER” para continuar. <pre> - COPIA DE SEGURIDAD REALIZADA EN /ETC/POSTFIX/MAIN.CF.20-11-2021_09:08 - Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>

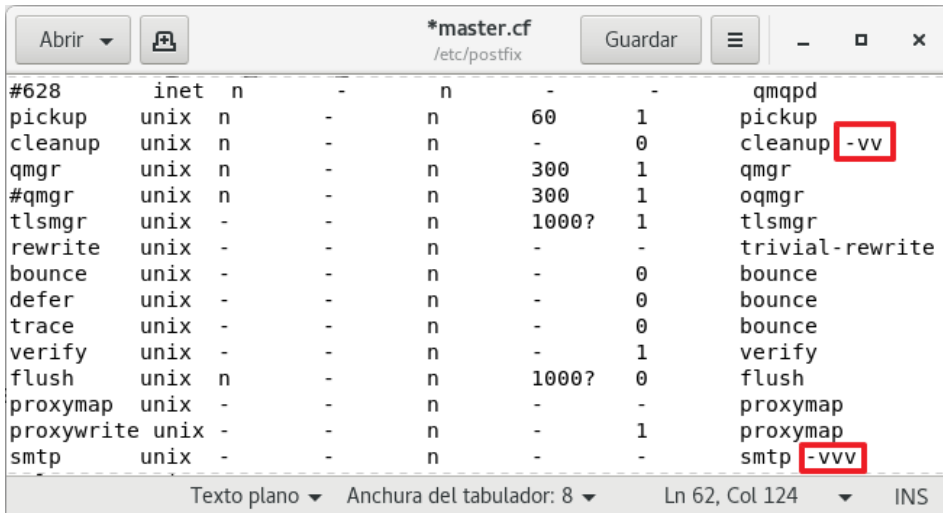
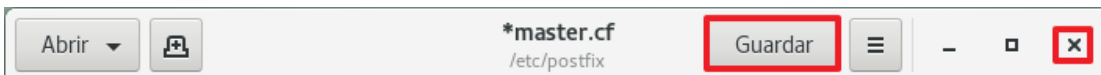
Paso	Descripción																																		
46.	Posteriormente se procederá a editar el archivo main.cf para el uso de ssl y tls. Pulse “ENTER” para continuar. <pre>-- SE PROCEDERA A CONFIGURAR EL ARCHIVO MAIN.CF -- -- PARA EL USO DE SSL Y TLS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar</pre>																																		
47.	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> <tr> <td>smtpd_tls_cert_file =</td><td>/etc/ssl/certs/<certificado.extension> Nota: Adapte la ruta y el nombre del certificado a la definida por su organización.</td></tr> <tr> <td>smtpd_tls_key_file =</td><td>/etc/ssl/certs/<clave.extension> Nota: Adapte la ruta y el nombre del certificado a la definida por su organización.</td></tr> <tr> <td>smtpd_tls_session_cache_database =</td><td>btree:/etc/postfix/smttd_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>	Parámetro	Valor	smtpd_sasl_auth_enable =	yes	broken_sasl_auth_clients =	yes	#smtpd_sasl_type =		smtpd_sasl_path =	private/auth	smtpd_sasl_security_options =	noanonymous	smtpd_recipient_restrictions =	permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination,reject_unauth_destination,permit_auth_destination	smtp_use_tls =	yes	smtp_tls_mandatory_protocols =	!SSLv2,!SSLv3, !TLSv1	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/smttd_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
Parámetro	Valor																																		
smtpd_sasl_auth_enable =	yes																																		
broken_sasl_auth_clients =	yes																																		
#smtpd_sasl_type =																																			
smtpd_sasl_path =	private/auth																																		
smtpd_sasl_security_options =	noanonymous																																		
smtpd_recipient_restrictions =	permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination,reject_unauth_destination,permit_auth_destination																																		
smtp_use_tls =	yes																																		
smtp_tls_mandatory_protocols =	!SSLv2,!SSLv3, !TLSv1																																		
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/smttd_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																																		

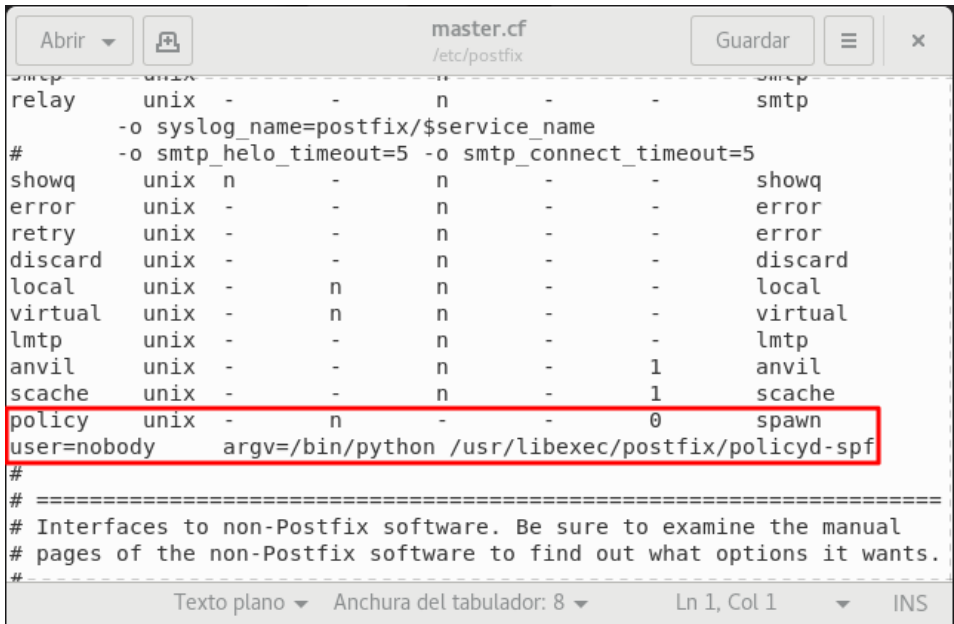
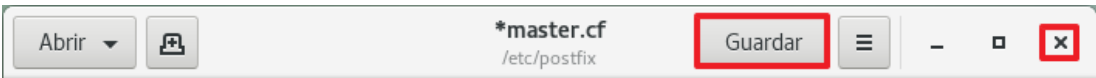
Paso	Descripción
	 Nota: Si detecta un parámetro duplicado elimine el que se encuentra por encima en el documento. Debe tener en cuenta que en el fichero de configuración de Postfix un parámetro sin ningún valor se considera como un valor válido de configuración. Así mismo, deberá tener en consideración 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. 
49.	El proceso termina con el mensaje mostrado como en la siguiente imagen. 
50.	Ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso5_Lista_negra.cf.sh</pre>

Paso	Descripción
51.	Para continuar con la ejecución del script, pulse “ENTER”. <pre> ----- -- CCN-STIC-681A21-POSTFIX-PASO 5 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- ----- ---- SE PROCEDE A CREAR UNA LISTA NEGRA DE CORREO ---- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
52.	Se va a proceder a realizar una configuración para que se tenga en consideración una lista negra de spam. El script creará un fichero de configuración. 
53.	Deberá insertar en el documento un listado de origen de correo electrónico a bloquear.  Nota: Adapte el documento con las necesidades específicas de su organización.

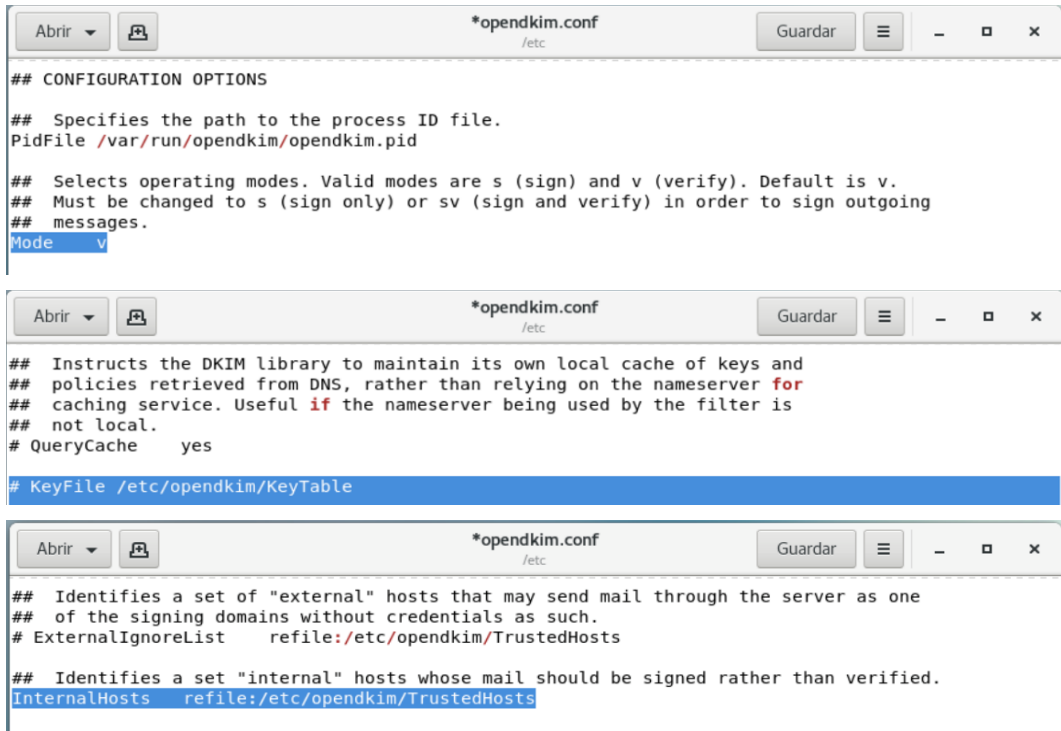
Paso	Descripción
54.	Seguidamente, deberá guardar el documento. Para ello pulse en “Guardar” y cierre el editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
55.	El script continuará realizando de una copia de seguridad del archivo a configurar, “/etc/postfix/main.cf”. Para continuar pulse la tecla “ENTER”. 
56.	Se confirma la realización de la copia de seguridad. Deberá pulsar la tecla “ENTER” para continuar. 
57.	El script procede a la comprobación de la integración de la “lista negra” de correo en el sistema Postfix. Para un correcto funcionamiento deberá modificar los siguientes parámetros en el archivo de configuración “main.cf”. Pulse “ENTER” para continuar. 

