centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-619B

IMPLEMENTACIÓN DE SEGURIDAD SOBRE CENTOS 8 (CLIENTE INDEPENDIENTE)

SEPTIEMBRE 2020

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

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

NIPO: 083-20-180-6

Fecha de Edición: septiembre de 2020
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

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 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 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE CENTOS EN EL ENS

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un puesto de trabajo con el sistema operativo CentOS 8 x86_64 DVD1 (build 1911) según criterios del ENS.

Debido a las características de los puestos de trabajo a los que van dirigidas las guías de la serie 600 se toma la determinación de establecer la versión CentOS 8 x86_64 (build 1911) de la distribución, con la opción de instalación "servidor con GUI" como la más adecuada para su implementación. Esto se basa en los siguientes condicionantes:

a) Estos equipos pueden estar conectados a Internet por lo cual determinadas funcionalidades como el instalador de aplicaciones o el entorno de escritorio GNOME, pueden ser utilizados o no, en función de las necesidades de cada organización.

b) El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.

c) La opción de "Servidor con GUI" de CentOS 8.1 permite garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con CentOS 8 Linux. No obstante, deben considerarse siempre las actualizaciones de seguridad como un elemento esencial para garantizar la seguridad de los puestos de trabajo en cualquier infraestructura.

Además de esta determinación existen varias configuraciones adicionales en el "ANEXO A.6 TAREAS ADICIONALES DE SEGURIDAD" para garantizar la securización del sistema. Dichas características son:

a) Protección de servicios de red Firewalld. Este componente se establece de manera predeterminada en CentOS 8. Este apartado se ha realizado para la configuración de una zona segura.

b) Protección de disco cifrado. El cifrado completo de una partición con cifrado LUKS, elimina todos los datos de dicha partición, por esta razón se recomienda cifrar las particiones desde la instalación. Este apartado se ha realizado para los sistemas CentOS 8 ya implementados que deseen crear una unidad o partición adicional cifrada.

c) Configuración adicional de seguridad, Selinux. SELinux (Linux con seguridad mejorada: «Security Enhanced Linux») es un sistema de control obligatorio de acceso («Mandatory Access Control») basado en la interfaz LSM (módulos de seguridad de Linux: «Linux Security Modules»). En la práctica, el núcleo pregunta a SELinux antes de cada llamada al sistema para saber si un proceso está autorizado a realizar dicha operación. SELinux utiliza una serie de reglas, conocidas en conjunto como una política («policy»), para autorizar o denegar operaciones. Puesto que estas reglas son difíciles de crear, en este apartado se recoge una configuración mínima de las mismas para mayor seguridad del sistema.

d) Configuración del interfaz de usuario y del interfaz de monitorización y gestión cockpit que viene de forma predeterminada en las versiones 8 del sistema operativo CentOS Linux.

No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas, puedan ser modificadas para adaptarlas a sus necesidades operativas.

La aplicación de esta guía se debe realizar en un sistema operativo CentOS 8.1 Linux que se acaba de instalar en un equipo que se encontraba formateado (sin datos).

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE CENTOS 8 PARA ENS

1. APLICACIÓN DE MEDIDAS EN CENTOS 8 LINUX

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de clientes con CentOS 8 Linux y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de configuraciones de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande.

La aplicación de medidas de seguridad atenderá a las siguientes condiciones de implantación de infraestructuras:

a) Aplicación de seguridad en clientes independientes, donde se realizará la ejecución de aplicaciones o el tratamiento de información sujetos al RD 3/2010 y se encontraran implementados con CentOS 8 Linux.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta CentOS 8 Linux, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de políticas de seguridad en instalación o las innatas a la gestión del sistema.

Esta guía por lo tanto no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean nativas al sistema operativo. Es factible en ello que se realicen referencias a soluciones de seguridad que como en el caso de CentOS 8 Linux vienen implementadas por el propio Sistema Operativo a través del software SELinux. No obstante, tal y como es lógico referenciar dicha implementación, y atendiendo a los requerimientos del ENS, requiere una administración centralizada que no aporta esta solución, cubriendo además solo uno de los aspectos requeridos por la medida de protección frente a código dañino.

Para un mejor entendimiento de las medidas, éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a los niveles que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de los diferentes niveles de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso abarca todo el conjunto de acciones que bien preparatorias o ejecutivas orientadas a determinar qué o quién puede o no, acceder a un recurso del sistema, mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará 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 comodidad de uso y la protección del sistema. De tal forma que la seguridad se irá incrementando en base al nivel exigido. Así en el nivel básico se prima la comodidad y en los niveles altos se prima la protección.

1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN

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

La identificación de usuario se traduce en la necesidad de crear cuentas únicas e inequívocas para cada usuario y servicio, a través de cuentas locales en los puestos de trabajo. Dichas cuentas deberán ser gestionadas de tal forma que deberán ser inhabilitadas cuando se dieran una serie de condicionantes:

a) El usuario deja la organización.

b) Cesa en la función para la cual se requería dicha cuenta.

c) La persona que lo autorizó emite una orden en contra.

Debe tenerse en consideración que nunca deberán existir dos cuentas iguales de forma que estas no puedan confundirse o bien imputarse acciones a usuarios diferentes.

1.1.1.2. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde la categoría básica y atenderán a la necesidad que los recursos del sistema queden protegidos con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de los derechos de acceso suficientes.

Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad para la organización, a través de la persona responsable de dicha determinación y haciendo uso de las tecnologías necesarias.

Desde el punto de vista tecnológico, esta medida abarca un gran número de actividades, de tal forma que los puntos de control para restringir o conceder un acceso son abundantes. Acceder a un fichero o una carpeta o imprimir en un recurso, son acciones que pueden ser controladas y determinar para ello los permisos asignados.

La plantilla de seguridad recoge una serie de permisos que serán asignados con objeto de limitar las acciones por parte de usuarios y administradores. De esta forma y controlando los requisitos de acceso, se reducirán todos aquellos riesgos del uso habitual de administración de un puesto de trabajo.

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Linux para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia.

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

Aplicable a partir de la categoría media, se considera un requerimiento importante para una organización la segregación de funciones en base a la actividad. De esta forma se establece cadenas de autorización y control enfocadas a evitar la existencia de una única persona autorizada y que ésta pueda abusar de sus derechos para cometer alguna acción ilícita.

Desde el punto de vista formal la segregación de funciones deberá realizarse al menos para las siguientes tareas:

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de otra función.

Dichos procesos de segregación son factibles realizarlos a través de los propios mecanismos que proporciona CentOS 8 Linux, así como las funcionalidades implicadas en la presente guía.

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura de documentación sobre la herramienta Audit incluida en CentOS 8 Linux. Aunque será mencionada a lo largo de la presente guía en relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en CentOS 8 Linux a través de la herramienta Audit.

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

Altamente vinculado al punto 1.1.1.2 OP. ACC. 2. REQUISITOS DE ACCESO, estas medidas requieren consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para poder cumplir las 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.

Como ya se comentó previamente, CentOS 8 Linux se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Adicionalmente y siguiendo uno de los principios fundamentales de mínimo privilegio posible, a través de la aplicación de la presente guía se configurarán diferentes permisos a las cuentas de usuario, limitando la utilización de la cuenta “root” para tareas específicas que necesiten un nivel de privilegios elevado, ésta configuración debe entenderse como un mecanismo para impedir que el trabajo directo con usuarios con privilegios de administrador, repercuta negativamente en la seguridad, a acometer todas las acciones con el máximo privilegio cuando este no es siempre requerido.

Así en la navegación a Internet, acceso a recurso o tratamientos ofimáticos por citar algunos ejemplos frecuentes, un usuario no requiere del privilegio de administración para desempeñarlo. Así y sin darse cuenta podría estar poniendo en grave riesgo la seguridad del sistema al tratar ficheros, ejecutables, componentes y otros, que descargados de Internet u otras fuentes de dudosa confianza con máximos privilegios.

En ambientes donde varios usuarios usan uno o más sistemas GNU/Linux, es necesario otorgar distintos permisos o privilegios para que estos puedan hacer uso de comandos propios del usuario administrador "root". Para que los usuarios puedan hacer uso de los programas propios de sus funciones pero que son propiedad de "root" sin "entregar" la contraseña la mejor alternativa es hacer uso de sudo.

Sudo permite implementar un control de acceso altamente configurable para que usuarios ejecutan que comandos. Si un usuario normal desea ejecutar un comando de root (o de cualquier otro usuario), sudo verifica en su lista de permisos y si está permitido la ejecución de ese comando para ese usuario, entonces sudo se encarga de ejecutarlo. Es decir, sudo es un programa que basado en una lista de control (/etc/sudoers) permite (o no) la ejecución al usuario que lo invocó sobre un determinado programa propiedad de otro usuario, generalmente del administrador del sistema "root".

Puesto que las condiciones de funcionalidad del comando sudo, pueden establecerse desde la usabilidad hasta la máxima seguridad y atendiendo a los criterios marcados por el propio Esquema Nacional de Seguridad, las diferentes plantillas de seguridad que se generan para los diferentes niveles atenderán a estos criterios de criticidad. No obstante, y aunque se detallará más adelante, el operador puede conocer la funcionalidad del comando SUDO a través de la información facilitada por el propio fabricante:

https://wiki.centos.org/es/TipsAndTricks/BecomingRoot

De esta forma el principio de mínima exposición y menor privilegio se puede materializar de forma extensiva a los propios administradores de los servidores y servicios que gestiona la organización.

1.1.1.5. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Dentro de los procesos habituales en el manejo de los sistemas de la información, el correspondiente a la autenticación, corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema "quién eres".

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una 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 o el servicio atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes generalidades estos serán:

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 passwords 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 para ello el uso de dispositivos físicos o de biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-807 de criptología de empleo en el ENS.

Conforme a las necesidades establecidas por el Esquema Nacional de Seguridad se deberá tener también en consideración lo establecido en la guía CCN-STIC-804 para los mecanismos de autenticación y que se encuentra recogido en el punto 4.2.5.

La presente guía tiene en consideración los siguientes aspectos, para el desarrollo de plantillas de seguridad por niveles, enfocados en los procesos de autenticación:

a) Gestión y definición de política de contraseñas.

b) Gestión y definición de política para los bloqueos de cuenta.

c) Implementación de algoritmos para el almacenamiento de contraseñas cifradas.

d) Implementación de mecanismos para el bloqueo de cuentas de usuario y de servicio.

e) Permisividad para el empleo de mecanismos de algoritmos y criptografía basados en biometría, certificados o tarjetas inteligentes.

Debe tenerse en consideración que la distribución CentOS Linux está basada en Red-Hat Enterprise Linux, por este motivo y de manera análoga CentOS ha ido implementando todas las funcionalidades y mecanismos de autenticación de Red-Hat Enterprise Linux, el cual tiene como premisa la máxima securización en entornos de servidores en producción.

CentOS Linux gracias a esta premisa, tiene la capacidad de implementar sistemas de autenticación que se adapten a cualquiera de las necesidades que puedan existir tanto ahora como en el futuro. Pudiendo emplear actualmente mecanismos de autenticación basados en el empleo de contraseñas con funcionalidades como Vault que permite almacenamiento central segura de la información privada del usuario, así como mecanismos basados en Kerberos.

1.1.1.6. OP. ACC. 6. ACCESO LOCAL

Se considera acceso local aquel que se ha realizado desde los puestos dentro de las propias instalaciones que tiene la organización.

El Esquema Nacional de Seguridad, tiene en cuenta la aplicación de medidas diferentes atendiendo a la criticidad de servicios y sistemas.

Así en función del nivel de seguridad deberán aplicarse medidas para:

a) En la categoría básica, se prevendrán ataques para evitar intentos de ataques reiterados contra los sistemas de autenticación. Adicionalmente la información proporcionada en caso de fallo en el acceso deberá ser mínima, siendo este hecho especialmente crítico en las aplicaciones web. También deberán registrarse los intentos satisfactorios y erróneos, así como la de informar a los usuarios de las obligaciones.

b) En la categoría media será exigencia el proporcionar al usuario el detalle de la última vez que se ha autenticado.

c) En la categoría alta deberán existir limitaciones para la fecha y hora en la que se accede. También se facilitará mediante identificación singular la renovación de la autenticación, no bastando el hecho de hacerlo en la sesión iniciada.

CentOS 8 Linux por medio de ficheros de configuración y módulos PAM, permite establecer mecanismos para garantizar bloqueos de cuenta, proporcionar información al usuario, así como establecer medidas para garantizar un cambio seguro de las credenciales. Estás serán aplicadas de forma progresiva en función del nivel de seguridad exigido.

1.1.1.7. OP. ACC. 7. ACCESO REMOTO

Las organizaciones deberán mantener las consideraciones de seguridad en cuanto al acceso remoto cuando éste se realice desde fuera de las propias instalaciones de la organización a través de redes de terceros.

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

CentOS 8 Linux faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación. Sin embargo, no todos los protocolos empleados por defecto después de una instalación común se pueden considerar seguros. La presente guía tiene en consideración estos detalles y por lo tanto habilitará o deshabilitará en su defecto aquellos protocolos que son considerados seguros o no, incluido en ello los correspondientes a autenticaciones empleadas en redes locales o remotas.

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 ellas una serie de procesos tanto para el control, como para la gestión 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

Los equipos antes de su entrada en producción deberán configurarse de tal forma que:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplicará la regla de mínima funcionalidad.

CentOS 8 Linux es un sistema libre con licencia copyleft GNU GPL por lo que se considera indispensable la comprobación de funcionalidades evitando en la medida de lo posible las provenientes de fuentes no confiables, manteniendo las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello se eliminarán o desactivarán mediante el control de la configuración, aquellas funciones que no sean de interés no sean necesarias e incluso aquellas que sean inadecuadas para el fin que se persigue.

Para el cumplimiento de este sentido las diferentes plantillas de seguridad 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 protegerán los más importantes de tal forma que quedarán configurados a través de las políticas que correspondieran por niveles. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

Adicionalmente la guía mostrará mecanismos de administración adicionales para configurar nuevos componentes con objeto de reducir la superficie de exposición, así como limitar la información remitida hacia Internet.

1.1.2.2. OP. EXP. 4. MANTENIMIENTO

Para mantener el equipamiento físico y lógico se deberán atender a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas. Se realizará un seguimiento continuo para garantizar la seguridad de los sistemas. Para ello deberá existir un procedimiento que permita analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

En este sentido la presente guía sigue los patrones establecidos tanto por CentOS, como por Red-Hat por ser el fabricante de la distribución en la que se basa CentOS. Debe tenerse en consideración que este Sistema Operativo es un elemento en constante evolución, donde ante la aparición de un riesgo de seguridad deberá dotar de los mecanismos necesarios para paliar el problema. Para ello Red-Hat y máximo 72 horas después CentOS, hace una constante difusión de actualizaciones de seguridad que deberá evaluar e implementar sobre los servidores, con objetos de mantener las garantías de seguridad necesarias.

Adicionalmente a las actualizaciones de seguridad, se debe tomar en consideración que CentOS ofrece ciclos de actualizaciones de 10 años. No debe confundir no obstante dichas actualizaciones de funcionalidad con las actualizaciones tradicionales de seguridad, sin embargo, CentOS Linux seguirá recibiendo las actualizaciones de seguridad dentro del ciclo natural de publicación de las mismas.

Para ello deberá diferenciar los siguientes tipos de actualizaciones:

a) Actualizaciones de seguridad. Las actualizaciones de seguridad vienen a subsanar problemas más frecuentes del Sistema Operativo, en relación a los componentes más críticos del sistema.

b) Actualizaciones de seguridad:

   i. Los proveedores de sistemas operativos Linux proporcionan actualizaciones periódicas, que en su mayoría son parches de seguridad del sistema operativo. Debe asegurarse de que los sistemas operativos actualizados con los parches de seguridad más recientes.

   ii. Mediante el plugin yum-security es posible listar y restringir las actualizaciones únicamente a las que sean por criterios de seguridad. Los paquetes los clasifica según:

      – Enhancement. Una mejora que entra dentro de criterios de seguridad por algún motivo, por ejemplo, una mejora en el paquete chkrootkit.

      – Bugfix. Solución de un bug, igualmente que cumple criterios de seguridad de forma secundaria.

      – Security. Solución a un problema de seguridad propiamente dicho.

c) Actualizaciones de los repositorios:

   i. Un repositorio es un directorio o sitio web que contiene paquetes de software y archivos de índices. Las utilidades de administración de software como yum automáticamente ubican y obtienen los paquetes RPM correctos desde esos repositorios. Este método soluciona tener que buscar e instalar las nuevas aplicaciones o actualizaciones de forma manual. Se puede utilizar un único comando para actualizar todo el software del sistema o buscar por nuevo software según un criterio dado. Las utilidades de administración de paquetes en CentOS 8 están preconfiguradas para utilizar tres de estos repositorios:

      – Base. Los paquetes que conforman un lanzamiento de CentOS, tal y como están en el disco.

      – Actualizaciones. Versiones actualizadas de los paquetes proporcionados en Base.

      – Extras. Paquetes para una variada gama de software adicional.

Las actualizaciones de CentOS, por lo general, mantienen una compatibilidad binaria con versiones anteriores.

Recuerde por lo tanto que deberá atender no solo a las especificaciones del fabricante en cuanto a las actualizaciones de seguridad, sino también a las actualizaciones que incluyen las mejoras de funcionalidad.

Nota: No es un objetivo de esta guía especificar los mecanismos o procedimientos necesarios para mantener los sistemas actualizados. Las plantillas de seguridad configuran las directivas adecuadas para que los sistemas operativos puedan ser actualizados empleando para ello el servicio de actualizaciones de CentOS 8 Linux.

1.1.2.3. OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La organización para puestos de trabajo deberá implementar una solución antimalware que proteja contra código dañino. Se considerarán como tal los virus, gusanos, troyanos, programas espías y en general cualquier tipo de aplicación considerada como malware.

Debe tomarse en consideración que, aunque CentOS 8.1 Linux venga provisto de SELinux, éste no está creado para proteger el sistema frente a código dañino. Se deberá incluir una solución antivirus y antimalware que pueda cubrir esta necesidad. No obstante, estas herramientas no están pensadas para analizar todo el espectro de protección frente a código dañino. Por ejemplo, sin una solución de administración centralizada no tendrá la visibilidad que realice la gestión centralizada de la seguridad y gestión de incidencias demandadas por el Esquema Nacional de Seguridad.

Adicionalmente este producto en sí mismo no ofrece un mecanismo de protección con administración centralizada, objetivo fundamental de toda organización no solo para centralizar los procesos de despliegue y configuración de políticas de protección, sino de la centralización de los estados y reportes de detección y eliminación de malware.

Las organizaciones deberán por lo tanto proveer de otra solución frente a código dañino que ofrezca un alcance completo en la detección y eliminación de malware, así como atender a las recomendaciones del fabricante para su mantenimiento.

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

Aplicable en las categorías básica, media y alta de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

a) Quién realiza la actividad, cuándo la realiza y sobre qué.

b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.

d) La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.

e) La categoría alta requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

CentOS 8.1 Linux, implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que de forma predeterminada los datos son almacenados localmente como la utilidad Audit o la inspección de sesiones.

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

En las categorías media y alta 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 la fecha y hora.

c) Permitir el mantenimiento de los registros sin que estos puedan ser alterados o eliminados por personal no autorizado.

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

1.2. MEDIDAS DE PROTECCIÓN

Este conjunto de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que se incluye una gran variedad de las mismas que son aplicables desde las más puramente procedimentales, a las puramente físicas o a las de aplicación técnica.

Solo estas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado son de aplicación sobre las funcionalidades del propio sistema operativo servidor. La mayor parte de ellas son de aplicación en la red o cuando un sistema tipo portátil sale de la organización, cuestión que no se considera de aplicación a un servidor que se considera ubicado en un entorno estable dentro del centro de procesamiento de datos (CPD) que tuviera la organización.

Se considera en este sentido que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto evitar el acceso a los equipos de escritorio existentes por parte de personal no autorizado.

1.2.1. PROTECCIÓN DE LOS EQUIPOS

Las medidas de protección de los equipos cubren todos aquellos mecanismos que son necesarios para garantizar tanto una configuración de seguridad válida para el sistema, así como para mantener la propia privacidad del trabajo desarrollado.

Dentro de las medidas se articulan la aplicación de mecanismos de índole tecnológica y otras de tipo física. Entre estas últimas, pueden localizarse las correspondientes a un puesto de trabajo despejado.

Aunque esta guía de seguridad se encuentra orientada a un sistema operativo tipo servidor, se tiene en consideración aquellas medidas que, siendo establecidas para un puesto de trabajo, le son de completa aplicación, por ejemplo, la necesidad de realizar un bloqueo del puesto de trabajo.

1.2.1.1. MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO

Aplicable desde la categoría media se establece la necesidad de realizar un bloqueo de la cuenta toda vez que se haya producido una inactividad en el sistema tras un tiempo prudencial. Dicho tiempo prudencial deberá ser establecido por política de seguridad.

Adicionalmente, a todos aquellos sistemas de categoría alta, deberán cancelarse las sesiones abiertas, cuando se supere un tiempo de actividad superior al anteriormente planteado.

Estos controles serán aplicables a Linux mediante la configuración de módulos PAM (Pluggable Authentication Modules) y ficheros de configuración local del equipo.

1.2.1.2. MP. EQ. 3. PROTECCIÓN DE LOS PORTÁTILES

Los equipos que salgan de las instalaciones donde opere la organización y por lo tanto no puedan beneficiarse de las medidas de protección física que éstas ofrezcan, deberán ser protegidos frente a riegos de pérdida o robo.

Como condición general a partir de la categoría básica, los sistemas portátiles, deberán ser identificados e inventariados. Deberá asimismo de proporcionarse de un mecanismo de comunicación de incidencias frente a pérdidas o sustracciones de los mismos.

En dicho procedimiento deberán consignarse mecanismos para las bajas de cuentas, inclusive aquellas que permitan conexiones remotas desde el equipo perdido o sustraído. Para ello deberá asimismo consignarse un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el equipo se conecte a redes, en particular si el equipo se conecta a redes públicas.

Para aquellos sistemas portátiles que manejen información considerada como categoría alta-DL según las definiciones del nivel ENS, deberán disponerse de mecanismos de cifrado que permitan la confidencialidad de los datos almacenados.

Existen en el mercado numerosas soluciones que permiten el cumplimiento de esta medida recogida para niveles altos de información en el RD 3/2010. CentOS 8 Linux en su versión 1911 permite el uso de la solución de LUKS (Linux Unified Key Setup) como mecanismo para garantizar la confidencialidad de los datos. La presente guía recoge los mecanismos para el cifrado de unidades con LUKS en el ANEXO A.6.2 PROTECCIÓN DEL DISCO. CIFRADO.

1.2.2. PROTECCIÓN DE LAS COMUNICACIONES

Los conjuntos de medidas orientadas a la protección de las comunicaciones tienen como objetivo la protección de la información en tránsito, así como dotar a los mecanismos para la detección y bloqueo de intrusos en una red.

1.2.2.1. 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, deberá prevenirse ataques activos, garantizando que los mismos serán al menos detectados, permitiendo activarse los procedimientos que se hubieran previsto en el tratamiento frente a incidentes.

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

Para aquellos entornos con sistemas o información catalogados como categoría alta-DL, es recomendable el empleo de dispositivos hardware para el establecimiento y utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberá tener en consideración los productos que se encuentran certificados y acreditados.

A través de controles centralizados en plantillas de seguridad, se establecerán mecanismos que controlen el acceso y salida de información a los puestos de trabajo mediante el empleo del firewall en su modalidad avanzada. Aunque se tratará en extensión en un anexo de la presente guía, el operador podrá conocer todos los detalles de esta solución a través de la información que proporciona el fabricante.

Nota: Aunque se proporciona una configuración base de firewalld de CentOS 8 con la presente guía, el administrador deberá aplicar y gestionar los perfiles y reglas del firewall acorde a las necesidades de su organización, prevaleciendo como regla primordial la mínima exposición hacia el exterior del equipo que se configura.

Además, se establecerán configuraciones relativas a la protección de la autenticación, habilitando solo aquellos protocolos que son válidos y seguros.

1.2.3. PROTECCIÓN DE LA INFORMACIÓN

Conjunto de procesos y medidas para un correcto uso y salvaguarda de los datos de carácter personal identificados en el sistema.

1.2.3.1. MP. INFO. 3. CIFRADO

Se debe asegurar la integridad de la información con un nivel alto de confidencialidad cifrada tanto durante su almacenamiento como durante su transmisión

Solo será visible en claro dicha información cuando se esté realizando uso de ella.

La presente guía establece mecanismos a través de LUKS para garantizar el cifrado de los datos existentes en los sistemas.

Las políticas y configuraciones en la presente guía establecen la implementación de los algoritmos más seguros posibles que garanticen la integridad y confidencialidad de los datos transmitidos dentro de la red de área local.

Deberá adicionalmente aplicar mecanismos que garanticen el cifrado de comunicaciones cuando acceda a servicios e información de la organización de forma remota cuando esté fuera de ella.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN CENTOS 8

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 aplicación de políticas de seguridad a nivel local o bien de la configuración de ficheros del sistema.

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 1	Auditoría y supervisión de actividad.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 4	Control de cuentas de usuario.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. ACC. 5	Política de contraseñas.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 5	Protocolos de autenticación local.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 6	Bloqueo de cuentas.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización. Configuraciones adicionales de seguridad descritas a través de la presente guía.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad.	Revisión de ficheros de configuración del sistema descritos en la presente guía.
OP. EXP. 2	Protección de aplicaciones de sistema para garantizar el principio de mínima funcionalidad.	Revisión de ficheros de configuración del sistema descritos en la presente guía.
OP. EXP. 4	Mantenimiento del Sistema Operativo.	Configuraciones adicionales descritas a través de la presente guía. Deberá implementar mecanismos en su organización para garantizar la actualización de los sistemas y aplicaciones.
OP. EXP. 6	Protección frente a código dañino.	La organización deberá emplear una solución adicional a las configuraciones que proporciona CentOS 8 por no cubrir este los mínimos exigidos por el ENS para la protección frente a código dañino.
OP. EXP. 8	Registro de actividad de los usuarios.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad.	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 requisito del registro de actividad es requerido desde la categoría básica.
MP. EQ. 2	Bloqueo de los puestos de trabajo.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
MP. EQ. 3	Protección de portátiles.	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 requisito del registro de actividad es requerido desde la categoría básica.
MP. COM. 3	Protección del sistema mediante implementación de firewall.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización, Se debe tomar en consideración que el cifrado proporcionado por CentOS 8 es el de LUKS, y debe implementarse desde la instalación del Sistema Operativo, si no es así, La organización deberá emplear una solución adicional a las configuraciones que proporciona CentOS 8 por no cubrir éste los mínimos exigidos por el ENS para la confidencialidad de los datos.
MP. SI. 2	Criptografía.	Configuraciones adicionales descritas a través de la presente guía.
MP. INFO. 3	Cifrado.	Implementación de configuración de firewall a nivel local según el punto ANEXO A.6.1 PROTECCIÓN DE SERVICIOS DE RED. CONFIGURACIÓN DEL FIREWALL de la presente guía.

ANEXO A.2. INSTALACIÓN DEL S.O. CONFIGURACIÓN SEGURA DEL GUI

1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DEL GUI CENTOS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes CentOS 8 independientemente de la categorización, 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 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 básica, media o alta, 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, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Los pasos que se describen a continuación se realizarán en todos aquellos clientes CentOS 8 Linux, independientes a un dominio, que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

Este anexo ha sido diseñado para ayudar a los operadores a implementar las distintas configuraciones de seguridad. A continuación, se describe, paso a paso, como realizar la instalación y configuración de seguridad de un cliente CentOS 8.1 Linux independiente de un dominio.

Antes de empezar deberán tenerse en cuenta las siguientes recomendaciones:

a) Todos los discos y particiones deberán formatearse utilizando el sistema de archivos XFS.

b) Por defecto el programa de instalación crea dos particiones /dev/sda1 para el MBR (Master Boot Record) y /dev/sda2 para la utilización del resto del disco. La partición /dev/sda1 se crea con el sistema de archivos XFS y la monta en /boot, mientras que la partición /dev/sda2 con LVM (Logical Volume Manager) y repartida en tres puntos de montaje:

   i. Un punto de montaje donde se almacena la base del sistema operativo (/dev/mapper/cl-root).

   ii. Un punto de montaje SWAP con sistema de archivos SWAP para uso de la memoria de intercambio (/dev/mapper/cl-swap).

   iii. Un punto de montaje con el sistema de archivos XFS para el resto del disco (/dev/mapper/cl-home).

c) En el “ANEXO A.6.2 PROTECCIÓN DEL DISCO. CIFRADO” de la presente guía podrá consultar una guía paso a paso para poder aplicarlo en los equipos CentOS 8 que requieran de su uso.

d) Es importante separar datos, aplicaciones y sistema operativo en distintos dispositivos de almacenamiento, tanto para mejorar el rendimiento como para evitar ataques que se realizan navegando entre directorios. Para la seguridad de un equipo con sólo CentOS 8 Linux no se requiere la existencia de distintas particiones, pero se deberá tener en cuenta durante el proceso de instalación, ya que existen ciertas configuraciones y permisos para los cuales se requiere que existan estas particiones diferenciadas.

e) Si existen datos en el equipo antes del proceso de instalación, deberán eliminarse antes de comenzar el proceso.

f) No deberán realizarse actualizaciones desde versiones previas, ya que de lo contrario no podrá garantizarse que los valores por defecto de los parámetros de seguridad se hayan aplicado.

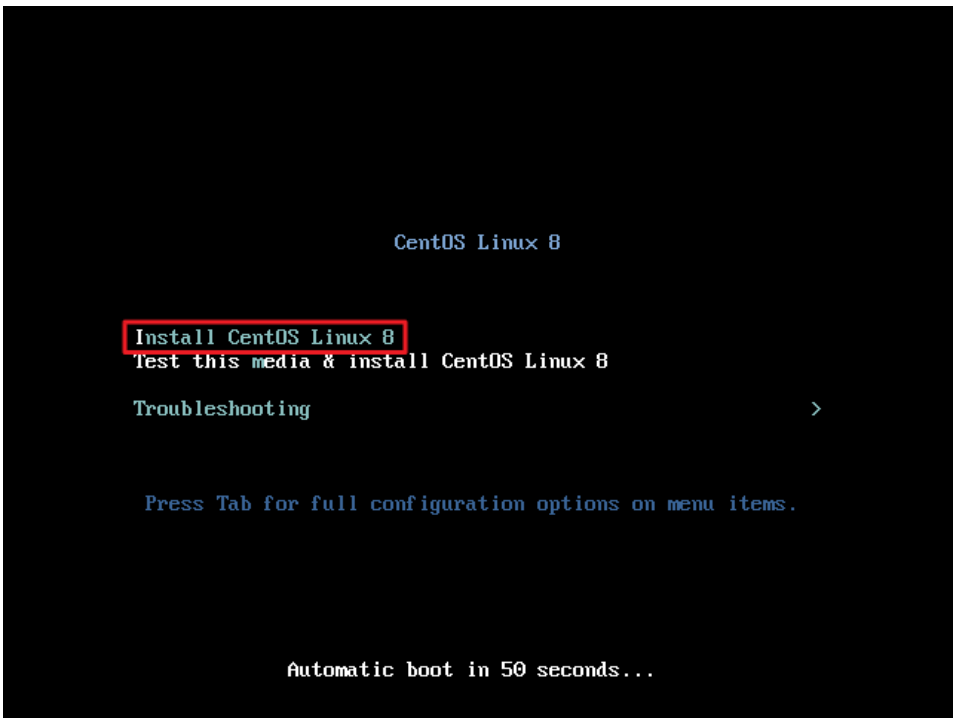
g) No utilizar discos o particiones que utilicen el sistema de archivos FAT.

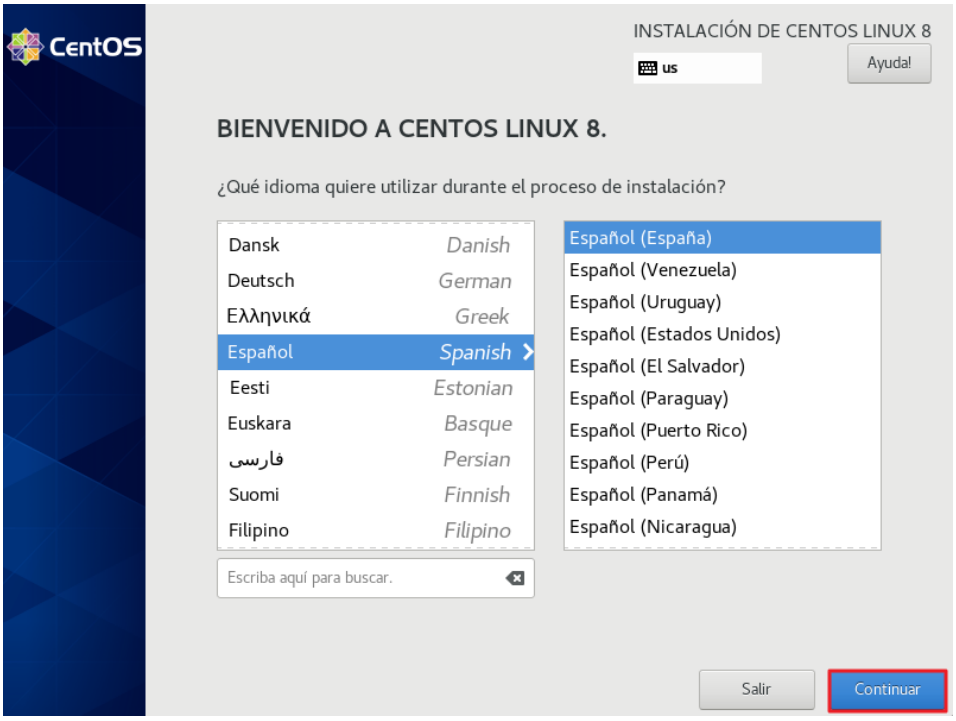
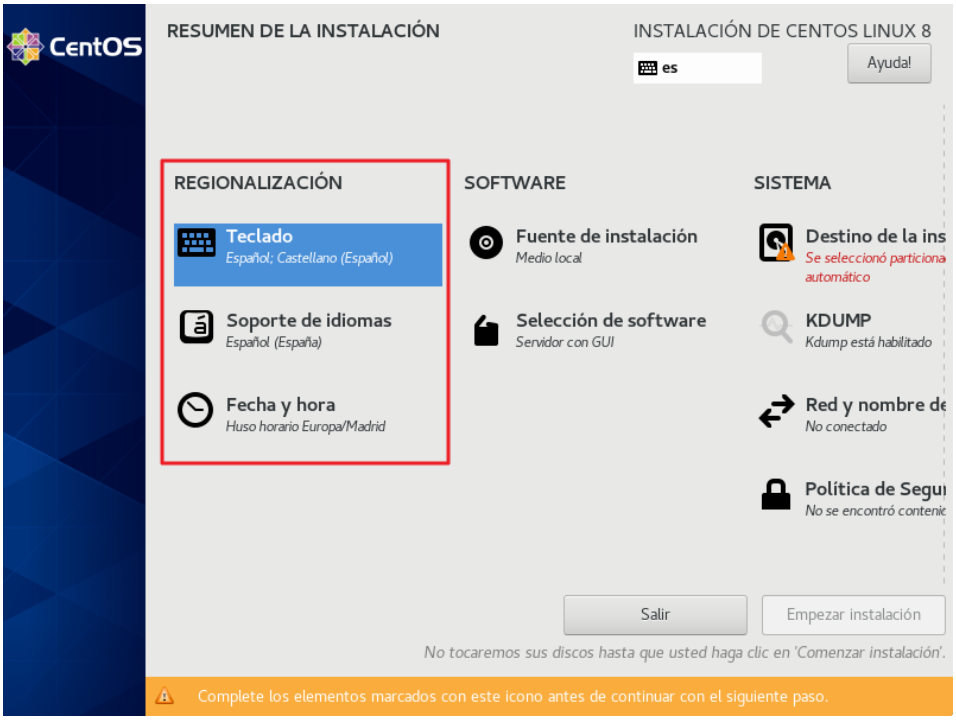
h) No instalar otros sistemas operativos en el equipo.