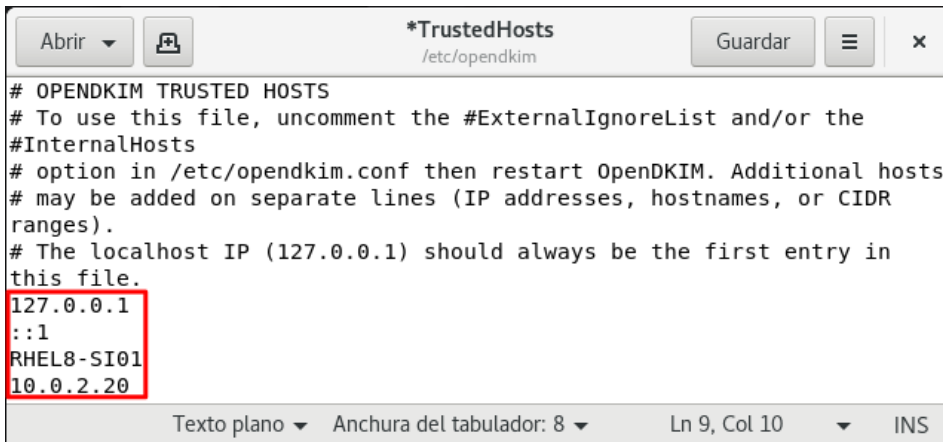
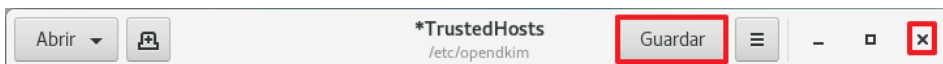
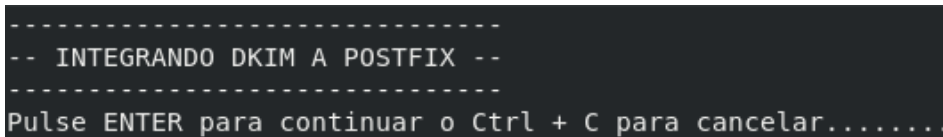
Paso	Descripción
58.	Añada la siguiente línea en el fichero de configuración de tal manera que se asemeje a la configuración de la siguiente imagen. smtpd_recipient_restrictions = check_sender_access hash:/etc/postfix/Lista_Negra 
59.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
60.	El proceso terminará con el siguiente mensaje. ---- CONFIGURACION TERMINADA ----

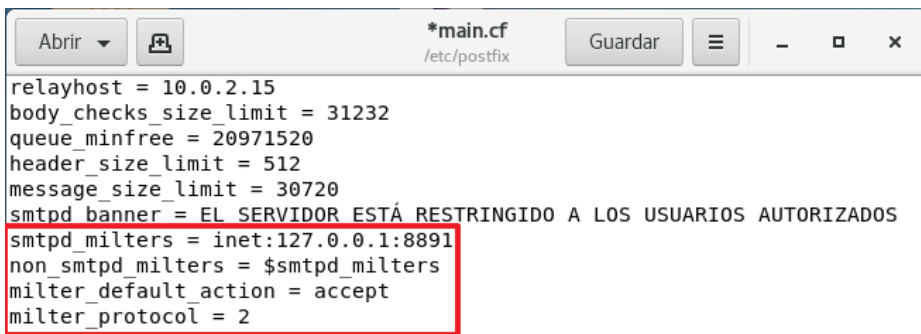
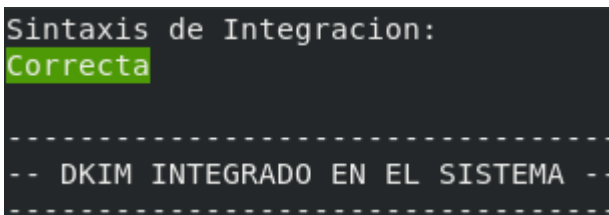
Paso	Descripción
61.	Posteriormente deberá modificar los registros del documento master.cf estableciendo un registro de actividad más elevado y detallado. Para tal fin, en una terminal, ejecute el siguiente comando. <pre>\$ sudo gnome-text-editor /etc/postfix/master.cf &>/dev/null</pre>  Nota: Deberá 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".
62.	Pulse "Guardar" y cierre el Editor de textos pulsando la "x" situada en la zona superior derecha de la ventana. 
63.	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". <pre>\$ cd /Scripts</pre>
64.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso6_spf.sh</pre> 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
65.	Para ello, primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar “ENTER” para continuar. <pre> ----- CCN-STIC-681A21-PAS06-spf Antes de ejecutar este script debe asegurarse que los ficheros y scripts se encuentran en el directorio /Scripts ----- SE CONFIGURA EL ARCHIVO MASTER.CF DE POSTFIX PARA INTEGRACION DE SPF. SE PROCEDE A REALIZAR UN COPIA DEL ARCHIVO MASTER.CF ----- COPIA REALIZADA EN /ETC/POSTFIX/MASTER.CF. ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
66.	El script editará el fichero master.cf. Inserte la siguiente línea en master.cf para configurar SPF. <pre> policy unix - n n - 0 spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf </pre>  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.
67.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 

Paso	Descripción
68.	El proceso finaliza con el siguiente mensaje, realizándose una comprobación de sintaxis de Postfix. <pre> configuracion de postfix Correcta ----- ---- CONFIGURACION TERMINADA ---- ----- </pre>
69.	Ejecute el siguiente comando para continuar con la configuración. Ingrese la contraseña si se le solicita. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso7_Dkim.sh</pre> 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.
70.	En un primer paso, se realiza una copia de seguridad de los archivos a configurar. Deberá pulsar “ENTER” para continuar. <pre> ----- -- CCN-STIC-681A21 PASO 7 DKim -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- ----- -- SE PROCEDE A CONFIGURAR EL ARCHIVO /ETC/OPENDKIM.CONF, -- -- /ETC/POSTFIX/MAIN.CF Y /ETC/OPENDKIM/TRUSTEDHOSTS -- -- SE REALIZARA UNA COPIA DE SEGURIDAD DE LOS ARCHIVOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>

Paso	Descripción										
71.	Se muestra la configuración a modificar en <code>opendkim.cf</code>, 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 border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </table> 	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
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										
72.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana.										
73.	Se procede a añadir la excepción de equipos de confianza. Pulse “ENTER” para continuar. <pre> ----- -- EQUIPOS DE CONFIANZA -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>										

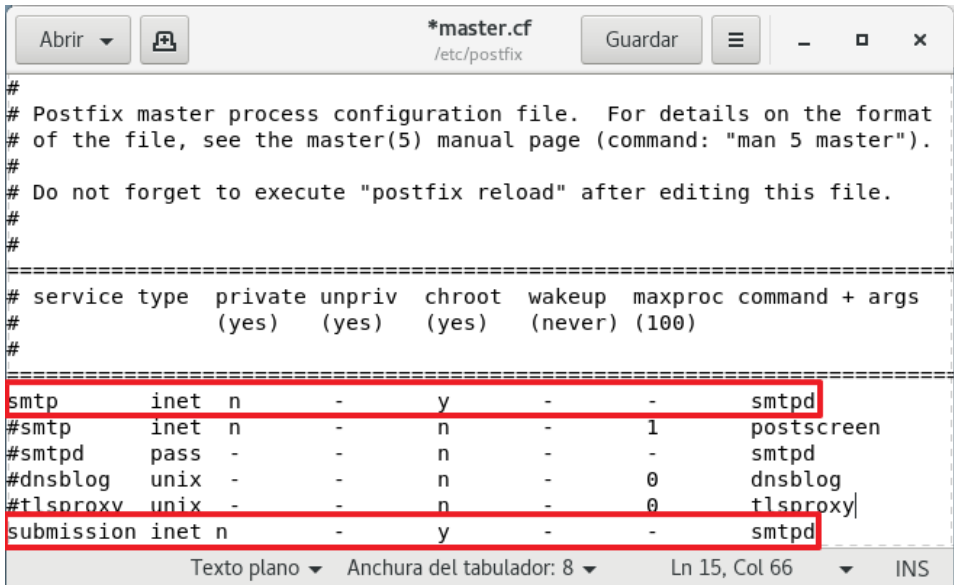
Paso	Descripción
74.	A continuación, se muestra, a modo de ejemplo, una configuración del archivo <code>/etc/openssl/TrustedHosts</code>.  <pre># OPENDKIM TRUSTED HOSTS # To use this file, uncomment the #ExternalIgnoreList and/or the #InternalHosts # option in /etc/openssl.conf then restart OpenDKIM. Additional hosts # may be added on separate lines (IP addresses, hostnames, or CIDR # ranges). # The localhost IP (127.0.0.1) should always be the first entry in # this file. 127.0.0.1 ::1 RHEL8-SI01 10.0.2.20</pre>
75.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
76.	Con la inserción de valores en el archivo <code>/etc/postfix/main.cf</code> se concluirá la integración de OpenDKim con Postfix. Pulse “ENTER” para continuar. 