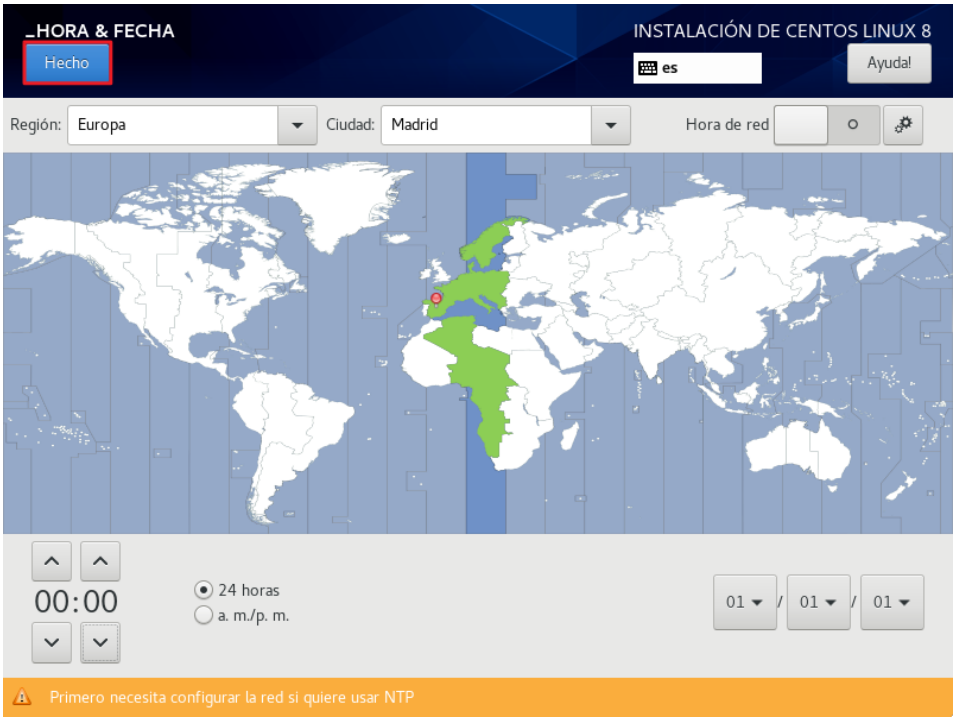
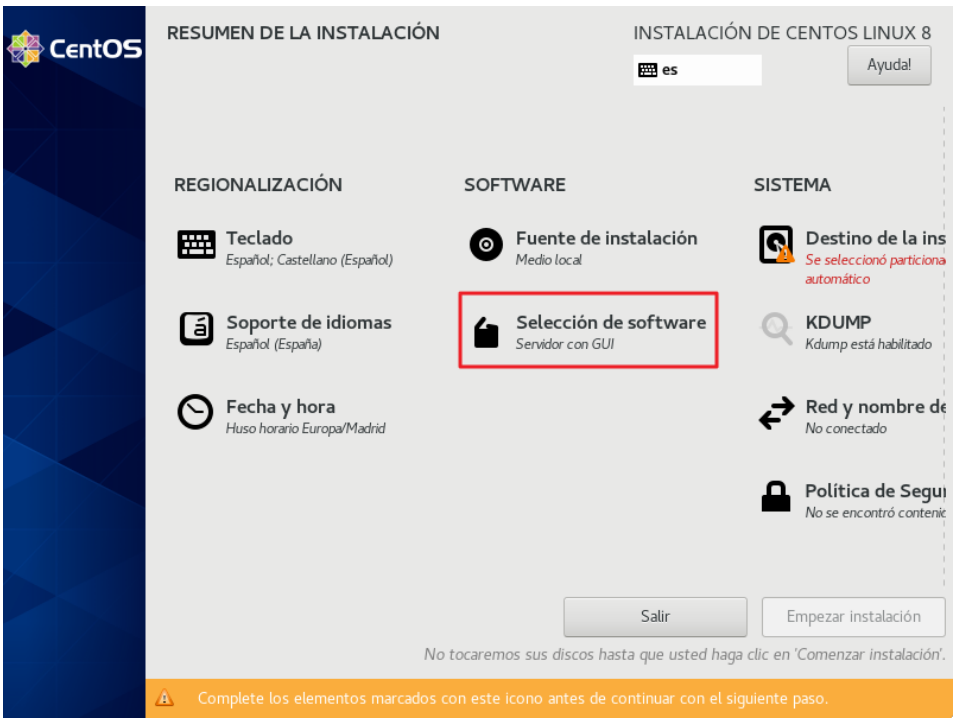
i) Asignar una contraseña compleja a la cuenta de usuario que se crea durante el proceso de instalación.

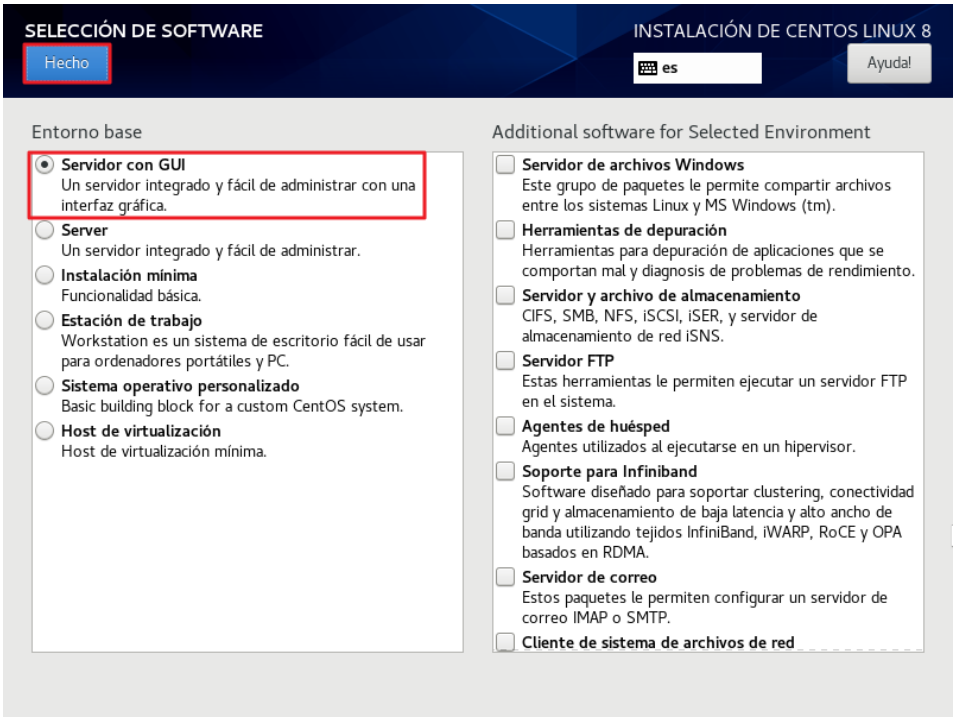
j) Una vez finalizada la instalación básica del sistema, asegurarse de que se instalan todas las actualizaciones de seguridad necesarias. Idealmente estas actualizaciones de seguridad se instalarán antes de conectar el equipo a la red o con el equipo conectado a una red segura.

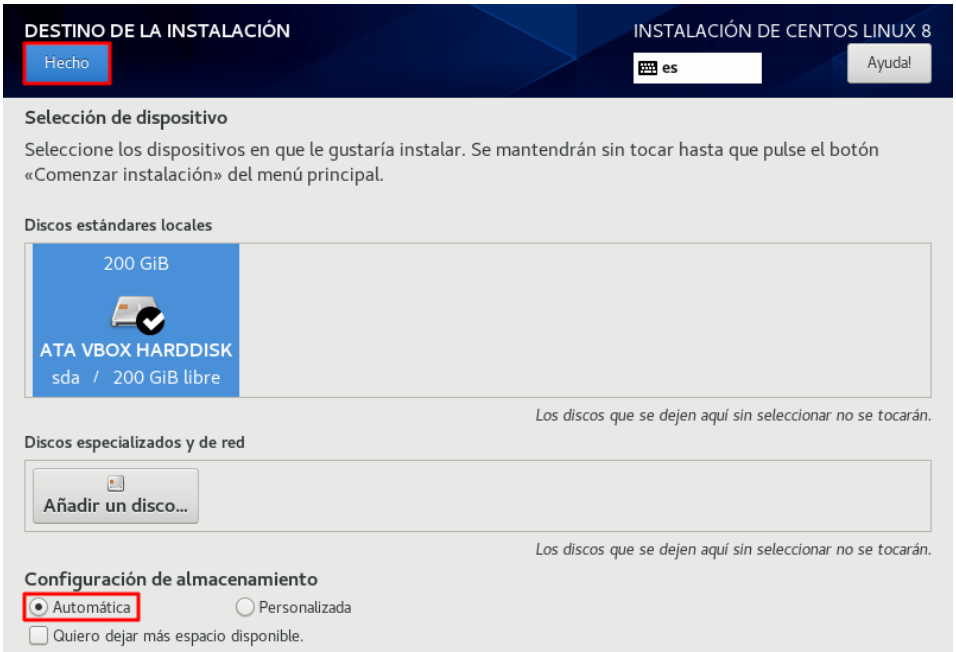
El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación.

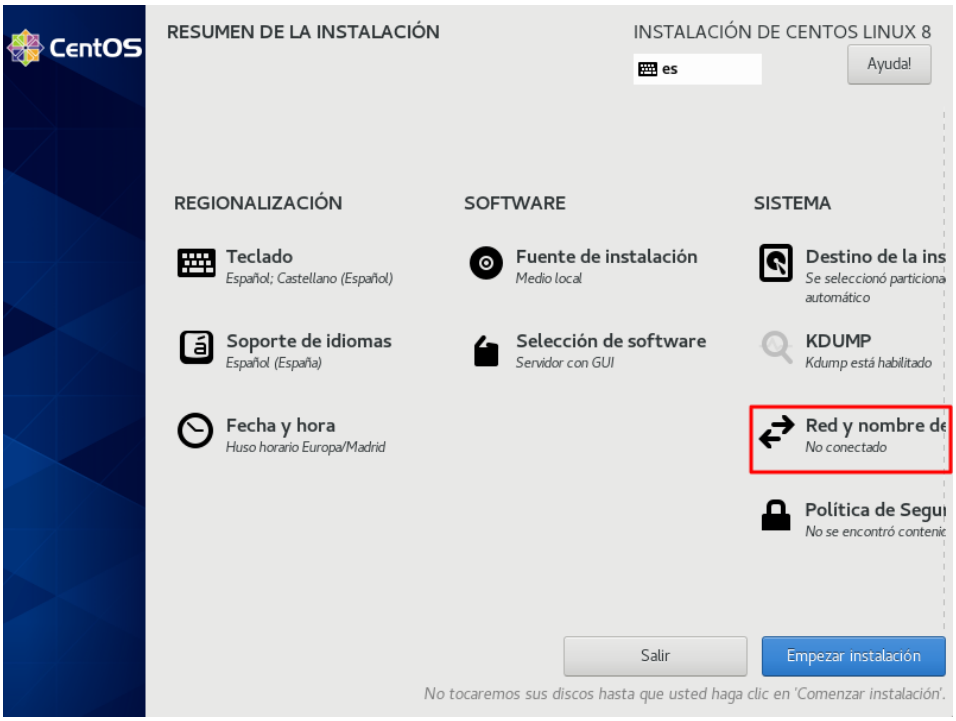
Paso	Descripción
1.	Introduzca el dispositivo USB o DVD de CentOS-8.1.1911-x86_64-dvd1.iso y, si fuera necesario, reinicie la máquina para iniciar la instalación del sistema.
2.	Cuando aparezca el mensaje “Press Tab for full configuration options on menu ítems.”, pulse la tecla correspondiente a la flecha de dirección arriba, seleccione “Install CentOS Linux 8” y pulse “Enter”.  **Nota:** Si el equipo no se inicia desde DVD revise los parámetros de la BIOS. No se debe pulsar ninguna tecla hasta que aparezca el menú de elección de idioma. En caso contrario se podría iniciar la instalación sin modo gráfico de Anaconda. Si esto sucede, reinicie el ordenador y comience desde el paso 1.

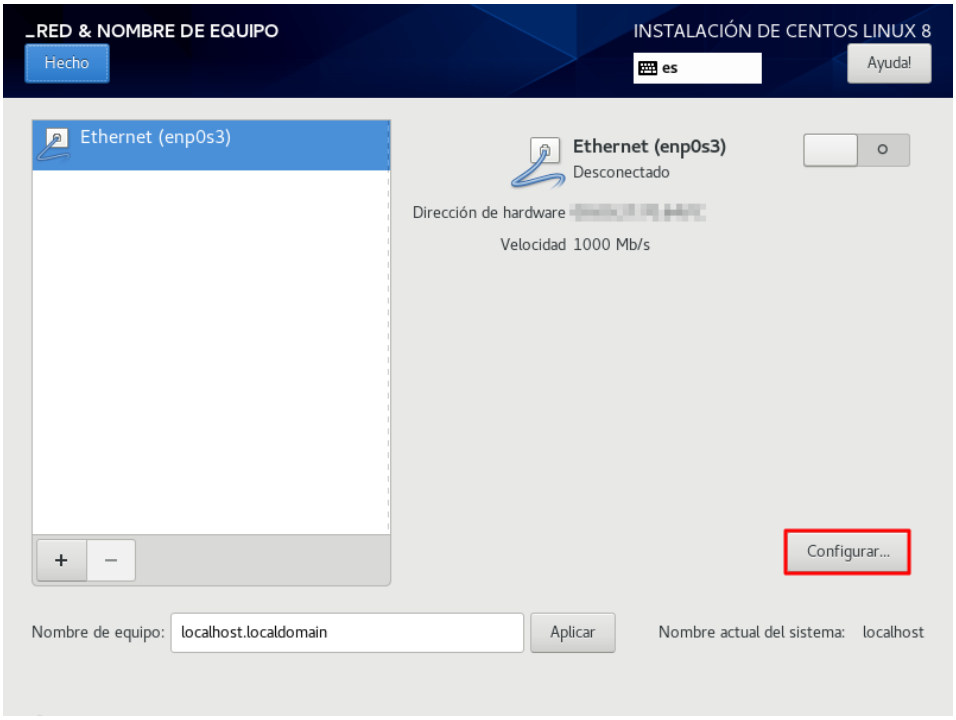
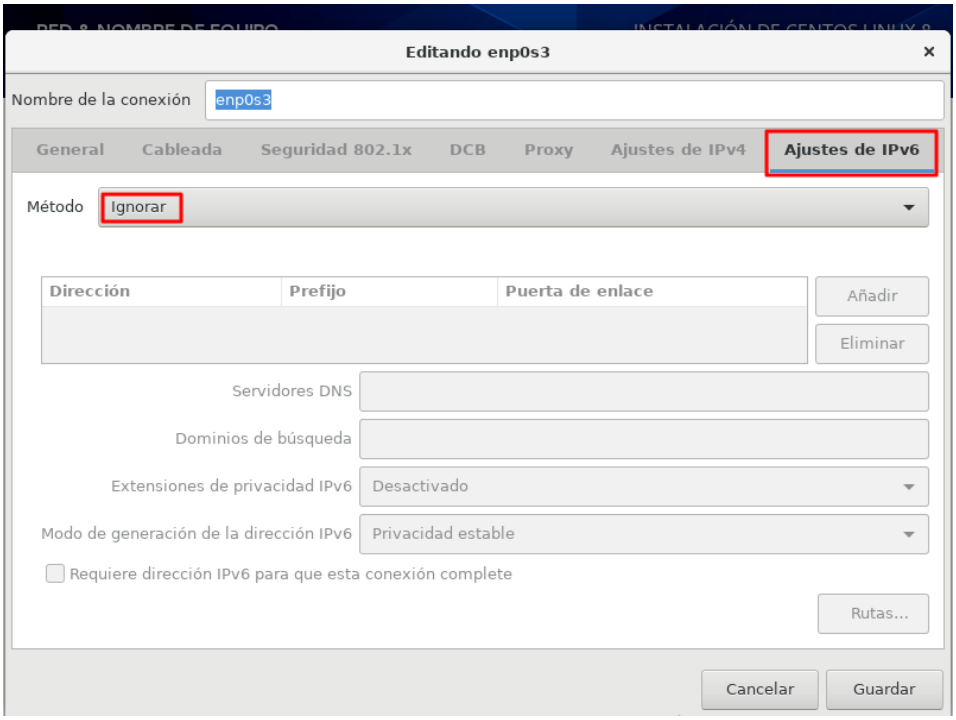
Paso	Descripción
3.	Cuando se le indique en pantalla, seleccione el idioma y la configuración de teclado en español. Pulse “Continuar” para seguir. 
4.	Compruebe que el título **REGIONALIZACIÓN** coincide con las preferencias de idioma y huso horario anteriormente configurados. 