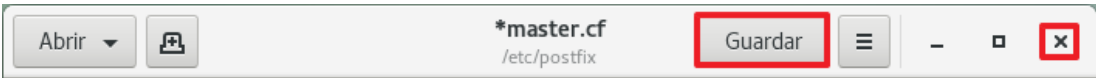
Paso	Descripción										
77.	El script editará el fichero de configuración, inserte los parámetros de seguridad recomendados contenidos en la siguiente tabla y adáptelos a los específicos de su organización. <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <tr> <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> </tbody> </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.	Parámetro	Valor	smtpd_milters =	inet:127.0.0.1:8891	non_smtpd_milters =	\$smtpd_milters	milter_default_action =	accept	milter_protocol =	2
Parámetro	Valor										
smtpd_milters =	inet:127.0.0.1:8891										
non_smtpd_milters =	\$smtpd_milters										
milter_default_action =	accept										
milter_protocol =	2										
78.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 										
79.	El script finaliza el proceso con una comprobación de sintaxis y el mensaje de finalización “DKIM INTEGRADO EN EL SISTEMA”. 										

Paso	Descripción
80.	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. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso8_comprobacion_configuracion.sh</pre> <pre>-- CCN-STIC-681A21-POSTFIX-PASO 8 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- -- SE COMPROBARA LA INTEGRIDAD DE LOS FICHEROS Y CARPETAS -- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>
81.	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. <pre>-- SE COMPROBARA LA INTEGRIDAD DE LOS FICHEROS Y CARPETAS -- Pulse ENTER para continuar o Ctrl + C para cancelar..... -rw-r--r--. 1 root root 10K Mar 20 15:50 /etc/postfix/main.cf main.cf SI pertenece a root Correcto -rw-r--r--. 1 root root 10K Mar 20 15:50 /etc/postfix/main.cf main.cf Permisos de acceso CORRECTOS Correcto -rw-r--r--. 1 root root 8.4K Mar 21 15:07 /etc/postfix/master.cf master.cf SI pertenece a root Correcto -rw-r--r--. 1 root root 8.4K Mar 21 15:07 /etc/postfix/master.cf master.cf Permisos de acceso CORRECTOS Correcto drwxr-xr-x. 20 root root 347 Mar 8 10:14 postfix /var/spool/postfix SI pertenece a root Correcto drwxr-xr-x. 20 root root 347 Mar 8 10:14 postfix /var/spool/postfix Permisos de acceso CORRECTOS Correcto -rw-rw----. 1 root monitorizacion 1.6K Mar 20 15:50 /var/log/maillog /var/log/maillog SI pertenece a root Correcto -rw-rw----. 1 root monitorizacion 1.6K Mar 20 15:50 /var/log/maillog /var/log/maillog Permisos de acceso CORRECTOS Correcto</pre> 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
82.	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”. <pre> -- SE VA A PROCEDER A LA COMPROBACION DE USUARIOS Y GRUPOS -- Pulse ENTER para continuar o Ctrl + C para cancelar..... mail:x:12:postfix,opendkim postdrop:x:90: postfix:x:89: Grupos existentes Correcto Debera crear el usuario postfix con shell /bin/false Valor NO conforme opendkim:x:975:972:OpenDKIM Milter:/run/opendkim:/sbin/nologin USUARIO opendkim EXISTE Debera modificar al usuario opendkim con shell /bin/false Valor NO conforme ----- ---- CONFIGURACION TERMINADA ---- ----- </pre> Nota: Si no existieran los grupos postdrop y postfix, o el usuario postfix, deberá reinstalar Postfix junto con su usuario y grupos correspondientes.
83.	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. <pre> \$ sudo chsh -s /bin/false postfix \$ sudo chsh -s /bin/false opendkim </pre> <pre> [usuario@RHEL8-SI01 Scripts]\$ sudo chsh -s /bin/false postfix Cambiando intérprete de órdenes para postfix. chsh: No se ha cambiado el intérprete de órdenes. [usuario@RHEL8-SI01 Scripts]\$ sudo chsh -s /bin/false opendkim Cambiando intérprete de órdenes para opendkim. Se ha cambiado el intérprete de órdenes. [usuario@RHEL8-SI01 Scripts]\$ </pre>

Paso	Descripción
84.	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”. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso7_comprobacion_configuracion.sh</pre> <pre> ----- -- SE VA A PROCEDER A LA COMPROBACION DE USUARIOS Y GRUPOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... mail:x:12:postfix,opendkim postdrop:x:90: postfix:x:89: Grupos existentes Correcto postfix:x:89:89:./var/spool/postfix:/bin/false Usuario existente y configurado correctamente Correcto opendkim:x:975:972:OpenDKIM Milter:/run/opendkim:/bin/false USUARIO opendkim EXISTE opendkim:x:975:972:OpenDKIM Milter:/run/opendkim:/bin/false USUARIO opendkim CONFIGURADO: CORRECTO ----- ---- CONFIGURACION TERMINADA ---- ----- </pre>
85.	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. <pre> \$ sudo systemctl unmask postfix.service \$ sudo systemctl start postfix.service \$ sudo systemctl enable postfix.service \$ sudo systemctl restart opendkim </pre>
86.	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”. <pre>\$ cd /Scripts</pre> Nota: El script presentado en esta guía ejecuta, en su parte, el script original dl fabricante.

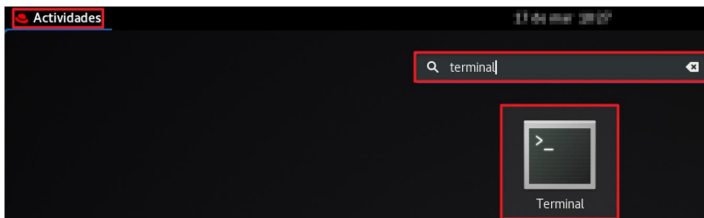
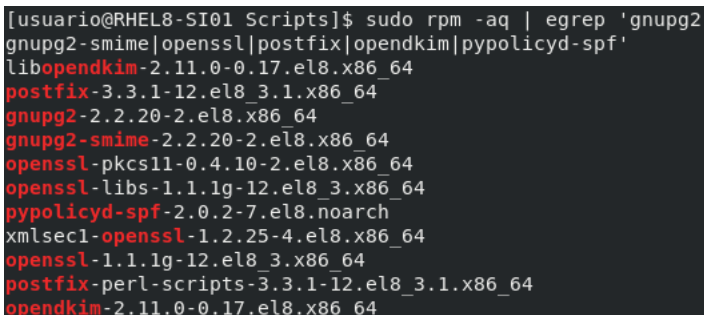
Paso	Descripción										
87.	Ejecute el siguiente comando para continuar con la configuración. Si se lo solicitase, ingrese la contraseña del usuario administrador. <pre>\$ sudo sh CCN-STIC-681A21_ENS_ALTA_Paso9_master.cf_chroot.sh</pre>										
88.	Se procede a realizar una jaula chroot sobre los procesos de Postfix. Para ello primero se realiza una copia de seguridad del archivo master.cf. Deberá pulsar "ENTER" para continuar. <pre> -- CCN-STIC-681A21-PASO 9 Chroot -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- -- -- SE PROCEDE A REALIZAR UNA JAULA CHROOT A POSTFIX -- -- -- SE REALIZARA UNA COPIA DE SEGURIDAD DEL ARCHIVO MASTER.CF -- -- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>										
89.	Posteriormente se abrirá, con el editor de textos el archivo "/etc/postfix/master.cf". Deberá modificar los siguientes valores. <table border="1"> <thead> <tr> <th>Valor Inicial</th><th>Valor final</th></tr> </thead> <tbody> <tr> <td>smtp inet n - n - -</td><td>smtp inet n - y - -</td></tr> <tr> <td>smtpd</td><td>smtpd</td></tr> <tr> <td>#submission inet n - n - -</td><td>submission inet n - y - -</td></tr> <tr> <td>smtpd</td><td>smtpd</td></tr> </tbody> </table>	Valor Inicial	Valor final	smtp inet n - n - -	smtp inet n - y - -	smtpd	smtpd	#submission inet n - n - -	submission inet n - y - -	smtpd	smtpd
Valor Inicial	Valor final										
smtp inet n - n - -	smtp inet n - y - -										
smtpd	smtpd										
#submission inet n - n - -	submission inet n - y - -										
smtpd	smtpd										
90.	En la siguiente imagen se muestra como deberán quedar definidos los parámetros en el archivo de configuración según la tabla anterior. 										

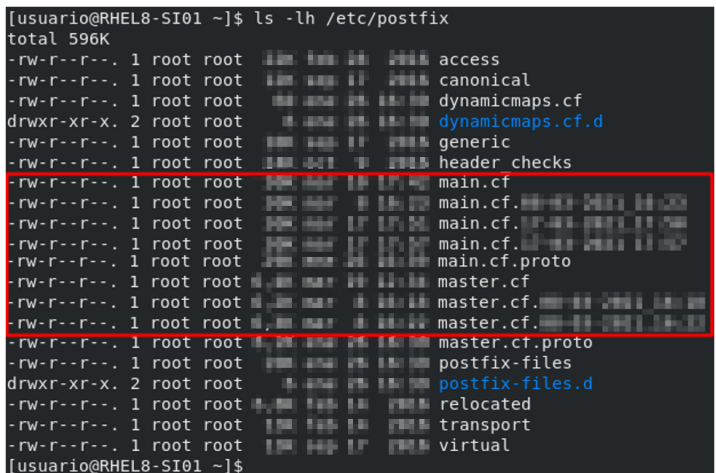
Paso	Descripción
91.	Pulse “Guardar” y cierre el Editor de textos pulsando la “x” situada en la zona superior derecha de la ventana. 
92.	La ejecución del script termina con una comprobación de funcionamiento de postfix. <pre>postfix/postfix-script: refreshing the Postfix mail system ----- -- CONFIGURACION REALIZADA -- -----</pre>
93.	Se procede a habilitar los servicios necesarios para el correcto funcionamiento del sistema. Ejecute los siguientes comandos. <pre>\$ 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</pre> 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. <pre>\$ sudo shutdown -r</pre>

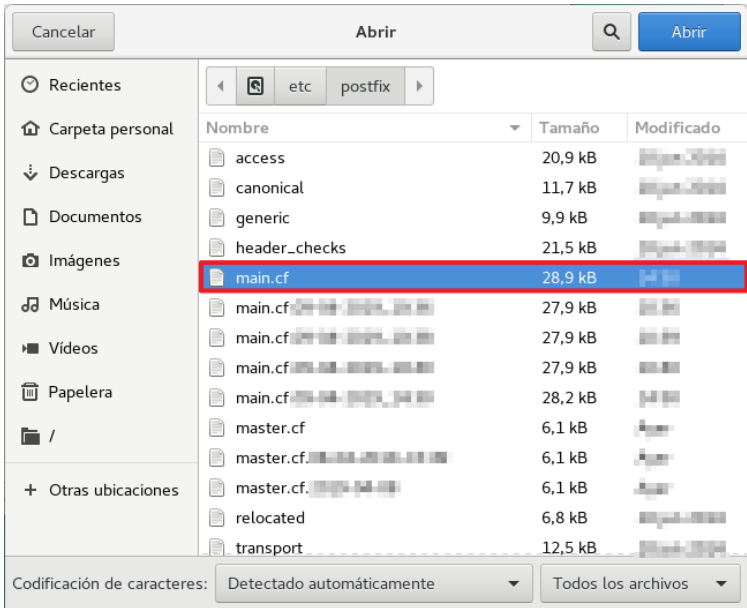
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE POSTFIX EN SERVIDOR REDHAT 8 ENS CATEGORÍA ALTA

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.

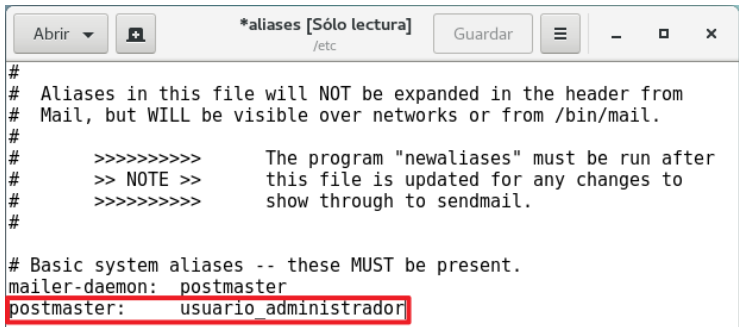
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En uno de los equipos Red Hat 8, inicie sesión con una cuenta que tenga privilegios de administración.
2. Inicie la Terminal de Linux.		Diríjase a la barra de tareas superior, pulse sobre “Actividades”, escriba y seleccione “Terminal”. 
3. Verifique que se encuentren instalados los paquetes necesarios.		En la “terminal” ejecute el siguiente comando. <pre>\$ sudo rpm -aq egrep 'gnupg2 gnupg2-smime openssl postfix opendkim pypolicyd-spf'</pre>  Nota: Deberá comprobar que las versiones de los paquetes que aquí se comprueban, se encuentran en sus últimas versiones.

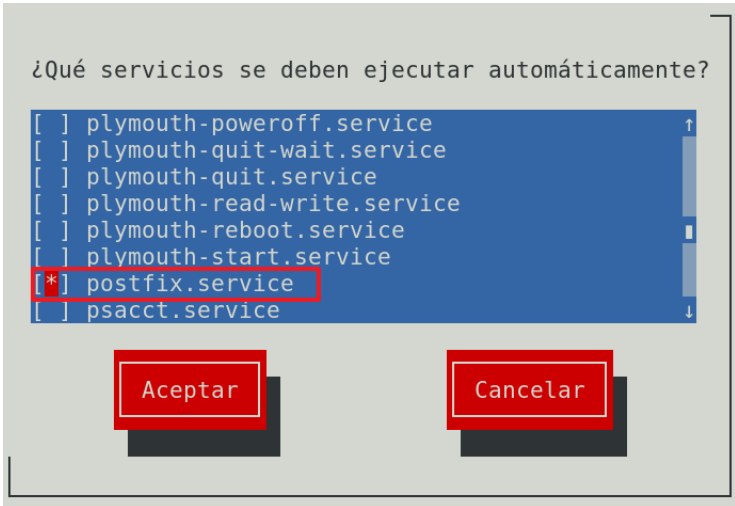
Comprobación	OK/NOK	Cómo hacerlo
	Parámetros	
		gnupg2-smime-[versión actualizada]
		openssl-[versión actualizada]
		postfix-[versión actualizada]
		pypolicyd-spf-[versión actualizada]
		gnupg2-[versión actualizada]
		openssl-libs-[versión actualizada]
		postfix-perl-scripts-[versión actualizada]
		xmlsec1-openssl-[versión 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	
		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. <pre>\$ ls -lh /etc/postfix \$ ls -lh /etc grep aliases</pre> Revise que se han realizado las correspondientes copias de seguridad de los archivos según la ejecución de los scripts correspondientes.  <pre>[usuario@RHEL8-SI01 ~]\$ ls -lh /etc/postfix total 596K -rw-r--r--. 1 root root 12K Jan 10 10:00 access -rw-r--r--. 1 root root 12K Jan 10 10:00 canonical -rw-r--r--. 1 root root 12K Jan 10 10:00 dynamicmaps.cf drwxr-xr-x. 2 root root 12K Jan 10 10:00 dynamicmaps.cf.d -rw-r--r--. 1 root root 12K Jan 10 10:00 generic -rw-r--r--. 1 root root 12K Jan 10 10:00 header_checks -rw-r--r--. 1 root root 12K Jan 10 10:00 main.cf -rw-r--r--. 1 root root 12K Jan 10 10:00 main.cf.proto -rw-r--r--. 1 root root 12K Jan 10 10:00 master.cf -rw-r--r--. 1 root root 12K Jan 10 10:00 master.cf.proto -rw-r--r--. 1 root root 12K Jan 10 10:00 postfix-files drwxr-xr-x. 2 root root 12K Jan 10 10:00 postfix-files.d -rw-r--r--. 1 root root 12K Jan 10 10:00 relocated -rw-r--r--. 1 root root 12K Jan 10 10:00 transport -rw-r--r--. 1 root root 12K Jan 10 10:00 virtual [usuario@RHEL8-SI01 ~]\$</pre> Nota: Tenga en consideración que poseerá tantas copias como veces haya ejecutado los scripts.

Comprobación	OK/NOK	Cómo hacerlo
	Configuración	
		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	

Comprobación	OK/NOK	Cómo hacerlo	
Parámetros		Valor	OK/NOK
smtpd_recipient_restrictions		permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, permit_auth_destination, check_sender_access hash:/etc/postfix/Lista_Negra	
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/smt_d_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. <pre> \$ 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 </pre>	

Comprobación	OK/NOK	Cómo hacerlo		
	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.		
		<pre>\$ ls -lh /etc/postfix/main.cf grep '\-rw-r--r--'</pre> <pre>\$ ls -lh /etc/postfix/master.cf grep '\-rw-r--r--'</pre> <pre>\$ ls -lh /var/spool/ grep postfix grep rwxr-xr-x.</pre> <pre>\$ ls -lh /var/log/maillog grep '\-rw\-----'</pre>		
	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.		
		<pre>\$ cat /etc/passwd egrep "postfix /bin/false "</pre> <pre>\$ cat /etc/group egrep "postfix postdrop"</pre> <pre>\$ cat /etc/passwd egrep "opendkim /bin/false "</pre> <pre>\$ cat /etc/group egrep " opendkim"</pre>		
	Configuración		Valor	OK/NOK
	Usuario: postfix		Existe	
	Shell: postfix		/bin/false	
	Grupo: postfix		Existe	
	Grupo: postdrop		Existe	
	Usuario: opendkim		Existe	
	Shell: opendkim		/bin/false	
	Grupo: opendkim		Existe	

Comprobación	OK/NOK	Cómo hacerlo															
10.Cambio de usuario de Postmaster		Compruebe que se han modificado los siguientes parámetros dentro del archivo aliases. Para ello dirijase 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. 															
11.Comprobación de los certificados OpenSSL.		En la “terminal” ejecute el siguiente comando para comprobar la creación de los certificados. <pre>\$ ls -lh /etc/ssl/certs</pre> Nota: Los valores deben de ser coincidentes con los nombres y configuraciones específicos de su organización. <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>	Configuración	Valor	OK/NOK	“NOMBREFIRMA”.“extensión”	Existencia		“CLAVEPRIVADA”.key	Existencia		Permisos “CLAVEPRIVADA”.key	-r-----		Permisos “NOMBREFIRMA”.“extensión”	-rw-r--r--	
Configuración	Valor	OK/NOK															
“NOMBREFIRMA”.“extensión”	Existencia																
“CLAVEPRIVADA”.key	Existencia																
Permisos “CLAVEPRIVADA”.key	-r-----																
Permisos “NOMBREFIRMA”.“extensión”	-rw-r--r--																

Comprobación	OK/NOK	Cómo hacerlo														
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 (*).														
		<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>	Configuración	Valor	OK/NOK	postfix.service	Activo		opendkim.service	Activo						
	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														
		<table><tr><th>Parámetros</th><th>OK/NOK</th></tr><tr><td>Etc</td><td></td></tr><tr><td>Lib</td><td></td></tr><tr><td>Lib64</td><td></td></tr><tr><td>Private</td><td></td></tr><tr><td>Public</td><td></td></tr><tr><td>usr</td><td></td></tr></table>	Parámetros	OK/NOK	Etc		Lib		Lib64		Private		Public		usr	
	Parámetros	OK/NOK														
	Etc															
	Lib															
	Lib64															
Private																
Public																
usr																