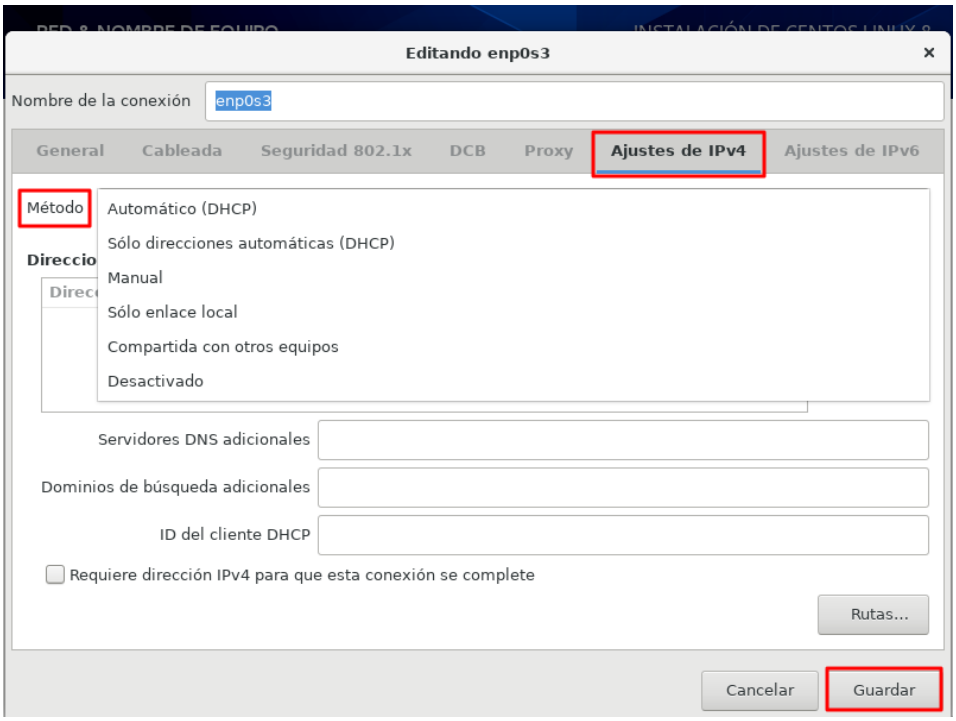
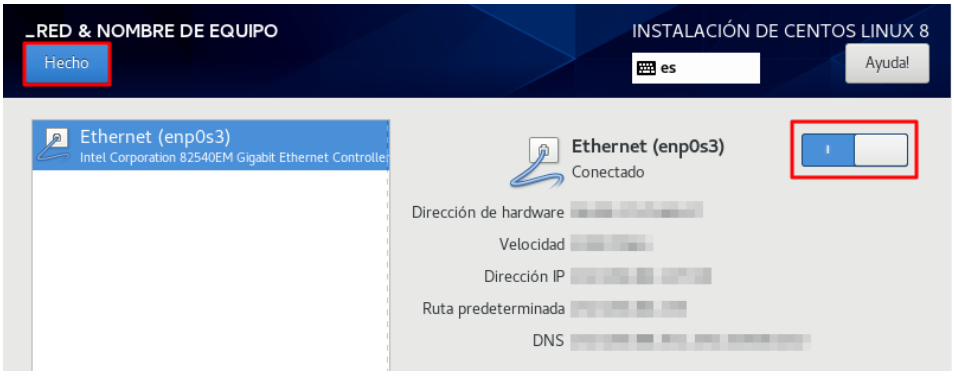
Paso	Descripción
5.	Si necesita cambiar algún parámetro de regionalización, pulse en el icono correspondiente y al finalizar pulse la tecla “Hecho”. 
6.	En el título **SOFTWARE**, seleccione el icono “Selección de software” 

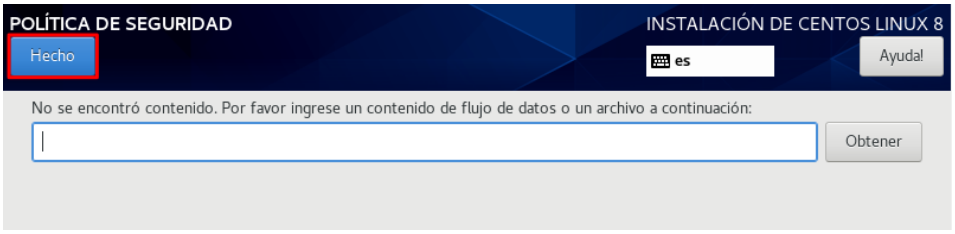
Paso	Descripción
7.	En el apartado “Entorno Base”, seleccione “Servidor con GUI” y en el apartado “Complementos para el entorno seleccionado”, no seleccione ninguna opción. En el caso de que algún casillero de este apartado estuviera marcado, deselecciónelo y posteriormente pulse “Hecho”. 
8.	En el título **SISTEMA**, seleccione el icono “Destino de la instalación”. 

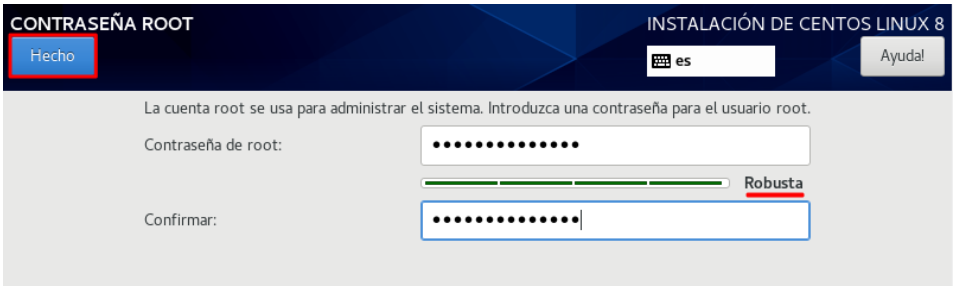
Paso	Descripción
9.	En el apartado “Discos estándares locales” verifique que el disco duro se ha detectado correctamente mediante la comprobación de la capacidad del sistema de almacenamiento y que el “check” de color blanco sobre fondo redondo negro se encuentra encima del icono del disco duro indicando que está seleccionado. Si no fuera así pulse sobre el icono del disco duro hasta que el icono quede seleccionado como en la siguiente imagen. 
10.	En el apartado “Configuración de almacenamiento” seleccione la opción “Automática” y posteriormente pulse el botón “Hecho”.  **Nota:** La capacidad del disco duro y de las particiones viene expresada en GiB que es una unidad de información utilizada como un múltiplo del byte. 1 GiB equivale a 1,07374 Gb.

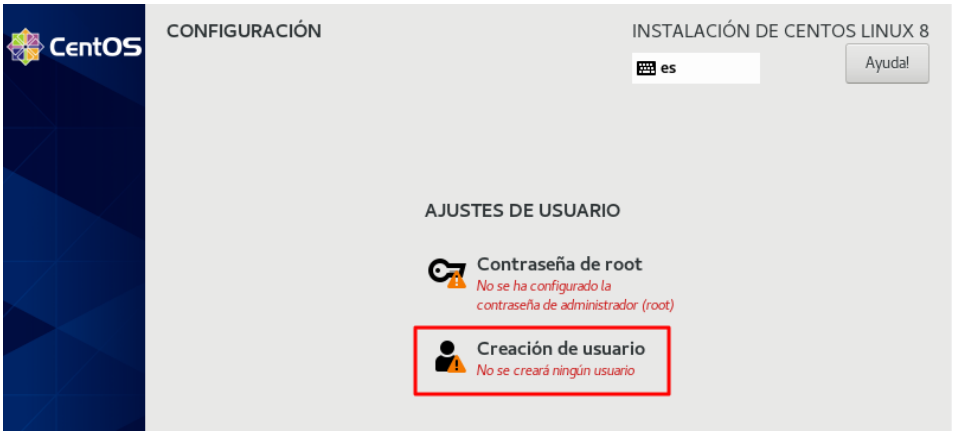
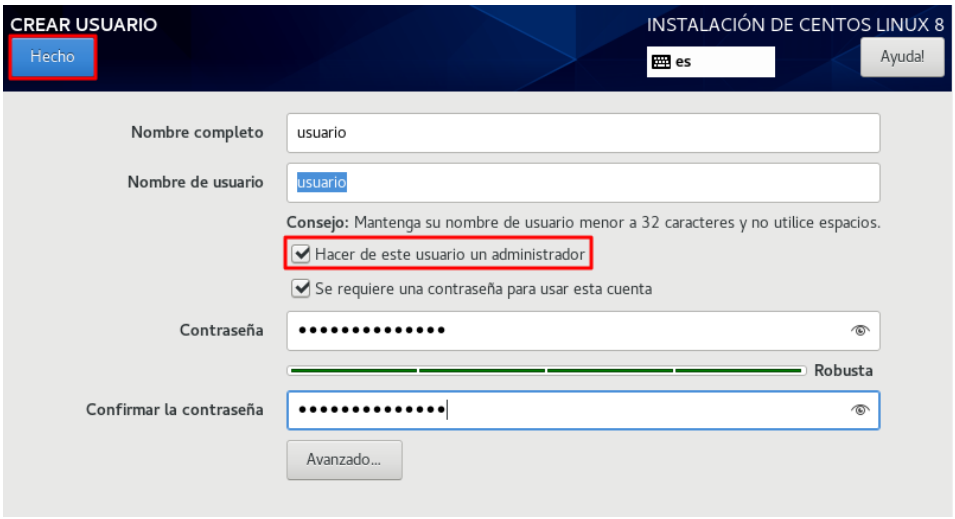
Paso	Descripción
11.	Vuelva al título **SISTEMA** y fíjese que “KDUMP” esté habilitado, si no es así habilítelo pulsando en el icono “KDUMP”, se configurará de forma automática y posteriormente pulse el botón “Hecho”. 
12.	Ahora en el apartado **SISTEMA**, sitúe el cursor encima del icono “Red y Nombre de Equipo” y pulse sobre él. Esto le llevará al menú de configuración de la red y nombre del equipo. 

Paso	Descripción
13.	En el menú "_RED & NOMBRE DE EQUIPO" pulse el botón "Configurar". 
14.	Diríjase a la pestaña "Ajustes de IPv6" y en el menú desplegable "Método" elija la opción "Ignorar". 

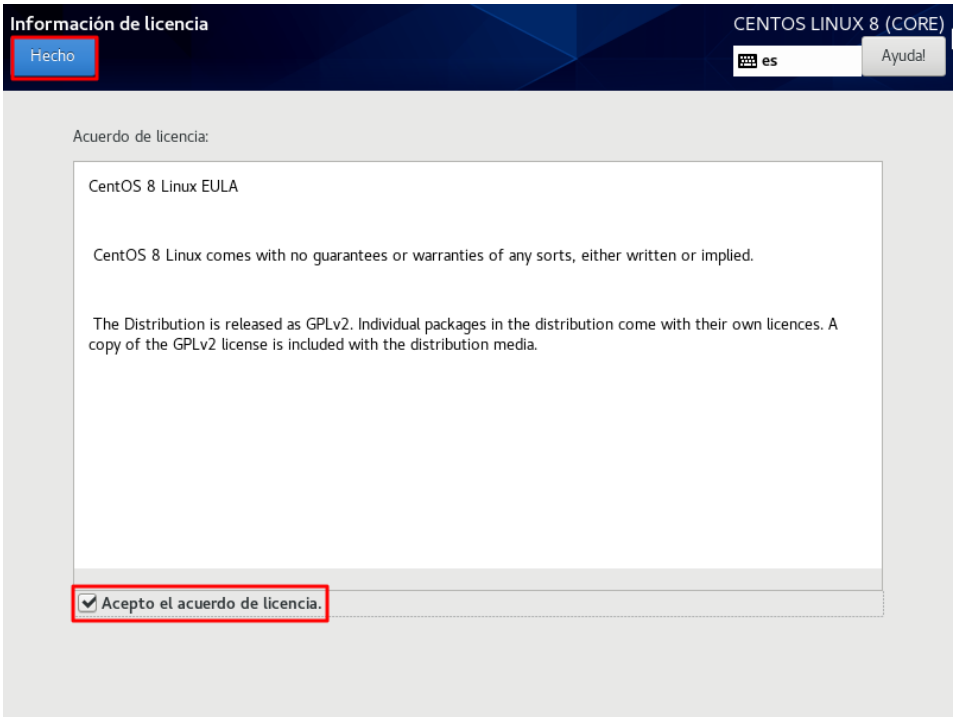
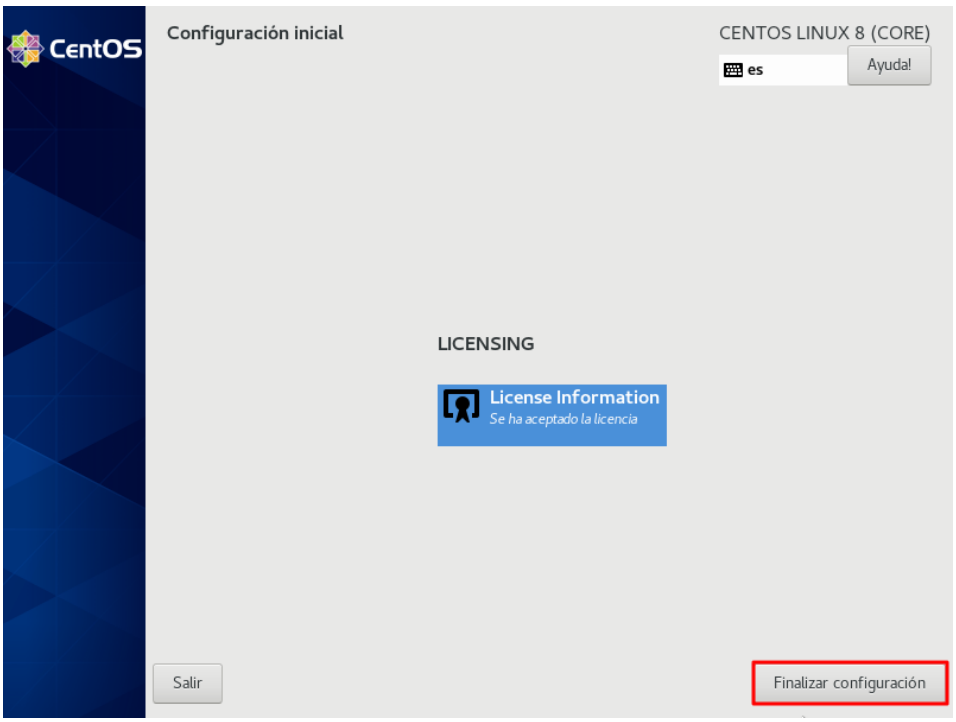
Paso	Descripción
15.	Posteriormente diríjase a la pestaña “Ajustes de IPv4” y en el menú desplegable “Método” elija la opción que más se ajuste a las necesidades de su organización. Posteriormente pulse el botón “Guardar” para aplicar los cambios. 
16.	Cambie el “Nombre de equipo” situado en la parte inferior izquierda de la pantalla por el que desee y pulse el botón “Aplicar”.  Así mismo, en el lado superior derecho de la pantalla, al lado del identificador del dispositivo de red (Ethernet (enp0s3)) hay un botón que se asemeja a un interruptor. Coloque el cursor sobre dicho interruptor y pulse con el botón izquierdo del ratón hasta que se active como se muestra en la imagen. En ese momento debería de actualizarse la información de pantalla y deberá informar la dirección IP, máscara de subred, Ruta predeterminada y DNS del equipo.  Cuando haya finalizado pulse el botón “Hecho”.

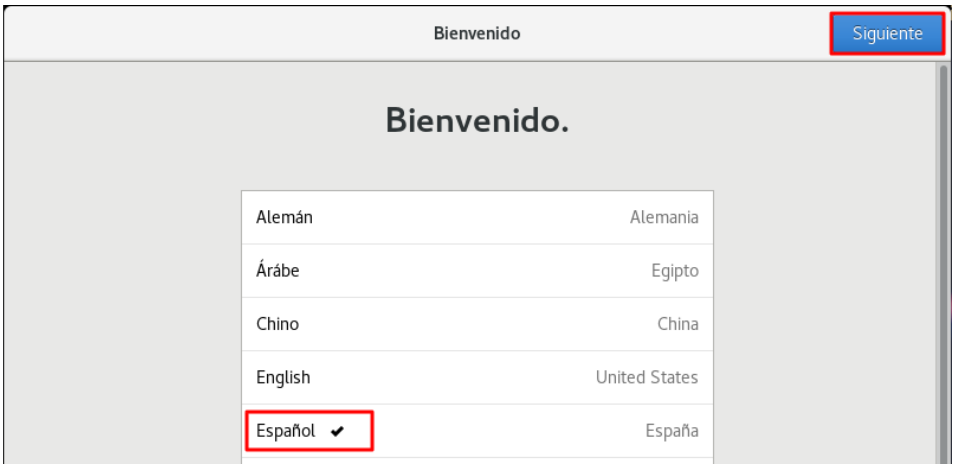
Paso	Descripción
17.	Pulse el icono “Política de seguridad” dentro del menú **SISTEMA**. 
18.	Si su organización posee políticas de seguridad predefinidas, introduzca la URL correspondiente y pulse el botón obtener. En cualquier caso, pulse el botón “Hecho” para regresar al menú **RESUMEN DE LA INSTALACIÓN**. 

Paso	Descripción
19.	Una vez terminados los pasos anteriores, pulse el botón “Empezar instalación” en la parte inferior derecha. 
20.	Mientras que se instala el sistema operativo, se muestra el menú denominado “**AJUSTES DE USUARIO”**, presione en el icono “Contraseña de root”. 
21.	Configure una contraseña con la complejidad requerida y pulse el botón “Hecho”. 