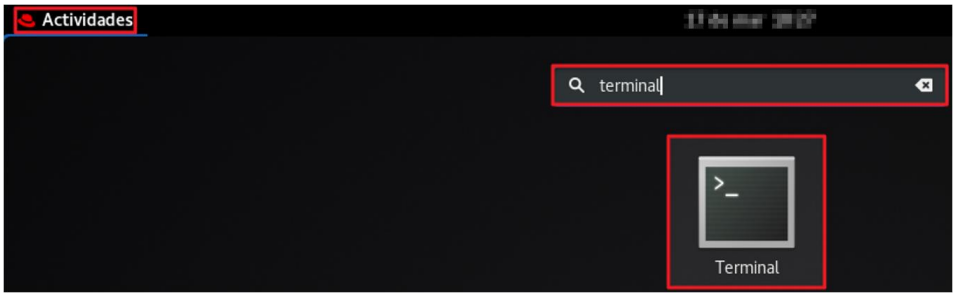
Comprobación	OK/NOK	Cómo hacerlo									
14.Configuración del archivo master.cf		Compruebe que se han modificado los siguientes parámetros del archivo master.cf. Para ello diríjase a la barra de tareas superior, pulse sobre “Aplicaciones” y en el apartado “Accesorios” seleccione “Editor de textos”. Abra el archivo /etc/postfix/master.cf Abrir  master.cf /etc/postfix Guardar      <pre># ===== # service type private unpriv chroot wakeup maxproc command + args # (yes) (yes) (yes) (never) (100) ===== smtp inet n - y - - smtpd #smtp inet n - n - 1 postscreen #smtpd pass - - n - - smtpd #dnsblog unix - - n - 0 dnsblog #tlsproxy unix - - n - 0 tlsproxy submission inet n - y - - smtpd # -o syslog_name=postfix/submission # -o smtpd_tls_security_level=encrypt # -o smtpd_sasl_auth_enable=yes # -o smtpd_reject_unlisted_recipient=no # -o smtpd_client_restrictions=\$mua_client_restrictions # -o smtpd_helo_restrictions=\$mua_helo_restrictions</pre> Texto plano  Anchura del tabulador: 8  Ln 1, Col 1  INS <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>	Parámetros	OK/NOK	smtp inet n - y - - smtpd		submission inet n - y - - smtpd		policyunix-nn-0spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf		
Parámetros	OK/NOK										
smtp inet n - y - - smtpd											
submission inet n - y - - smtpd											
policyunix-nn-0spawn user=nobody argv=/bin/python /usr/libexec/postfix/policyd-spf											
15.Comprobación de la existencia de una lista negra.		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. <pre>\$ ls -lr /etc/postfix</pre> -rw-r--r--. 1 root root 30318 main.cf -rw-r--r--. 1 root root 12288 Lista_Negra.db -rw-r--r--. 1 root root 116 Lista_Negra -rw-r--r--. 1 root root 23802 header_checks -rw-r--r--. 1 root root 10221 generic drwxr-xr-x. 2 root root 6 dynamicmaps.cf.d -rw-r--r--. 1 root root 60 dynamicmaps.cf -rw-r--r--. 1 root root 12000 canonical -rw-r--r--. 1 root root 21535 access <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>	Fichero	Comprobación	OK/NOK	[nombre fichero lista negra]	Existencia		[nombre fichero base de datos].db	Existencia	
Fichero	Comprobación	OK/NOK									
[nombre fichero lista negra]	Existencia										
[nombre fichero base de datos].db	Existencia										

ANEXO A.5. TAREAS ADICIONALES

ANEXO A.5.1. 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 “3 AMAVIS”.

1. PAQUETES ADICIONALES

Paso	Descripción
1.	Inicie sesión en el equipo Red Hat 8 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 “Actividades”, escriba y seleccione “Terminal”. 
3.	Cree la carpeta “Scripts”. Para ello, en el terminal, ejecute el comando siguiente. <pre>\$ cd /</pre> Para crear la carpeta en la ubicación ejecute el siguiente comando. <pre>\$ sudo mkdir Scripts</pre> Nota: Puede comprobar que la carpeta ha sido creada ejecutando <code>ls /</code>.
4.	Introduzca el CD/DVD que contenga los scripts correspondientes a la guía “CCN-STIC-681A21- IMPLEMENTACIÓN DE SEGURIDAD EN POSTFIX SOBRE RED HAT 8 LINUX”. Introduzca las credenciales si se lo solicita.

Paso	Descripción
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”. Para ello, ejecute el comando siguiente. <pre>\$ sudo cp /run/media/usuario/ISO\ Label/Scripts/ENS_ADICIONALES/* /Scripts/</pre> 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.
6.	Expulse el CD/DVD de la unidad y diríjase a la carpeta “Scripts”. Para ello ejecute el comando siguiente. <pre>\$ cd /Scripts</pre>
7.	Se va a comprobar los paquetes necesarios para la instalación de las diversas soluciones descritas durante el desarrollo de este punto (ANEXO A.5.1 TAREAS DE SEGURIDAD). Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. <pre>\$ sudo sh CCN-STIC-681A21_ENS_Paso1_ADICIONALES_comprobacion_paquetes_necesarios.sh</pre>
8.	Pulse “ENTER” para continuar. <pre>----- -- CCN-STIC-681A21-ADICIONALES-PASO 1 -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>

Paso	Descripción
9.	Seguidamente se comprobará la instalación de los paquetes necesarios. Pulse “ENTER” para continuar. <pre> ----- -- SE COMPROBARAN PROGRAMAS Y PAQUETES NECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.. Debe instalar spamassassin Debe instalar clamav Debe instalar clamav-update Debe instalar amavis Debe instalar clamav-data Debe instalar clamd ----- ---- CONFIGURACION TERMINADA ---- ----- </pre> Nota: Los resultados mostrados en pantalla pueden variar dependiendo de las configuraciones específicas de su organización.
10.	Instale o actualice los componentes que el script muestre en color rojo por medio de los siguientes comandos. <pre> \$ sudo yum install <Paquete1 Paquete2 Paquete 3 ...> \$ sudo yum update <Paquete1 Paquete2 Paquete 3 ...> </pre> <pre> [usuario@RHEL8-SI01 ENS_ADICIONALES]\$ yum install spamas sassin clamav clamav-update amavis clamav-data clamd </pre>

Paso	Descripción
11.	Ejecute el script de nuevo para comprobar que la configuración es correcta. <pre>\$ sudo sh CCN-STIC-681A21_ENS_Paso1_ADICIONALES_comprobacion_paquetes_necesarios.sh</pre> <pre> spamassassin-3.4.2-10.el8.x86_64 spamassassin Instalado clamav-data-0.103.0-1.el8.noarch clamav-filesystem-0.103.0-1.el8.noarch clamav-update-0.103.0-1.el8.x86_64 clamav-lib-0.103.0-1.el8.x86_64 clamav-0.103.0-1.el8.x86_64 clamav Instalado clamav-update-0.103.0-1.el8.x86_64 clamav-update Instalado amavis-2.12.1-5.el8.noarch amavis Instalado clamav-data-0.103.0-1.el8.noarch clamav-data Instalado clamd-0.103.0-1.el8.x86_64 clamd Instalado ----- ---- CONFIGURACION TERMINADA ---- ----- </pre>
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. <pre> \$ sudo cp -f /etc/mail/spamassassin/local.cf /home/usuario/BACKUP \$ sudo cp -f /etc/freshclam.conf /home/usuario/BACKUP \$ sudo cp -f /usr/lib/systemd/system/clamd@.service /home/usuario/BACKUP </pre> 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.

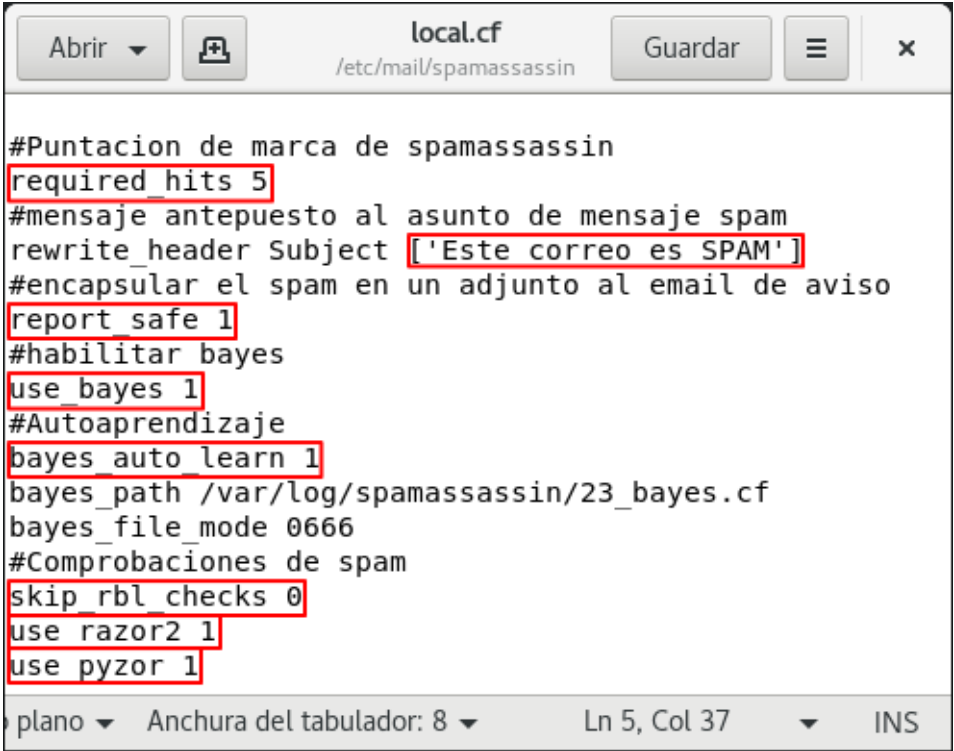
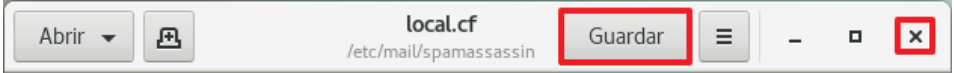
2. SPAMASSASSIN

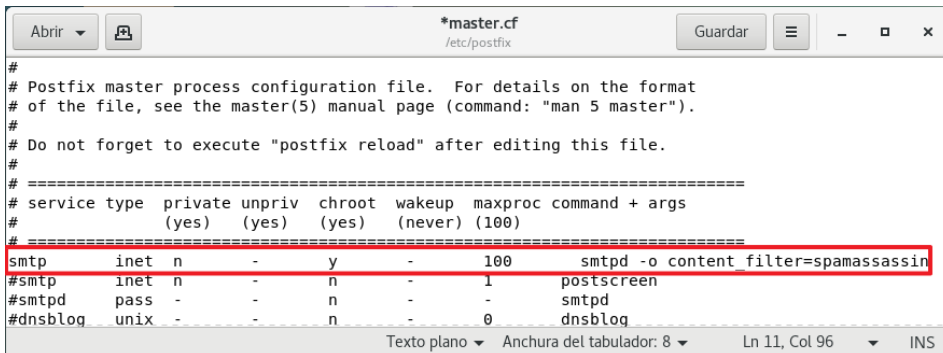
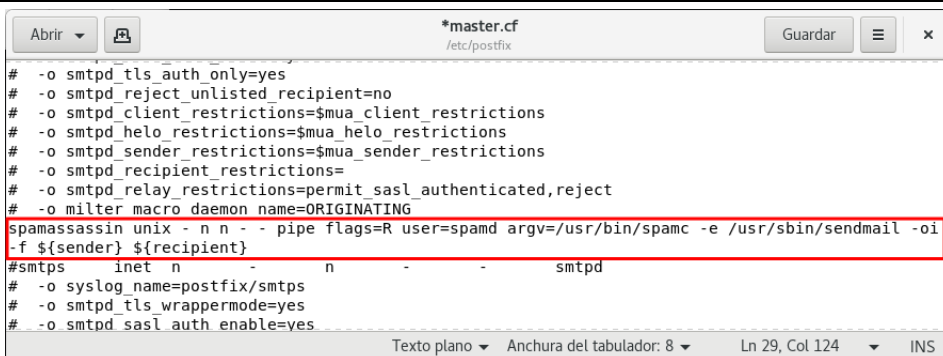
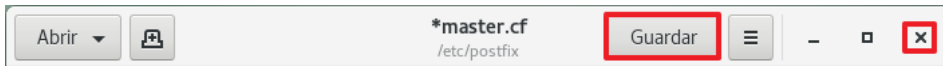
SpamAssassin es una herramienta de filtrado de spam en los servidores de correo electrónico. Spamassassin analiza los mensajes de correo determinando la probabilidad de que sean spam.

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 “3 AMAVIS” de la presente guía.

Paso	Descripción
1.	Inicie sesión en el equipo Red Hat 8 Linux que está asegurando, con una cuenta administrador o sudoers.
2.	Diríjase al directorio “/Scripts”. <pre>\$ cd /Scripts</pre>
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. <pre>\$ sudo groupadd spamd \$ sudo useradd -g spamd -s /bin/false -d /var/log/spamassassin spamd \$ sudo chown spamd:spamd /var/log/spamassassin</pre>
4.	Ejecute el siguiente comando y siga los pasos que le indica. Ingrese la contraseña si se le solicita. <pre>\$ sudo sh CCN-STIC-681A21_ENS_Adicional_Spam.sh</pre>
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. <pre>----- -- CCN-STIC-681A21-POSTFIX_ENS_SPAM -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- ----- -- SE REALIZARA UNA COPIA DE SEGURIDAD DEL ARCHIVO -- -- /ETC/MAIL/SPAMASSASSIN/LOCAL.CF -- -- /ETC/POSTFIX/MASTER.CF -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>

Paso	Descripción																		
6.	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 border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <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> </tbody> </table> 	Parámetro	Valor	required_hits	5	rewrite_header Subject	['\$mensaje']	report_safe	1	use_bayes	1	bayes_auto_learn	1	skip_rbl_checks	0	use_razor2	1	use_pyzor	1
Parámetro	Valor																		
required_hits	5																		
rewrite_header Subject	['\$mensaje']																		
report_safe	1																		
use_bayes	1																		
bayes_auto_learn	1																		
skip_rbl_checks	0																		
use_razor2	1																		
use_pyzor	1																		
7.	Pulse sobre “Guardar” y cierre el editor de textos pulsando sobre la “x” en la esquina superior derecha de la ventana. 																		

Paso	Descripción						
8.	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 border="1"> <thead> <tr> <th>Valor inicial</th><th>Valor final</th></tr> </thead> <tbody> <tr> <td>smtp inet n - yes - 100</td><td>smtp inet n - y - 100</td></tr> <tr> <td>smtpd</td><td>smtpd -o content_filter=spamassassin</td></tr> </tbody> </table> 	Valor inicial	Valor final	smtp inet n - yes - 100	smtp inet n - y - 100	smtpd	smtpd -o content_filter=spamassassin
Valor inicial	Valor final						
smtp inet n - yes - 100	smtp inet n - y - 100						
smtpd	smtpd -o content_filter=spamassassin						
9.	Añada la siguiente línea al final del archivo de configuración. <pre>spamassassin unix - n n - - pipe flags=R user=spamd argv=/usr/bin/spamc -e /usr/sbin/sendmail -oi -f \${sender} \${recipient}</pre> 						
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 una comprobación de la sintaxis de configuración de postfix y con el siguiente mensaje. <pre>postfix/postfix-script: refreshing the Postfix mail system ----- --- CONFIGURACION TERMINADA --- -----</pre>						

Paso	Descripción
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. <pre>\$ sudo spamassassin --lint</pre> 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-681A21-ENS_Adicional_Spam.sh”.

3. AMAVIS Y CLAMAV

Nota: En el actual AMAVIS, cuando se realiza la instalación, por defecto instala clamAV y spamassassin.

Paquetes necesarios para el correcto funcionamiento de Amavis:

Nombre Paquete	Versión
Amavis	2.12.1-5.el8
altermime	0.3.10-21.el8
bzip2	1.0.6-26.el8
clamav-data	0.103.2-1.el8
clamav-filessystem	0.103.2-1.el8
clamav-lib	0.103.2-1.el8
clamav-update	0.103.2-1.el8
clamd	0.103.2-1.el8
Cpio	2.12-10.el8
File	5.33-16.el8_3.1
Gzip	1.9-12.el8
Libprelude	5.2.0-1.el8
lrzsz	0.12.20-43.el8
lzip	1.21-1.el8
lz4	1.8.3-2.el8
Lzop	1.03-20.el8
perl-Authen-SASL	2.16-13.el8
perl-BerkeleyDB	0.63-2.el8
perl-Convert-ASN1	0.27-17.el8
perl-Convert-BinHex	1.125-13.el8
perl-Crypt-OpenSSL-Bignum	0.09-5.el8
perl-Crypt-OpenSSL-RSA	0.31-1.el8
perl-Crypt-OpenSSL-Random	0.15-3.el8
perl-Data-Dump	1.23-7.module+el8.3.0+6498+9eecfe51
perl-Digest-HMAC	1.03-17.module+el8.3.0+6498+9eecfe51
perl-Encode-Detect	1.01-28.el8

Nombre Paquete	Versión
perl-Error	1:0.17025-2.el8
perl-File-LibMagic	1.16-9.el8
perl-File-Listing	6.04-17.module+el8.3.0+6498+9eecfe51
perl-GSSAPI	0.28-23.el8
perl-HTML-Parser	3.72-15.module+el8.3.0+6498+9eecfe51
perl-HTML-Tagset	3.20-34.module+el8.3.0+6498+9eecfe51
perl-HTTP-Cookies	6.04-2.module+el8.3.0+6498+9eecfe51
perl-HTTP-Date	6.02-19.module+el8.3.0+6498+9eecfe51
perl-HTTP-Message	6.18-1.module+el8.3.0+6498+9eecfe51
perl-HTTP-Negotiate	6.01-19.module+el8.3.0+6498+9eecfe51
perl-IO-HTML	1.001-11.module+el8.3.0+6498+9eecfe51
perl-IO-Multiplex	1.16-9.el8
perl-IO-Socket-INET6	2.72-12.el8
perl-IO-stringy	2.111-9.el8
perl-JSON	2.97.001-2.el8
perl-LWP-MediaTypes	6.02-15.module+el8.3.0+6498+9eecfe51
perl-MIME-tools	5.509-9.el8
perl-Mail-DKIM	0.54-1.el8
perl-Mail-SPF	2.9.0-15.el8
perl-MailTools	2.20-2.el8
perl-NTLM	1.09-17.module+el8.3.0+6498+9eecfe51
perl-Net-DNS	1.15-1.el8
perl-Net-HTTP	6.17-2.module+el8.3.0+6498+9eecfe51
perl-Net-LibIDN	0.12-35.el8
perl-Net-SMTP-SSL	1.04-5.el8
perl-Net-Server	2.009-3.el8
perl-NetAddr-IP	4.079-7.el8
perl-Razor-Agent	2.85-33.el8
perl-Socket6	0.28-6.el8
perl-Text-Soundex	3.05-8.el8
perl-Text-Unidecode	1.30-5.el8
perl-TimeDate	1:2.30-15.module+el8.3.0+6498+9eecfe51
perl-Try-Tiny	0.30-7.module+el8.3.0+6498+9eecfe51
perl-Unix-Syslog	1.1-29.el8
perl-WWW-RobotRules	6.02-18.module+el8.3.0+6498+9eecfe51
perl-common-sense	3.7.4-8.el8
perl-libwww-perl	6.34-1.module+el8.3.0+6498+9eecfe51
Procmail	3.22-47.el8
Spax	3.10.22-30.el8
zip	1.9-7.el8
Unzip	0.103.2-1.el8