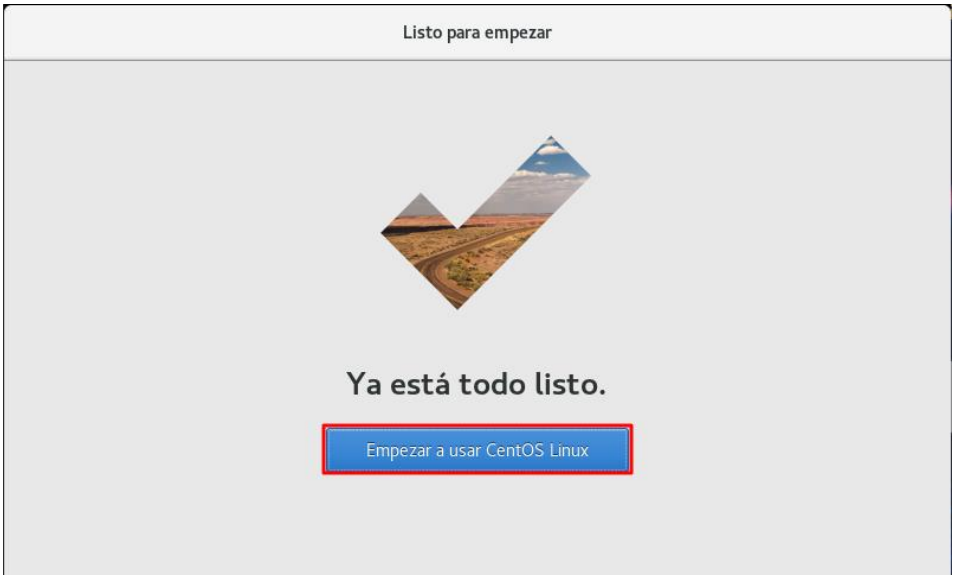
Paso	Descripción
22.	Posteriormente pulse sobre el icono “Creación de usuario” y cree un usuario con permisos de administrador. 
23.	Configure el nombre más adecuado para su organización y seleccione el campo “Hacer que este usuario sea administrador”, fíjese que queda seleccionado el campo “Se requiere una contraseña para usar esta cuenta” y configure una contraseña robusta. Cuando haya finalizado pulse el botón “Hecho”. 

Paso	Descripción
24.	La instalación continuará y cuando finalice, se mostrará un mensaje en la parte inferior y un botón “Reiniciar”. Pulse sobre el botón “Reiniciar” para finalizar la instalación. 
25.	El equipo se reiniciará. Tras el reinicio mostrará el menú denominado “**LICENSING**”, pulse en el icono “License Information”. 

Paso	Descripción
26.	Acepte los términos de licencia seleccionando el campo “Acepto el acuerdo de licencia” y pulse el botón “Hecho”. 
27.	Posteriormente pulse el botón “Finalizar configuración”. 

Paso	Descripción
28.	Ahora el sistema mostrará la pantalla de bienvenida, con el usuario creado. Pulse sobre el usuario e introduzca las credenciales. 
29.	Una vez introducidos las credenciales, pulse el botón “Iniciar sesión”. 
30.	Al iniciar el sistema por primera vez, aparecerá la pantalla de bienvenida del escritorio Gnome. En la primera pantalla compruebe que está configurado el idioma español y pulse el botón “Siguiente”. 

Paso	Descripción
31.	La siguiente pantalla mostrará las opciones de distribución de teclado y métodos de entrada. Revise que se encuentra seleccionado el idioma Español y pulse el botón “Siguiente”. 
32.	La siguiente pantalla mostrará las opciones de Privacidad, pulse en el interruptor de “Servicios de ubicación” para desactivarlo y compruebe se muestra igual que en la imagen. Posteriormente pulse el botón “Siguiente”. 
33.	La siguiente pantalla mostrará la configuración de distintas cuentas en línea, configure las cuentas que más se ajusten a su organización. Si no tiene ninguna pulse el botón “Omitir” y continúe con el siguiente paso. 

Paso	Descripción
34.	Cuando esté todo listo, aparecerá la pantalla “Listo para empezar”, pulse el botón “Empezar a usar CentOS Linux”. 
35.	Por último, se mostrará una ventana llamada “Primeros pasos”, se recomienda leer y seguir los tutoriales si no está familiarizado con el entorno gráfico GNOME. Cuando haya terminado, cierre la ventana. 
36.	Finalmente se mostrará el escritorio.

ANEXO A.3. CATEGORÍA BÁSICA

ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES CENTOS 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

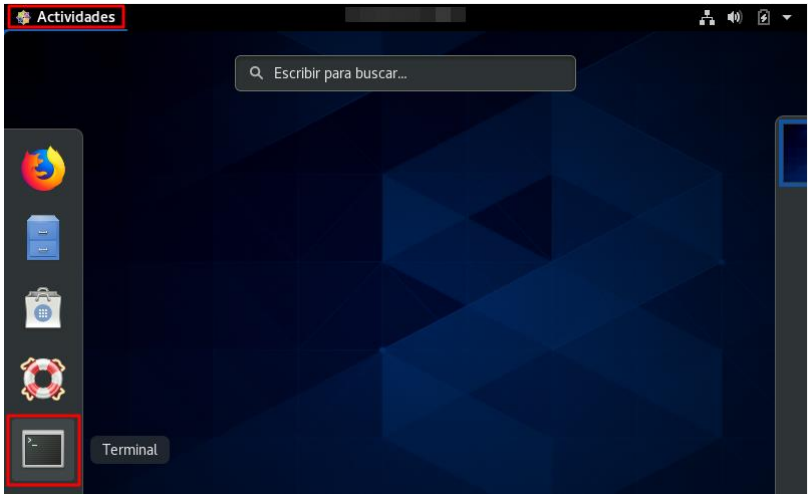
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes CentOS 8 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación 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 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, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

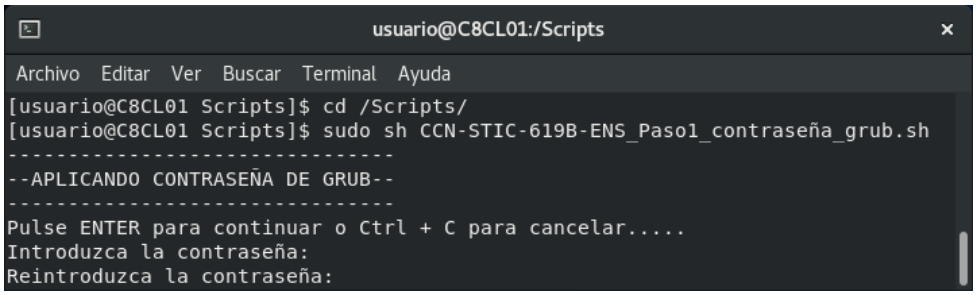
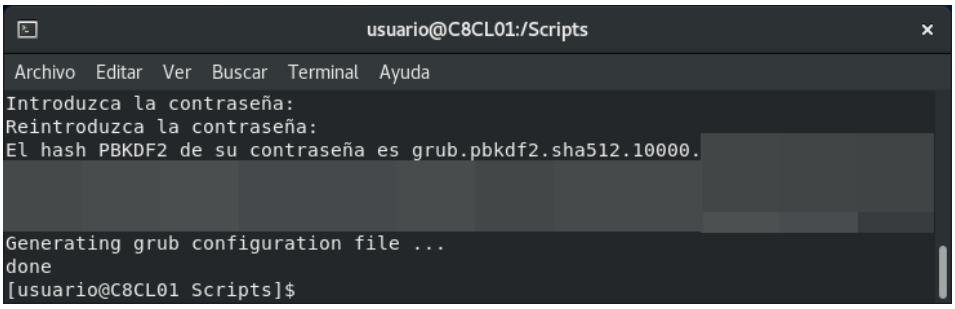
Los pasos que se describen a continuación se realizarán en todos aquellos clientes CentOS 8, independientes a un dominio, que implementen servicios o información de categoría básica y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

1. CONFIGURACIÓN SEGURA DEL ARRANQUE DEL SISTEMA

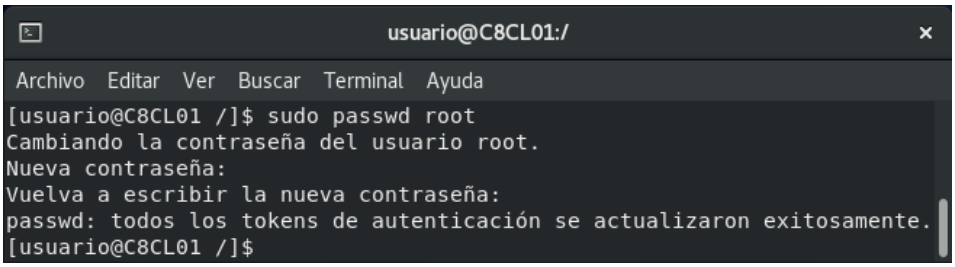
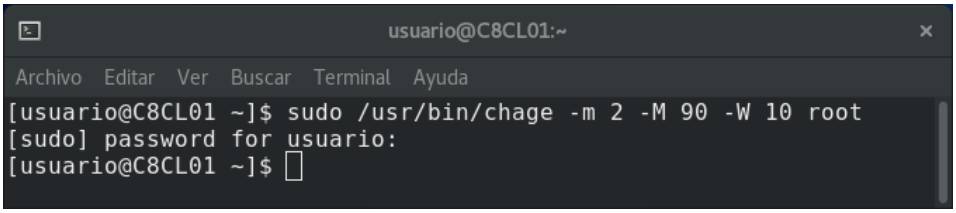
Antes de comenzar se tiene en cuenta que ha realizado los siguientes puntos.

Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS.
2.	Inicie sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Cree la carpeta “**Scripts**” en “**/**” y copie el contenido de la categoría “BÁSICA” correspondiente al directorio “ENS_BASICA” asociado a esta guía en la ruta “**/Scripts**”.
4.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente a la terminal. 
5.	Ejecute el comando “**cd /**” y pulse la tecla “Enter”.

1.1. CONTRASEÑA DE GRUB

Paso	Descripción
6.	Se procede a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso1_contraseña_grub.sh** Pulse “Enter” para continuar. Introduzca la contraseña deseada.  **Nota**: Se generará automáticamente un hash con la contraseña elegida, ese hash no es necesario guardarlo, puesto que ya se ha copiado al fichero de grub. Es importante fijarse en que la última salida por pantalla sea un “done”.  **Nota:** Si se introduce mal la contraseña y las contraseñas no coinciden, no se generará el hash, pero la configuración se exportará vacía al fichero de configuración de grub. Si sucede esto, repita el paso 6 desde el inicio antes de pasar al siguiente punto. Por defecto, el script configura el usuario “root” para iniciar la configuración de grub. Si por requisitos de su organización debe modificar el mismo, deberá adaptar el script a sus necesidades.
7.	No cierre la terminal entre pasos hasta que se le indique, para poder continuar con el proceso. A continuación, introduzca el siguiente comando y pulse “Enter”. **$ clear** **Nota:** Deberá ejecutar este comando cuando requiera “limpiar” la “Terminal”.

1.2. CONTRASEÑA SEGURA DE ROOT

Paso	Descripción
8.	Ejecute el comando "**cd /**" y pulse la tecla "Enter". **Nota:** Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**".
9.	Ejecute el siguiente comando. **$ sudo passwd root**
10.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se mostrará en pantalla el siguiente comentario "Cambiando la contraseña del usuario root". Se pedirá la nueva contraseña y la confirmación de la misma. 
11.	Cuando el proceso haya terminado se mostrará el siguiente mensaje. "**passwd: todos los tokens de autenticación se actualizaron exitosamente**." Si no muestra ese mensaje, vuelva al paso 8 y repita la operación.
12.	Una vez actualizada la contraseña deberá adaptar la caducidad de la cuenta a los parámetros se seguridad requeridos, para ello ejecute el siguiente comando: **$ sudo /usr/bin/chage -m 2 -M 90 -W 10 root** 

1.3. BÚSQUEDA DE CUENTAS SIN CONTRASEÑA

Paso	Descripción
13.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
14.	Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1**
15.	El comando no debería devolver ningún resultado por pantalla, si por el contrario, sale algún resultado, significaría que esos usuarios no tienen contraseña configurada y deben ser eliminados. **Nota:** Si no conoce el proceso de eliminación de usuarios vaya al punto "3.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS"

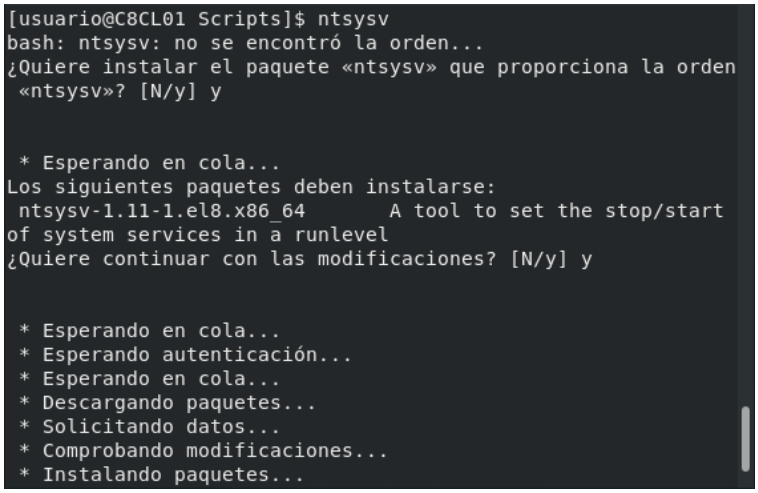
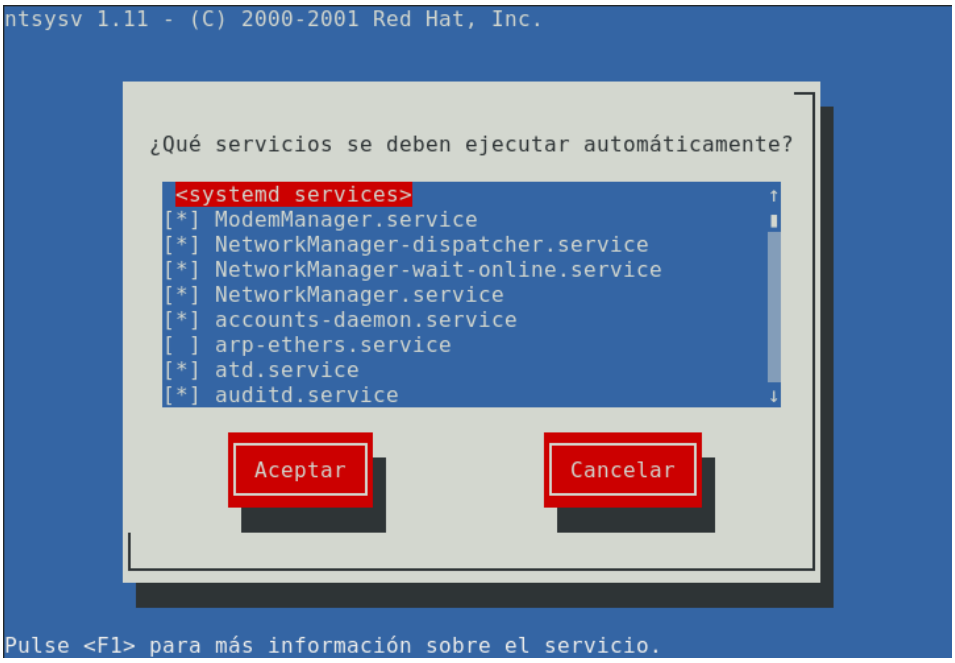
1.4. USUARIOS CON UID 0 QUE NO SEAN ROOT

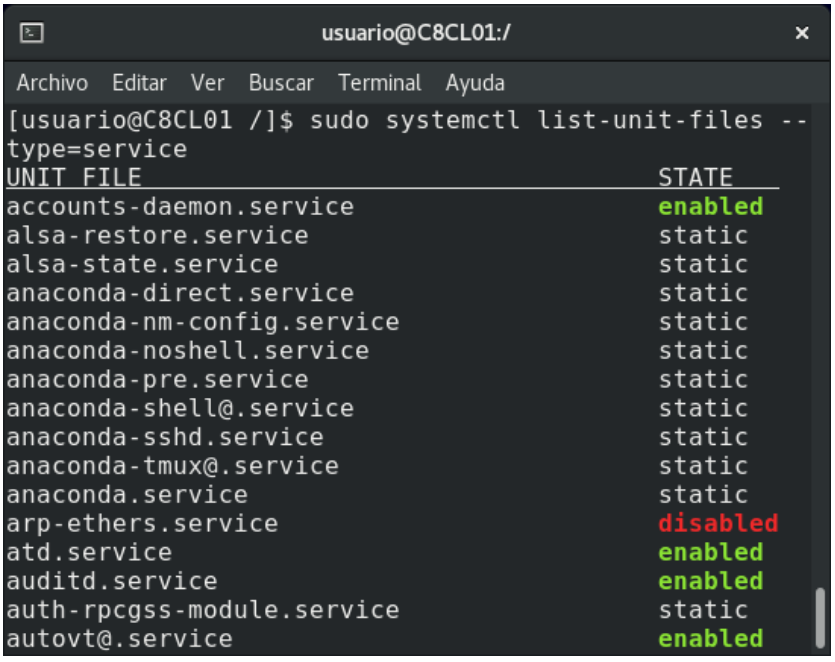
Paso	Descripción
16.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
17.	Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1**
18.	El comando deberá devolver "root" como resultado por pantalla, si por el contrario, sale algún resultado que no sea root, significará que ese/esos usuario/s tienen "UID" 0 y por ende permisos demasiado elevados y deben ser eliminados. **Nota:** Si no conoce el proceso de eliminación de usuarios vaya al punto "3.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

2. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

2.1. LIMITACIÓN DE SERVICIOS Y DEMONIOS

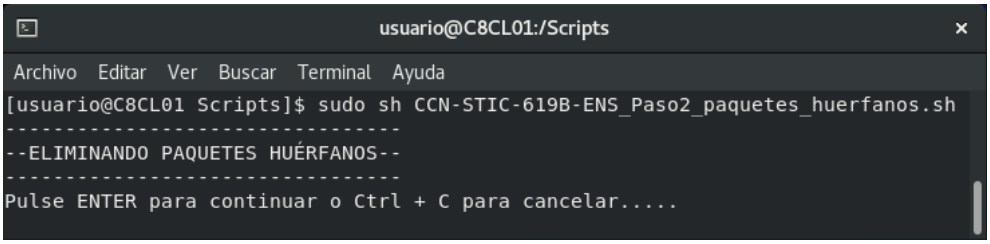
Paso	Descripción
19.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".