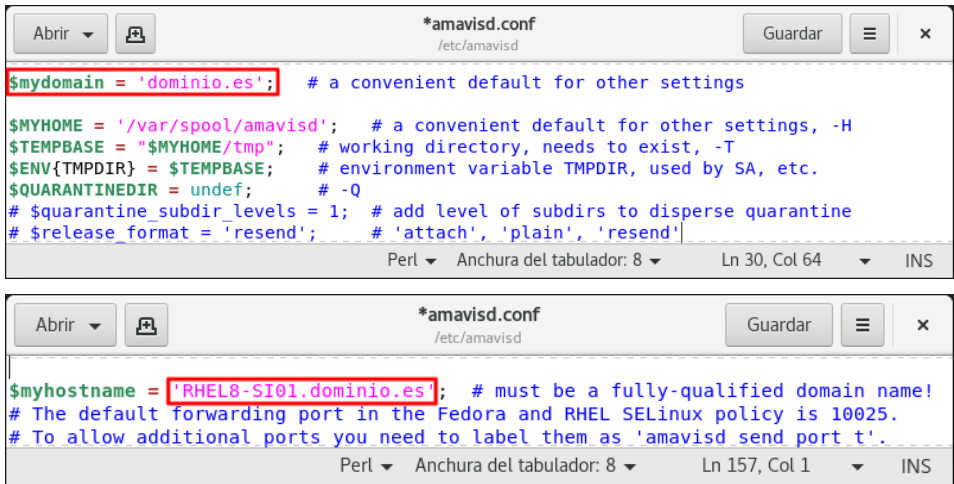
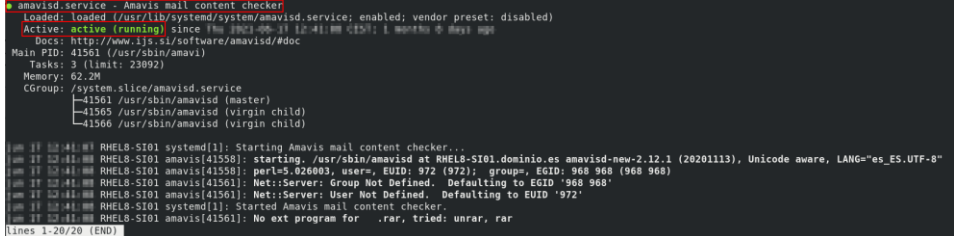
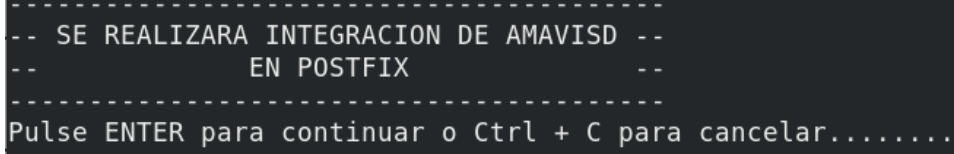
Nombre Paquete	Versión
Arj	1.5.3-13.el8
cabextract	3.0-23.el8
freeze	2.5.0-26.el8
Nomarch	1.4-21.el8
p7zip	16.02-16.el8
p7zip-plugins	16.02-16.el8
perl-Convert-TNEF	0.18-17.el8
perl-Convert-UUlib	3:1.8-1.el8
perl-LDAP	1:0.66-7.el8
spamassassin	3.4.2-10.el8
unzoo	4.4-27.el8

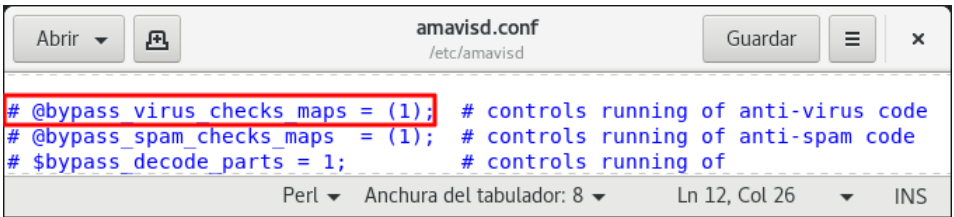
Amavis es una solución de código abierto para el correo electrónico que se ocupa del filtrado de mensajes, protegiendo el sistema de correo electrónico de mensajes no deseados, de virus y de otros programas maliciosos. Actúa como una interfaz entre el MTA y los filtros de contenido antivirus, filtro 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 Red Hat 8 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-681A21_ENS_Adicional_Amavis.sh

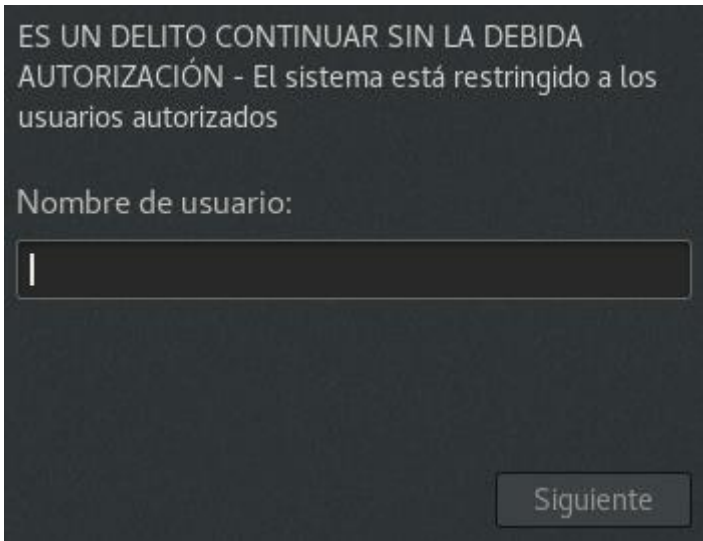
Paso	Descripción
4.	La solución Amavis integra ClamAV, como filtro antivirus. Se procede a realizar los pasos necesarios para completar dicha integración en el sistema. El proceso comienza con la comprobación de la instalación de la herramienta “amavis”. <pre> ----- -- CCN-STIC-681A21_ENS_ADICIONAL_AMAVIS_CLAMAV -- -- Antes de ejecutar este script debe asegurarse que los ficheros -- -- y scripts se encuentran en el directorio /Scripts -- ----- Amavis se encuentra instalado en su sistema. Se aconseja el uso de la versión amavisd-new-2.12.1 \ (20201113\), para el correcto uso de esta guía. Su versión de amavis es: amavisd-new-2.12.1 (20201113) Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
5.	Se procede a configurar el servicio de “amavisd”, para tal tarea se realizará una copia de seguridad de los archivos modificados. Deberá pulsar la tecla “ENTER” para continuar con el proceso de configuración. <pre> ----- -- SE VA A PROCEDER A CONFIGURAR AMAVISED -- -- PARA ELLO SE VA A REALIZAR COPIA DE SEGURIDAD -- -- DE LOS SIGUIENTES ARCHIVOS DE CONFIGURACION -- ----- /etc/amavisd/amavisd.conf /etc/postfix/main.cf /etc/postfix/master.cf LA UBICACION DE LAS COPIAS DE SEGURIDAD, SON LAS MISMAS QUE DE LOS ARCHIVOS ORIGINALES, TERMINADOS CON LA FECHA Y HORA DEL MOMENTO DE LA MODIFICACION Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
6.	Se procede a definir las variables correspondientes con su organización. Para tal cometido presione “ENTER”. <pre> ----- -- SE DEFINEN LA VARIABLES DE SU ORGANIZACION PARA LA CONFIGURACION -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>

Paso	Descripción						
7.	Deberá buscar los siguientes parámetros en el archivo de configuración y modificar sus valores. Guarde y cierre el documento cuando termine de modificar los valores correspondientes y pulsar “ENTER” para continuar. <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <tr> <td>\$mydomain</td><td>'DominioOrganización.es'</td></tr> <tr> <td>\$myhostname</td><td>'Nombre.equipo'</td></tr> </tbody> </table>  Nota: Deberá adaptar las configuraciones a los parámetros de su organización.	Parámetro	Valor	\$mydomain	'DominioOrganización.es'	\$myhostname	'Nombre.equipo'
Parámetro	Valor						
\$mydomain	'DominioOrganización.es'						
\$myhostname	'Nombre.equipo'						
8.	El proceso continúa verificando el correcto funcionamiento del servicio de “Amavis”. Para salir de la pantalla de comprobación del servicio de “amavisd” pulse la tecla “q”.  Nota: En caso de que falle el proceso de verificación, deberá restablecer los ficheros de configuración con los ficheros de respaldo y volver a realizar el punto de este anexo.						
9.	Una vez aplicada las configuraciones en la solución “Amavis”, se procede a su integración con “Postfix”, para continuar con el proceso de integración pulse la tecla “ENTER”. 						

Paso	Descripción						
10.	Deberá buscar los siguientes parámetros en el archivo de configuración y modificar sus valores. Guarde y cierre el documento cuando termine de modificar los valores correspondientes y pulsar “ENTER” para continuar. <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <tr> <td>content_filter</td><td>smtp-amavis:[127.0.0.1]:10024</td></tr> <tr> <td>smtpd_proxy_options</td><td>speed_adjust</td></tr> </tbody> </table>  Nota: Deberá adaptar las configuraciones a los parámetros de su organización.	Parámetro	Valor	content_filter	smtp-amavis:[127.0.0.1]:10024	smtpd_proxy_options	speed_adjust
Parámetro	Valor						
content_filter	smtp-amavis:[127.0.0.1]:10024						
smtpd_proxy_options	speed_adjust						
11.	Este proceso terminará comprobando la sintaxis y el funcionamiento de “postfix”. Pulsando “ENTER”, continuará la ejecución del script.						
12.	Se continua con la configuración de los usuarios y grupos necesarios. Pulsando “ENTER” se continua con la ejecución del script. <pre>configuracion de postfix Correcta Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>						
13.	Se procede a integrar “ClamAV” en “Amavis”. Pulse “ENTER” para continuar. <pre>----- -- SE CONFIGURA AMAVIS -- -- PARA LA INTEGRACION DE CLAMAV -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>						
14.	Asegúrese que el siguiente parámetro se encuentra comentado por el símbolo “#”. Guarde el documento y ciérrelo, pulsando “ENTER” para continuar. <table border="1"> <thead> <tr> <th>Parámetro</th><th>Valor</th></tr> </thead> <tbody> <tr> <td># @bypass_virus_checks_maps</td><td>(1);</td></tr> </tbody> </table> 	Parámetro	Valor	# @bypass_virus_checks_maps	(1);		
Parámetro	Valor						
# @bypass_virus_checks_maps	(1);						