Paso	Descripción
20.	En la versión 8 de CentOS no se proporciona la herramienta gráfica de configuración de servicios “ntsysv” de forma nativa con la instalación “servidor con GUI”, no obstante, puede instalarla de forma manual o mediante los medios proporcionados por el propio CentOS.  **Nota:** No es motivo de esta guía especificar las formas de instalación de la herramienta, sin embargo, se debe de tener en consideración que las fuentes de instalación de la misma sean fuentes oficiales y que la versión escogida sea la última recomendada por el fabricante.
21.	Se procede a deshabilitar servicios y demonios innecesarios. Si ha instalado la herramienta “ntsysv” en el punto anterior continúe con el siguiente punto, en caso contrario siga desde el punto 25.
22.	Ejecute el siguiente comando en la terminal. **$ sudo ntsysv** 

Paso	Descripción
23.	El funcionamiento de la herramienta es sencillo, los servicios con un asterisco serán los que estarán habilitados al inicio del sistema. Si quisiera deshabilitar algún servicio, basta con situarse encima del mismo con ayuda de los cursores del teclado y pulsar "**Espacio".** Cuando haya finalizado pulse la tecla **"Tab"** (tabulador) una vez para seleccionar **"Aceptar"** y a continuación pulse "Enter". Si por el contrario quisiera cancelar los cambios, pulse la tecla **"Tab"** dos veces para posicionarse encima del recuadro **"Cancelar"** y pulse "Enter".
24.	Deshabilite todos los servicios innecesarios y mantenga los mínimos necesarios para el correcto funcionamiento del sistema.
25.	Si por necesidades de su organización no cabe la posibilidad de instalación de la herramienta "ntsysv", deberá hacer uso de la terminal por medio de comandos de systemctl. Para revisar el estado del total de los servicios del sistema. Ejecute el siguiente comando. Introduzca la contraseña si se le solicita. **$ sudo systemctl list-unit-files --type=service**  **Nota:** Si necesita más información sobre la utilización de systemctl pude ver el siguiente enlace. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/managing-services-with-systemd_configuring-basic-system-settings

2.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

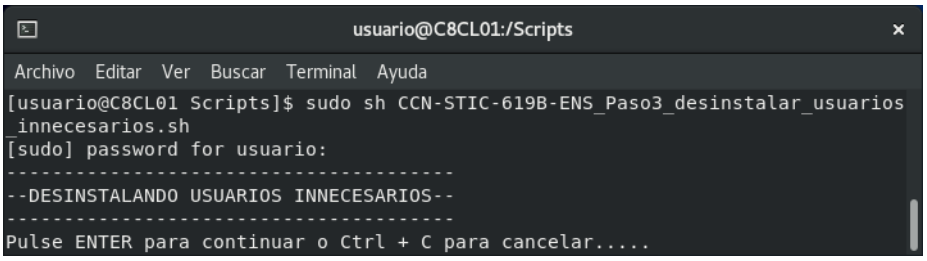
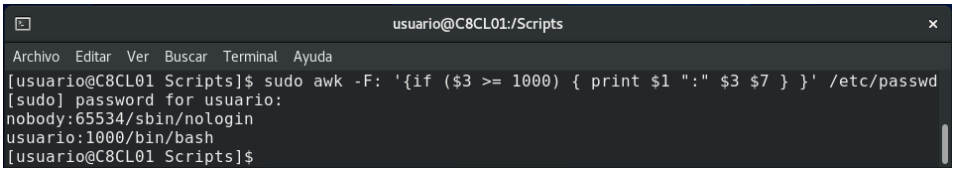
Paso	Descripción
26.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".

Paso	Descripción
27.	En la versión 8 de CentOS no se proporciona el conjunto de herramientas “yum-utils” de forma nativa con la instalación “servidor con GUI”, no obstante, puede instalarla de forma manual o mediante los medios proporcionados por el propio CentOS. El script que se ejecutará en el paso siguiente, comprobará e instalará si es necesario los paquetes requeridos. Compruebe que tiene correctamente configurado un repositorio oficial de CentOS o uno propio de su organización y acceso al mismo antes de continuar.
28.	Se procederá a eliminar los antiguos kernel, los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso2_paquetes_huerfanos.sh**  Pulse “Enter” para comenzar la ejecución del script. El script iniciará un proceso de desinstalación de dichos paquetes, para ello instalará la herramienta “yum-utils” . No pulse ninguna tecla ni cierra la ventana hasta que finalice con un mensaje en pantalla de **“¡Listo!”**. **Nota:** Si el script detectara algún paquete candidato para su desinstalación, una vez finalice el proceso, se recomienda volver al punto 26 de este apartado para revisar los servicios y volver a ejecutar el script, para eliminar posibles paquetes huérfanos.

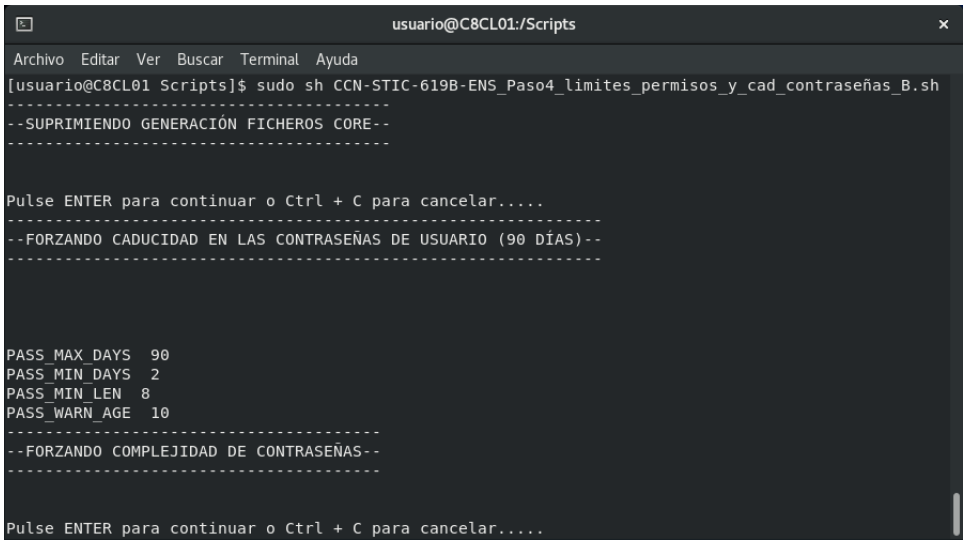
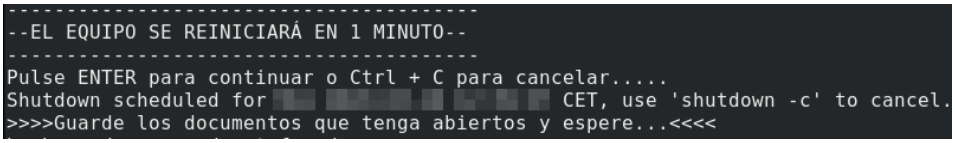
3. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

3.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

Paso	Descripción
29.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “**Terminal**”. Ejecute el comando “**cd /**” y pulse la tecla “Enter”.
30.	Se va a proceder a eliminar los usuarios creados por defecto en la instalación y que son innecesarios. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**

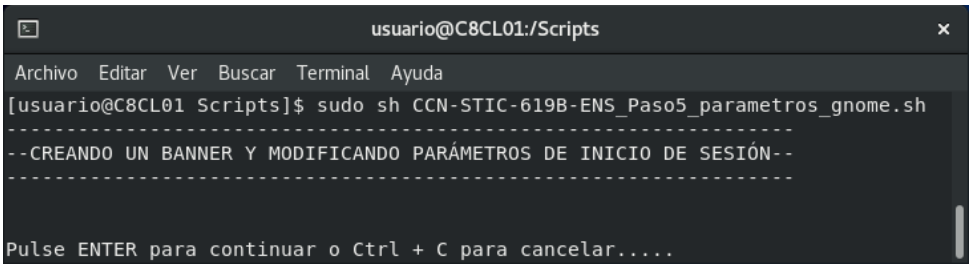
Paso	Descripción
31.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso3_desinstalar_usuarios_innecesarios.sh**  El script iniciará un proceso que deshabilitará los usuarios innecesarios, y corregirá las shells predeterminadas en caso de no ser las correctas. No pulse ninguna tecla ni cierre la ventana hasta que el proceso finalice. Ignore los mensajes de pantalla.
32.	Si ha detectado que en la actualidad está habilitado un usuario que ya no tiene necesidad de acceder al sistema puede usar el siguiente comando (**sin comillas**), siendo **NOMBREDELUSUARIO** el nombre del usuario candidato para su eliminación. **$ sudo userdel -r "NOMBREDELUSUARIO".**
33.	Ahora compruebe las "shells" predeterminadas de los usuarios con UID por encima del número 1000 (usuarios normales del sistema). Para ello ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd** Se mostrarán todos los usuarios y sus respectivas shells. Compruebe que todas las shells de usuario coinciden con "**/bin/bash**".  **Nota:** Como se puede observar puede aparecer el usuario nobody con uid:65534 y como excepción se deberá conservar su shell. Por defecto, los directorios compartidos NFS cambian el usuario root (superusuario) por el usuario nfsnobody, una cuenta de usuario sin privilegios. De esta forma, todos los archivos creados por root son propiedad del usuario nfsnobody, lo que previene la carga de programas con la configuración del bit setuid. En Centos 8 el usuario "nobody" sustituye a "nfsnobody" para los siguientes grupos y usuarios: - El par de usuarios nobody y grupos con el ID de 99. - El par de usuario nfsnobody y grupo con el ID de 65534, que también es el ID de desbordamiento predeterminado del núcleo. Este cambio reduce la confusión sobre los archivos que son propiedad de NFS nobody pero no tienen nada que ver con NFS.
34.	Cuando finalice todas las tareas reinicie el sistema.

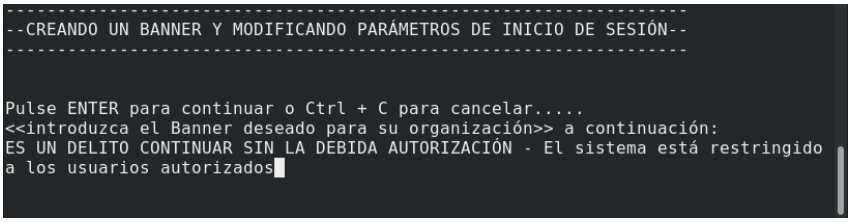
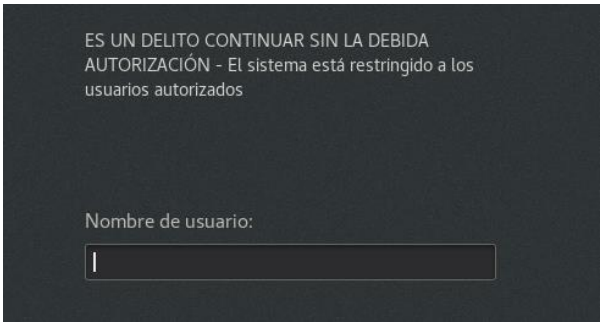
3.2. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

Paso	Descripción
35.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
36.	Antes de comenzar este paso, asegúrese de haber cerrado y guardado las aplicaciones y los documentos importantes. Se va a proceder a limitar los recursos disponibles para los usuarios, en particular limitar los "**volcados de núcleo** (core dumps)". Así mismo se forzará la caducidad de contraseñas para los nuevos usuarios y los ya existentes, la complejidad y los permisos en los directorios "/home" de cada usuario. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente script. **$ sudo sh CCN-STIC-619B-ENS_Paso4_limites_permisos_y_cad_contraseñas_B.sh**  Cuando finalice el script, saldrá un mensaje advirtiendo que el sistema se reiniciará en 1 minuto. Espere y cierre las aplicaciones que tenga abiertas. 

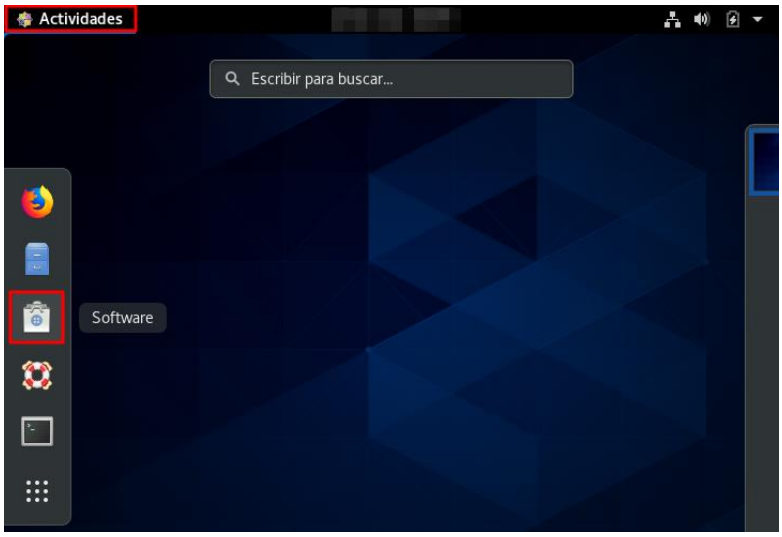
Paso	Descripción
37.	Cuando reinicie el sistema e inicie sesión, aparecerá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos. 
38.	Le pedirá la contraseña actual de nuevo y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.

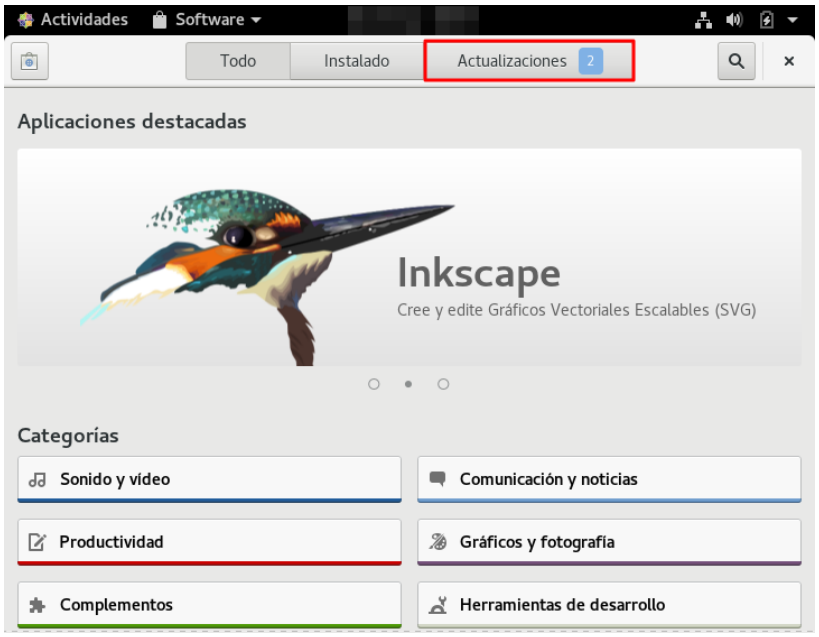
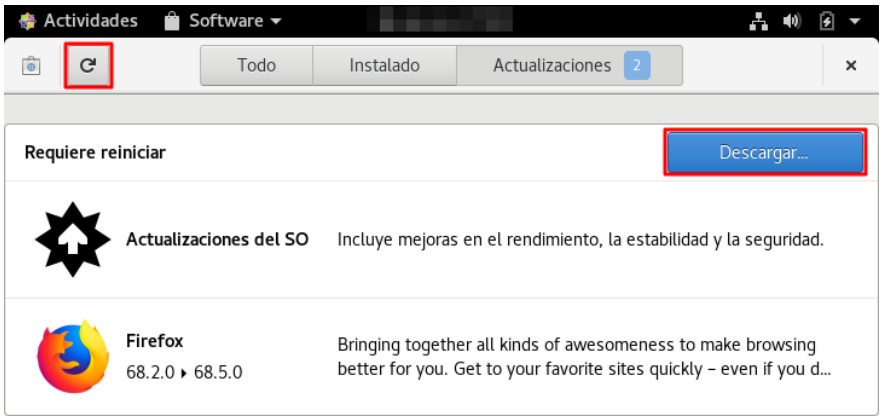
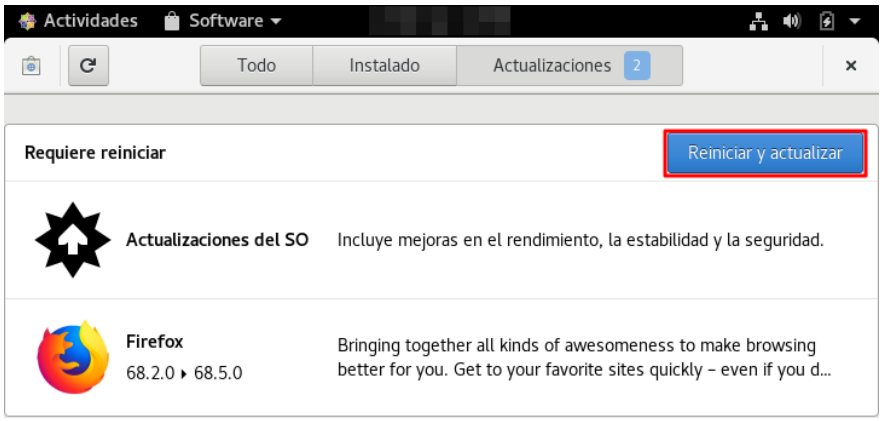
3.3. CONFIGURACIÓN SEGURA DE GNOME

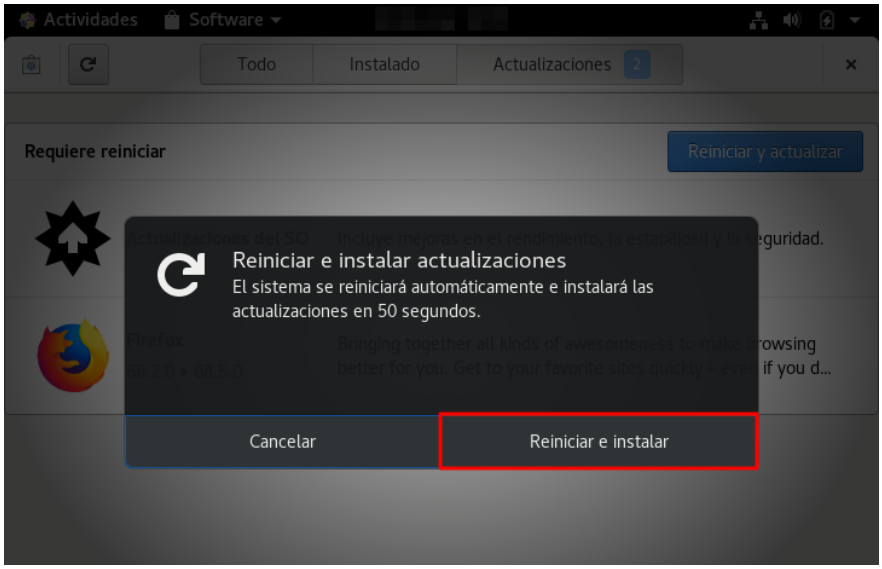
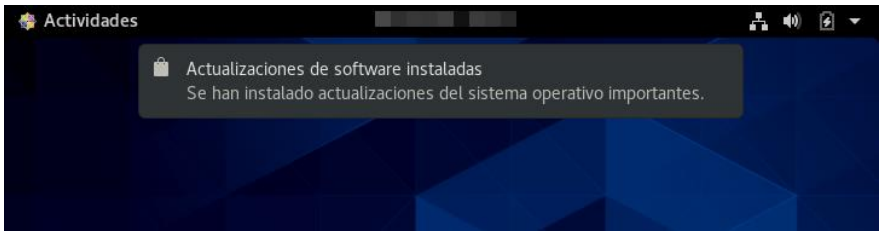
Paso	Descripción
39.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
40.	Se va a proceder a configurar parámetros de seguridad en el escritorio Gnome. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso5_parametros_gnome.sh** 

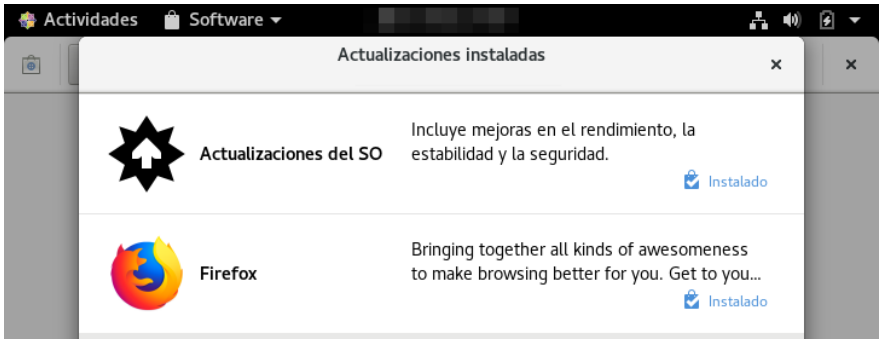
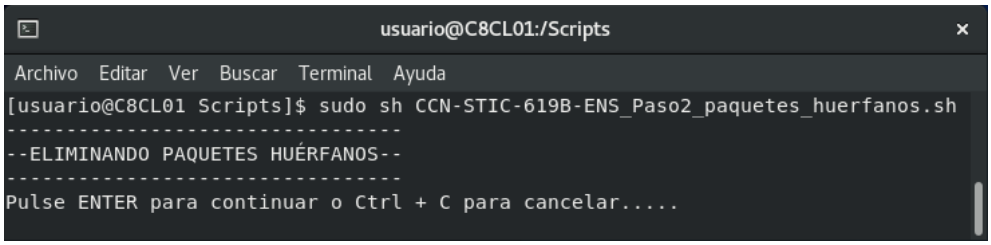
Paso	Descripción
41.	Introduzca el Banner deseado acorde con su organización. 
42.	El script iniciará un proceso que modificará la pantalla de inicio de CentOS 8 Linux para que aparezca un mensaje disuasorio (banner) al inicio y solicite usuario y contraseña. Así mismo se configurará un tiempo mínimo de bloqueo según requisitos de seguridad.  **Nota:** CentOS 8 Linux presenta mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

4. APLICACIÓN DE ACTUALIZACIONES

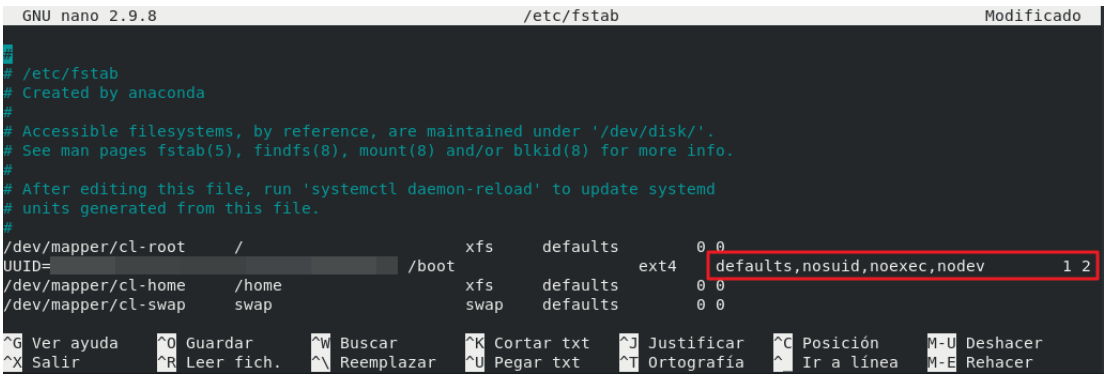
Paso	Descripción
43.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a “**Software**”. 

Paso	Descripción
44.	Una vez iniciada la aplicación, pulse sobre la pestaña “Actualizaciones”. 
45.	pulse sobre el botón de la flecha. ⟳ Comprobará si hay más actualizaciones; cuando finalice pulse en el botón “Descargar…”. 
46.	Cuando las actualizaciones se descarguen pulse “Reiniciar y Actualizar”- 

Paso	Descripción
47.	Confirme el reinicio en el botón 
48.	El sistema se reiniciará y comenzará a instalar las actualizaciones.  El proceso puede durar varios minutos, no presione ninguna tecla hasta que el proceso de actualización finalice.
49.	Cuando finalice, aparecerá la pantalla de inicio de CentOS 8. Inicie sesión y le saldrá un mensaje en el escritorio que le notificará las actualizaciones instaladas. 

Paso	Descripción
50.	Si presiona sobre el mensaje, aparecerán todas las aplicaciones que han sido actualizadas para su comprobación. 
51.	Cuando termine de revisar, cierre la ventana y su sistema estará actualizado. 
52.	Una vez finalizada la actualización, vuelva a ejecutar el script "CCN-STIC-619B-ENS_Paso2_paquetes_huerfanos.sh" del punto "2.2 COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS". Para ello diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "Terminal". Ejecute el comando "**cd /**" y pulse la tecla "**Enter**". Diríjase a la carpeta "**/Scripts**" y ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso2_paquetes_huerfanos.sh**  El script iniciará un proceso de desinstalación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice con un mensaje en pantalla de "¡Listo!".
53.	Reinicie el sistema para finalizar el proceso.

5. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

Paso	Descripción
54.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
55.	Ejecute el siguiente comando e introduzca la contraseña si se le solicita. **$ sudo nano /etc/fstab**
56.	Edite el fichero de configuración con el editor de textos "nano", modificando los permisos de la partición "/boot" para que el resultado sea similar al de la imagen (defaults,nosuid,noexec,nodev 1 2).  **Nota:** Para la modificación del fichero con el editor "nano" deberá navegar por el fichero mediante las flechas del teclado y modificar los datos eliminando o añadiendo las partes necesarias. Para guardar, pulse la combinación de teclas "Crtl + o" y luego "Enter" y para salir pulse la combinación de teclas "Crtl + x". Si requiere mas información sobre la utilización del editor "nano" diríjase a la siguiente URL: https://www.nano-editor.org/dist/v2.1/nano.html
57.	Cuando finalice de editar, pulse la combinación de teclas "Crtl + o" y luego "Enter" para guardar y la combinación de teclas "Crtl + x" para salir. Elimine el directorio "/Scripts" y todo su contenido. **Nota:** Debe tener en consideración, que para realizar actualizaciones del kernel es posible que deba restablecer los valores de la partición "/boot" a defaults y posteriormente cuando la actualización finalice, revertirlos a los establecidos por esta guía.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE CLIENTE CENTOS 8 PARA LA CATEGORÍA BÁSICA

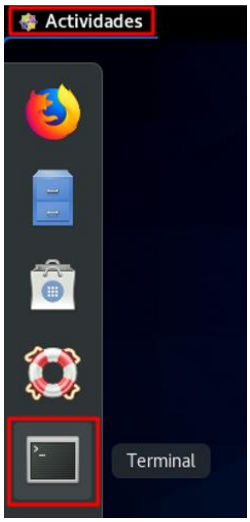
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.3.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES CENTOS 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS".

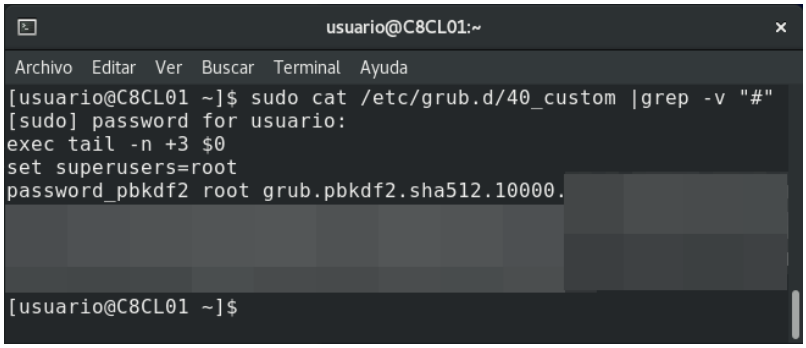
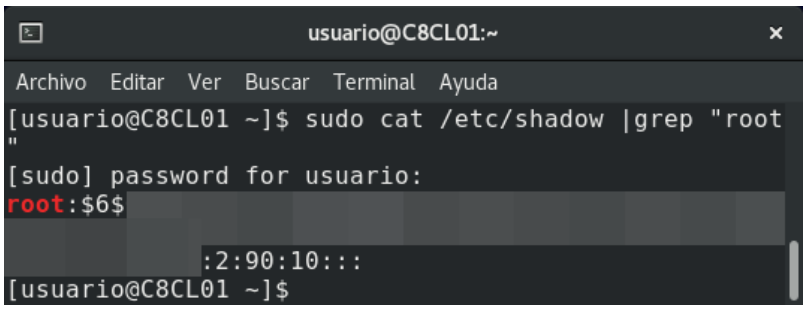
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes CentOS 8 independientes con implementación de seguridad en la categoría básica del ENS.

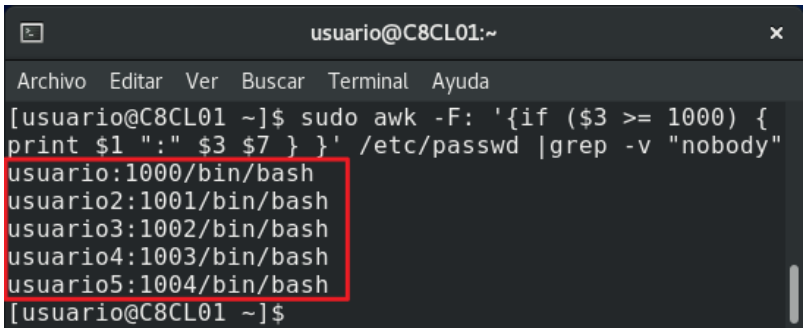
Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

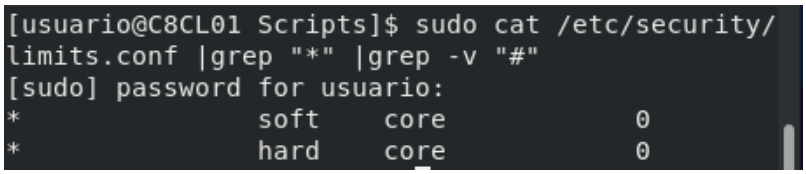
Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas que se utilizarán son las siguientes:

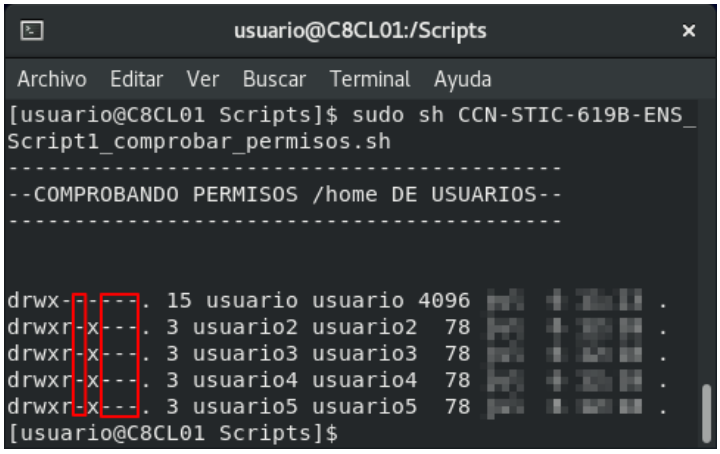
a) Terminal de Linux

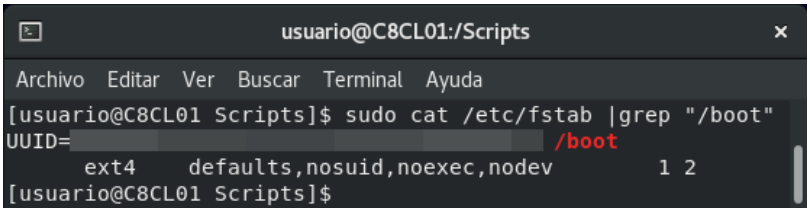
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de root. Cree la carpeta "Scripts" en "/" y copie el contenido del nivel de seguridad "BÁSICA" correspondiente al directorio "Scripts/ENS_BASICA" asociado a esta guía en la ruta "/Scripts".
2. Inicie la Terminal de Linux.		Ejecute la "Terminal", para ello diríjase a la barra de tareas superior, pulse sobre "Actividades" y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen. 

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que grub tiene contraseña configurada y root como único usuario de modificación.		En la "Terminal" ejecute el siguiente comando. **$ sudo cat /etc/grub.d/40_custom |grep -v "#"**  **Nota:** Fíjese en las letras y números que están situadas después de "password_pbkdf2 root grub.pbkdf2.sha512.". Pueden ser diferentes dependiendo del usuario, ya que se trata de un hash generado a partir de la contraseña dada al ejecutar el script.
4. Contraseña de root segura.		Abra la Terminal y ejecute el siguiente comando. **$ sudo cat /etc/shadow |grep "root"**  Fíjese que el inicio del hash de la contraseña de "root" comienza por "**6**", esto le indicará en qué tipo de hash está la contraseña de "root", en este caso es SHA-512, (Secure Hash Algorithm) y por lo tanto tiene 86 caracteres en total. Fíjese adicionalmente en que el final de la configuración termina por "**:2:90:10:::**" indicando que se ha configurado correctamente la caducidad de la cuenta.
5. Búsqueda de usuarios sin contraseña.		Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1** **Nota:** Si la configuración es correcta, no deberá mostrar ningún resultado la salida del comando.

Comprobación	OK/NOK	Cómo hacerlo
6. Búsqueda de usuarios con UID 0.		Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1 |grep -v "root"** **Nota:** Si la configuración es correcta, no deberá mostrar ningún resultado la salida del comando.
7. Servicios innecesarios		Abra la Terminal y ejecute el siguiente comando. **$ sudo systemctl list-unit-files --type=service**  Revise que los servicios activos al iniciar el sistema son los correctos para su organización.
8. Comprobación de usuarios y shells predeterminadas.		Ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $7 } }' /etc/passwd |grep -v "nobody"**  Compruebe si los usuarios que se muestran son los más adecuados para su organización y que están correctas las shells predeterminadas.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Configuración de los volcados de núcleo (core dumps)</td><td></td><td>Ejecute el siguiente comando.
$ sudo cat /etc/security/limits.conf |grep "*" |grep -v "#"
 
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Soft core</td><td>0</td><td></td></tr>
<tr><td>Hard core</td><td>0</td><td></td></tr>
</table></td></tr>
<tr><td>10. Banner disuasorio.</td><td></td><td>Ejecute los siguientes comandos.
$ cat /etc/issue
$ cat /etc/issue.net
$ cat /etc/motd
Compruebe si se han configurado bien los mensajes disuasorios (banners).</td></tr>
<tr><td>11. Verifique la directiva de caducidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MAX_DAYS"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MIN_DAYS"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MIN_LEN"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_WARN_AGE"
$ sudo cat /etc/login.defs |grep "UMASK"
$ sudo cat /etc/login.defs |grep "ENCRYPT_METHOD"
Compruebe si se han configurado bien los siguientes valores.
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>PASS_MAX_DAYS</td><td>90</td><td></td></tr>
<tr><td>PASS_MIN_DAYS</td><td>2</td><td></td></tr>
<tr><td>PASS_MIN_LEN</td><td>8</td><td></td></tr>
<tr><td>PASS_WARN_AGE</td><td>10</td><td></td></tr>
<tr><td>UMASK</td><td>027</td><td></td></tr>
<tr><td>ENCRYPT_METHOD</td><td>SHA512</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="6">12.Verifique la directiva de complejidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/security/pwquality.conf |grep "minlen ="
$ sudo cat /etc/security/pwquality.conf |grep "dcredit ="
$ sudo cat /etc/security/pwquality.conf |grep "ucredit ="
$ sudo cat /etc/security/pwquality.conf |grep "lcredit ="
Compruebe si se han configurado bien los siguientes valores.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>minlen</td><td>8</td><td></td></tr>
<tr><td>dcredit</td><td>-1</td><td></td></tr>
<tr><td>ucredit</td><td>-1</td><td></td></tr>
<tr><td>lcredit</td><td>-1</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>Se va a proceder a revisar los permisos de la ruta “/home” de casa usuario del sistema.
Para ello diríjase a la carpeta “Scripts”.
$ cd /Scripts
Ejecute el siguiente comando.
$ sudo sh CCN-STIC-619B-ENS_Script1_comprobar_permisos.sh
El script mostrará los permisos de las carpetas “/home” y se debe comprobar que coincidan las columnas marcadas se encuentren vacías.
 