Paso	Descripción
15.	El proceso concluirá con la comprobación de los permisos de los ficheros de configuración, para su correcto acceso. <pre> ----- COMPROBANDO CONFIGURACION ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... CONFIGURACION POSTFIX CORRECTA -rw-r--r--. 1 root root 1.1K 2021-01-21 11:21 /etc/freshclam.conf freshclam.conf Permisos de acceso CORRECTOS Correcto -rw-r--r--. 1 root root 1.1K 2021-01-21 11:21 /usr/lib/systemd/system/clamd@.service clamd@.service SI pertenece a root Correcto -rw-r--r--. 1 root root 1.1K 2021-01-21 11:21 /usr/lib/systemd/system/clamd@.service clamd@.service Permisos de acceso CORRECTOS Correcto ----- CONFIGURACION TERMINADA ----- </pre>

4. FIREWALLD

Paso	Descripción
1.	Se va a proceder a revisar el estado de Firewalld, así como su configuración.
2.	Inicie sesión en el equipo Red Hat 8 Linux que está asegurando, con la cuenta del grupo “wheel” creada en la instalación. 
3.	Diríjase al directorio “/Scripts”. <pre>\$ cd /Scripts</pre>

Paso	Descripción
4.	Revise el correcto estado de funcionamiento de “Firewall”, ejecutando los siguientes comandos. <pre>\$ sudo systemctl status firewalld.service</pre> <pre>\$ sudo firewall-cmd --state</pre> <pre>● firewalld.service - firewalld - dynamic firewall daemon Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled) Active: active (running) since Fri 2022-09-02 10:11:11 -04; 3 weeks 5 days ago Docs: man:firewalld(1) Main PID: 963 (firewalld) Tasks: 2 (limit: 23092) Memory: 33.3M CGroup: /system.slice/firewalld.service └─963 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid RHEL8-SI01 systemd[1]: Starting firewalld - dynamic firewall daemon... RHEL8-SI01 systemd[1]: Started firewalld - dynamic firewall daemon.</pre>
5.	Firewalld posee varias zonas diferenciadas de funcionamiento. Para poder comprobar en que zona se encuentra ejecute el siguiente comando. <pre>\$ firewall-cmd --get-default-zone</pre> <pre>[usuario@RHEL8-SI01 Scripts]\$ firewall-cmd --get-default-zone public [usuario@RHEL8-SI01 Scripts]\$</pre>
6.	Para conocer que reglas están asociadas a dicha zona podemos usar el siguiente comando. <pre>\$ sudo firewall-cmd --list-all</pre> <pre>[usuario@RHEL8-SI01 Scripts]\$ sudo firewall-cmd --list-all public (active) target: default icmp-block-inversion: no interfaces: enp0s3 sources: services: cockpit dhcpv6-client ssh ports: protocols: masquerade: no forward-ports: source-ports: icmp-blocks: rich rules:</pre>
7.	Para asignar una zona específica a una interfaz de red del equipo, deberá ejecutar el siguiente comando. <pre>\$ sudo firewall-cmd --zone=public --change-interface=enp0s3</pre> <pre>[usuario@RHEL8-SI01 Scripts]\$ sudo firewall-cmd --zone=public --change-interface=enp0s3 success</pre>

Paso	Descripción
8.	A continuación, se procede a realizar a modo de ejemplo la inserción del puerto 25 a la excepción de firewallld. <pre>\$ sudo firewall-cmd --zone=public --add-port=25/tcp --permanent \$ sudo firewall-cmd --reload \$ sudo firewall-cmd --list-services</pre> 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.

ANEXO A.5.2. 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 Red Hat 8 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>

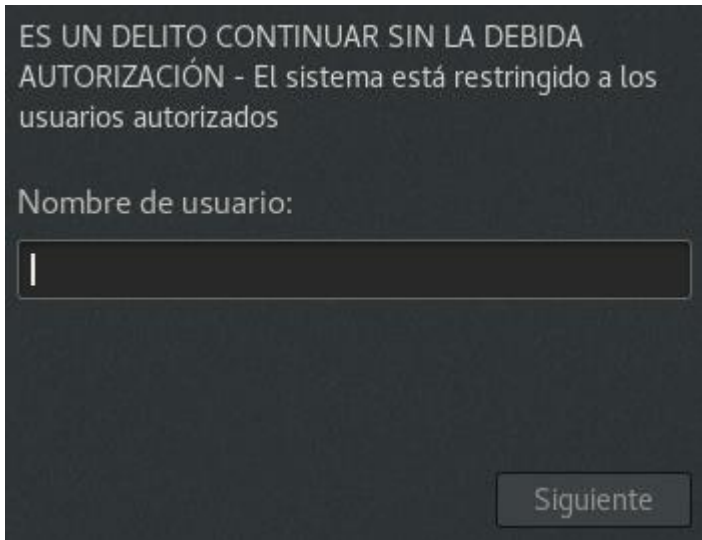
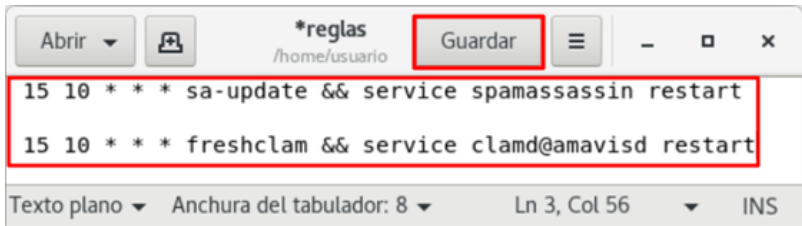
<https://spamasassin.apache.org/downloads.cgi?update=201809160000>

<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 Red Hat 8 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".
2.	Diríjase a la barra de tareas superior, pulse sobre "Actividades", escriba y seleccione "Terminal".
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 Red Hat 8Linux. Para ello, ejecute el siguiente comando. <pre>\$ sudo gnome-text-editor reglas &>/dev/null</pre>
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. 

Paso	Descripción
5.	Deberá de redireccionar, como super usuario, el archivo creado al comando encargado de la realización de las tareas programadas “cron”. <pre>\$ sudo crontab < reglas</pre>
6.	Deberá borrar el archivo “reglas” y comprobar la creación de la tarea programada en cron. Para ello ejecute los siguientes comandos. <pre>\$ sudo rm /reglas \$ sudo crontab -l</pre> <pre>[usuario@RHEL8-SI01 Scripts]\$ sudo crontab -l 15 10 * * * sa-update && service spamassassin restart 15 10 * * * freshclam && service clamd@amavisd restart [usuario@RHEL8-SI01 Scripts]\$</pre>

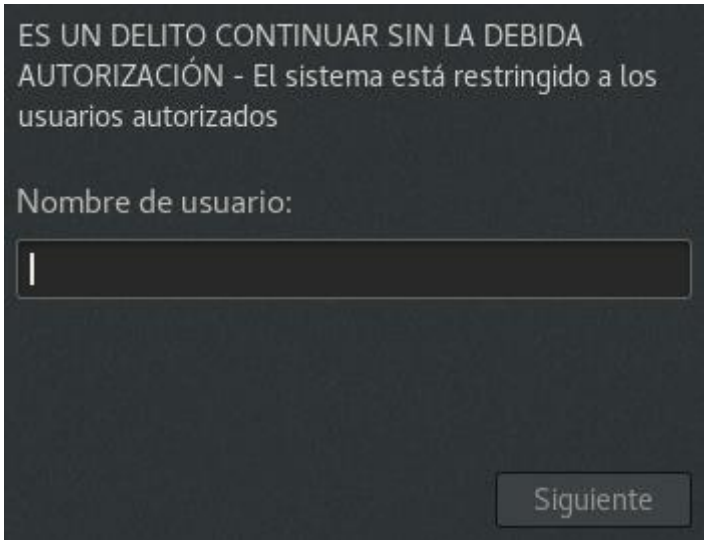
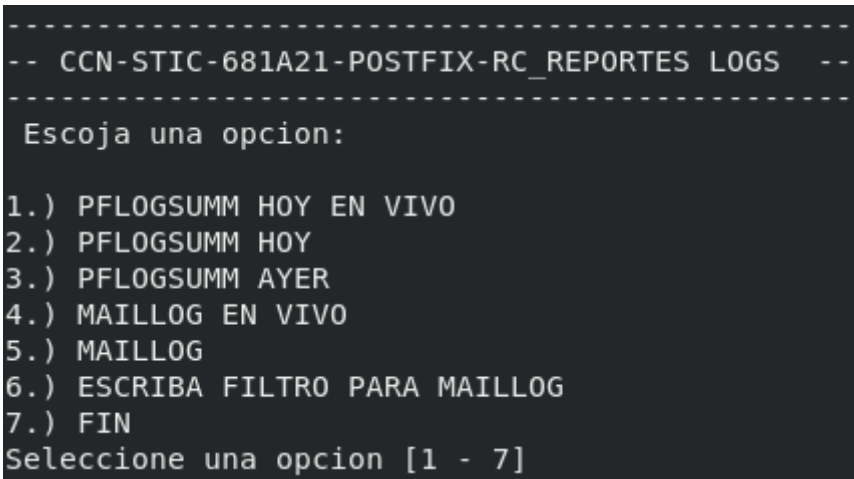
2. PFLOGSUMM

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 Red Hat 8Linux 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 "Actividades", escriba y seleccione "Terminal". Ejecute el comando "<code>cd /</code>" 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. <pre>\$ sudo sh CCN-STIC-681A21_Adicional_Log.sh</pre>
4.	Se desplegará un menu que le facilitara la tarea de visualizado de logs. 
5.	Para finalizar cualquier proceso pulse "CTRL+C".