</td></tr>
<tr><td></td><td></td></tr>
<tr><td>13.Configuración de Gnome</td><td></td><td>Se va a proceder a revisar los parámetros de configuración de Gnome.
Para ello ejecute los siguientes comandos.
$ cat /etc/dconf/db/gdm.d/01-banner-message</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>banner-message-enable</td><td>true</td><td></td></tr>
<tr><td>banner-message-text</td><td>“Texto elegido”</td><td></td></tr>
</table>
$ cat /etc/dconf/db/gdm.d/00-login-screen |grep "disable-user-list"
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>disable-user-list</td><td>true</td><td></td></tr>
</table>
$ cat /etc/dconf/db/local.d/00-screensaver |grep "idle-delay=uint32"
$ cat /etc/dconf/db/local.d/00-screensaver |grep "lock-enabled"
$ cat /etc/dconf/db/local.d/00-screensaver |grep "lock-delay=uint32"
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>idle-delay=uint32</td><td>1800</td><td></td></tr>
<tr><td>lock-enabled</td><td>true</td><td></td></tr>
<tr><td>lock-delay=uint32</td><td>1</td><td></td></tr>
</table>
$ cat /etc/dconf/db/local.d/03-privacy |grep "hide-identity"
$ cat /etc/dconf/db/local.d/03-privacy |grep "old-files-age"
$ cat /etc/dconf/db/local.d/03-privacy |grep "remember-recent-files"
$ cat /etc/dconf/db/local.d/03-privacy |grep "remove-old-temp-files"
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>hide-identity</td><td>true</td><td></td></tr>
<tr><td>old-files-age</td><td>0</td><td></td></tr>
<tr><td>remember-recent-files</td><td>false</td><td></td></tr>
<tr><td>remove-old-temp-files</td><td>true</td><td></td></tr>
</table>
</td></tr>
<tr><td>14. Permisos partición de inicio.</td><td></td><td>Compruebe que se han guardado los permisos en el fichero de configuración.
$ sudo cat /etc/fstab |grep "/boot"
 
</td></tr>
</table>

ANEXO A.4. CATEGORÍA MEDIA

ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES CENTOS 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

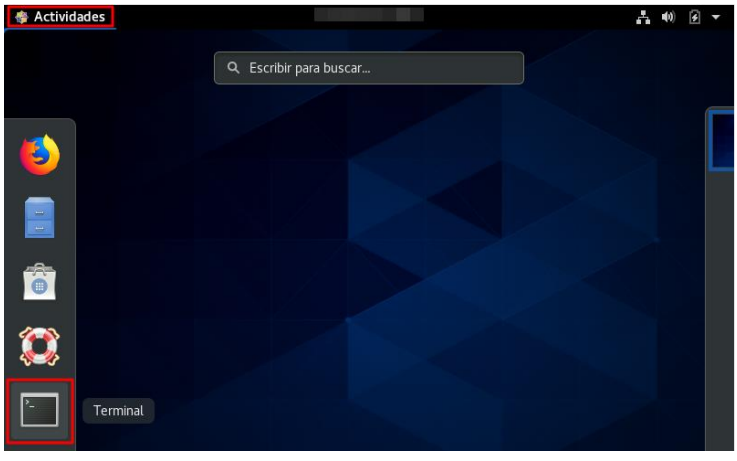
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes CentOS 8 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar 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 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, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

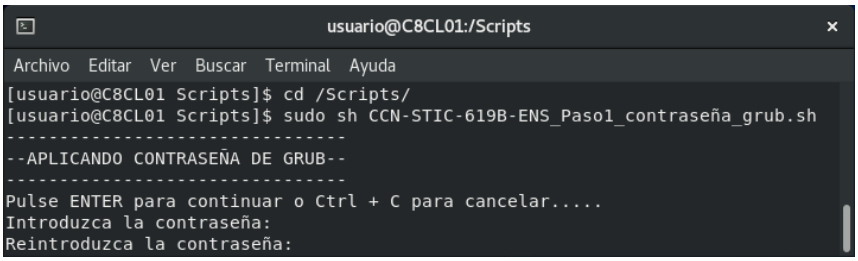
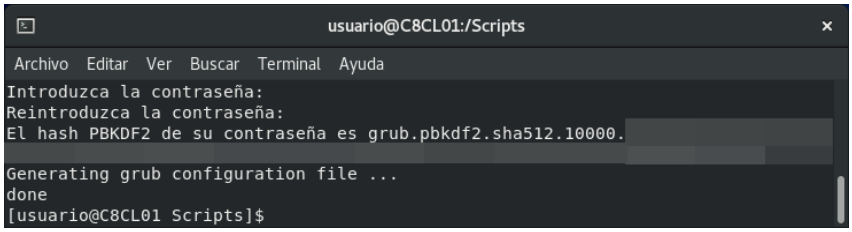
Los pasos que se describen a continuación se realizarán en todos aquellos clientes CentOS 8, independientes a un dominio, que implementen servicios o información de categoría media y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

1. CONFIGURACIÓN SEGURA DEL ARRANQUE DEL SISTEMA

Antes de comenzar se tiene en cuenta que ha realizado los siguientes puntos.

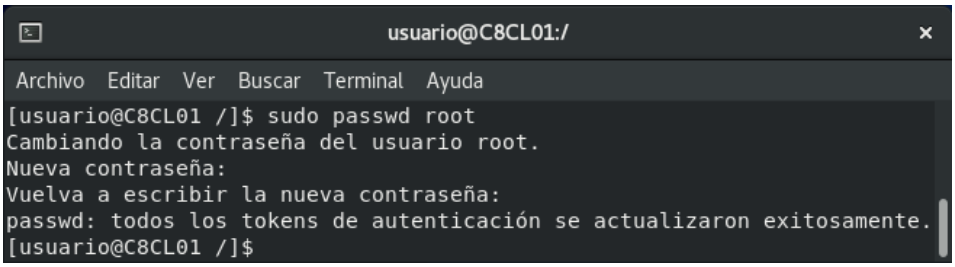
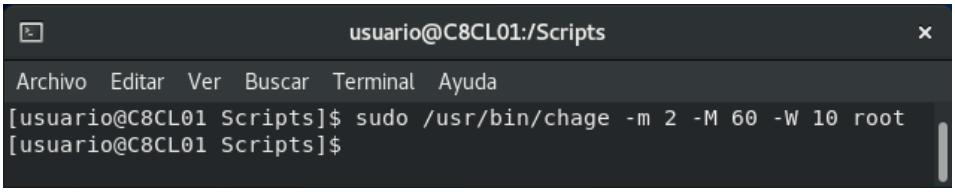
Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS.
2.	Inicie sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Cree la carpeta “**Scripts**” en “**/**” y copie el contenido de la categoría “MEDIA” correspondiente al directorio “ENS_MEDIA” asociado a esta guía en la ruta “**/Scripts**”.
4.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente a la terminal. 
5.	Ejecute el comando “**cd /**” y pulse la tecla “Enter”.

1.1. CONTRASEÑA DE GRUB

Paso	Descripción
6.	Se procede a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso1_contraseña_grub.sh** Pulse “Enter” para continuar. Introduzca la contraseña deseada.  **Nota**: Se generará automáticamente un hash con la contraseña elegida, ese hash no es necesario guardarlo, puesto que ya se ha copiado al fichero de grub. Es importante fijarse en que la última salida por pantalla sea un “done”.  **Nota:** Si se introduce mal la contraseña y las contraseñas no coinciden, no se generará el hash, pero la configuración se exportará vacía al fichero de configuración de grub. Si sucede esto, repita el paso 6 desde el inicio antes de pasar al siguiente punto. Por defecto, el script configura el usuario “root” para iniciar la configuración de grub. Si por requisitos de su organización debe modificar el mismo, deberá adaptar el script a sus necesidades.
7.	No cierre la terminal entre pasos hasta que se le indique, para poder continuar con el proceso. A continuación, introduzca el siguiente comando y pulse “Enter”. **$ clear** **Nota:** Deberá ejecutar este comando cuando requiera “limpiar” la “Terminal”.

1.2. CONTRASEÑA SEGURA DE ROOT

Paso	Descripción
8.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “**Terminal**”. Ejecute el comando “**cd /**” y pulse la tecla “Enter”.

Paso	Descripción
9.	Ejecute el siguiente comando. **$ sudo passwd root**
10.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se mostrará en pantalla el siguiente comentario "Cambiando la contraseña del usuario root". Se pedirá la nueva contraseña y la confirmación de la misma. 
11.	Cuando el proceso haya terminado se mostrará el siguiente mensaje. "**passwd: todos los tokens de autenticación se actualizaron exitosamente**." Si no muestra ese mensaje, vuelva al paso 8 y repita la operación.
12.	Una vez actualizada la contraseña deberá adaptar la caducidad de la cuenta a los parámetros se seguridad requeridos, para ello ejecute el siguiente comando: **$ sudo /usr/bin/chage -m 2 -M 60 -W 10 root** 

1.3. BÚSQUEDA DE CUENTAS SIN CONTRASEÑA

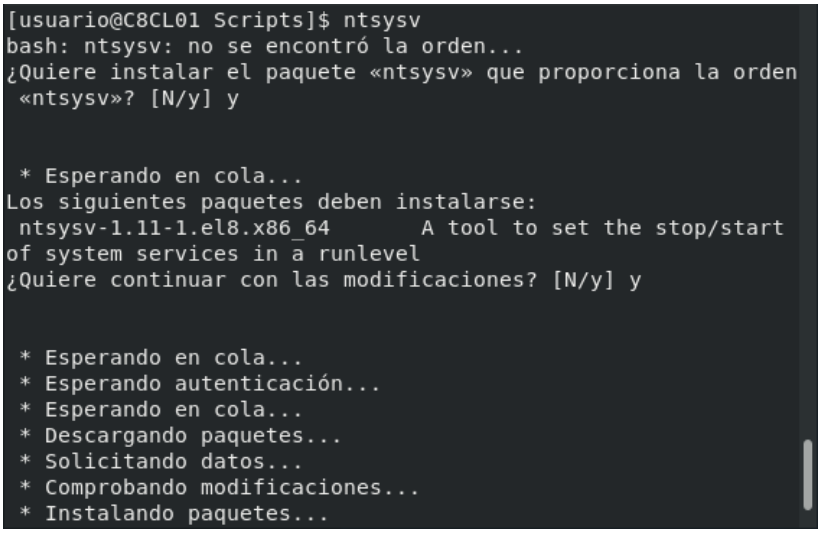
Paso	Descripción
13.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
14.	Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1**
15.	El comando no debería devolver ningún resultado por pantalla, si por el contrario, sale algún resultado, significaría que esos usuarios no tienen contraseña configurada y deben ser eliminados. **Nota:** Si no conoce el proceso de eliminación de usuarios vaya al punto "4.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS"

1.4. USUARIOS CON UID 0 QUE NO SEAN ROOT

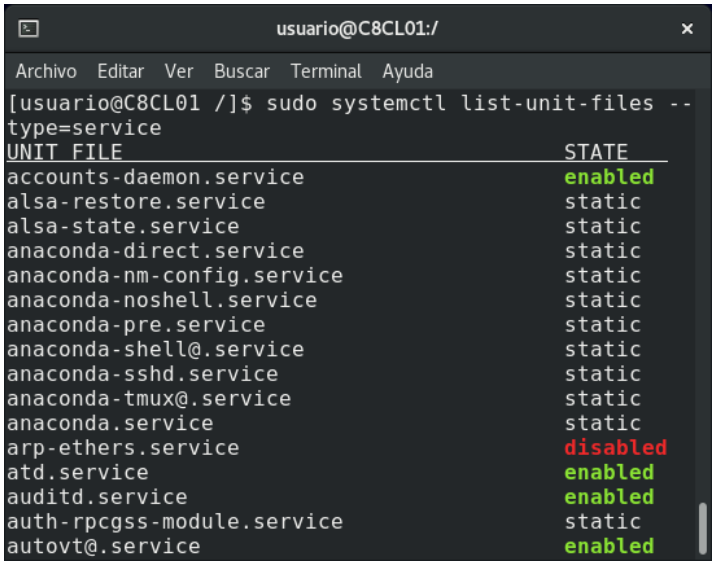
Paso	Descripción
16.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
17.	Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1**
18.	El comando deberá devolver "root" como resultado por pantalla, si por el contrario, sale algún resultado que no sea root, significará que ese/esos usuario/s tienen "UID" 0 y por ende permisos demasiado elevados y deben ser eliminados. **Nota:** Si no conoce el proceso de eliminación de usuarios vaya al punto "4.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

2. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

2.1. LIMITACIÓN DE SERVICIOS Y DEMONIOS

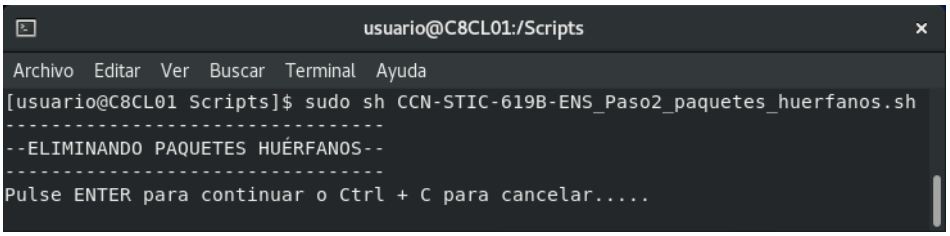
Paso	Descripción
19.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
20.	En la versión 8 de CentOS no se proporciona la herramienta gráfica de configuración de servicios "ntsysv" de forma nativa con la instalación "servidor con GUI", no obstante, puede instalarla de forma manual o mediante los medios proporcionados por el propio CentOS.  **Nota:** No es motivo de esta guía especificar las formas de instalación de la herramienta, sin embargo, se debe de tener en consideración que las fuentes de instalación de la misma sean fuentes oficiales y que la versión escogida sea la última recomendada por el fabricante.

Paso	Descripción
21.	Se procede a deshabilitar servicios y demonios innecesarios. Si ha instalado la herramienta “ntsysv” en el punto anterior continúe con el siguiente punto, en caso contrario siga desde el punto 25.
22.	Ejecute el siguiente comando en la terminal. **$ sudo ntsysv** 
23.	El funcionamiento de la herramienta es sencillo, los servicios con un asterisco serán los que estarán habilitados al inicio del sistema. Si quisiera deshabilitar algún servicio, basta con situarse encima del mismo con ayuda de los cursores del teclado y pulsar “**Espacio”.** Cuando haya finalizado pulse la tecla **“Tab”** (tabulador) una vez para seleccionar **“Aceptar”** y a continuación pulse “Enter”. Si por el contrario quisiera cancelar los cambios, pulse la tecla **“Tab”** dos veces para posicionarse encima del recuadro **“Cancelar”** y pulse “Enter”.
24.	Deshabilite todos los servicios innecesarios y mantenga los mínimos necesarios para el correcto funcionamiento del sistema.

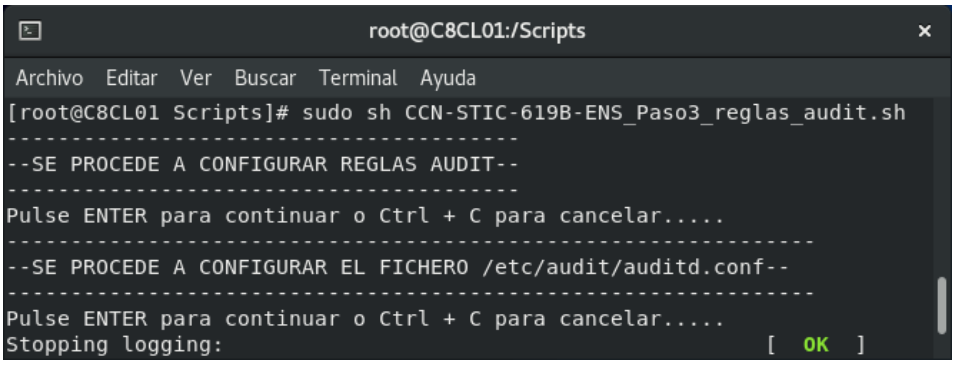
Paso	Descripción
25.	Si por necesidades de su organización no cabe la posibilidad de instalación de la herramienta “ntsysv”, deberá hacer uso de la terminal por medio de comandos de systemctl. Para revisar el estado del total de los servicios del sistema. Ejecute el siguiente comando. Introduzca la contraseña si se le solicita. **$ sudo systemctl list-unit-files --type=service**  **Nota:** Si necesita más información sobre la utilización de systemctl pude ver el siguiente enlace. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/managing-services-with-systemd_configuring-basic-system-settings

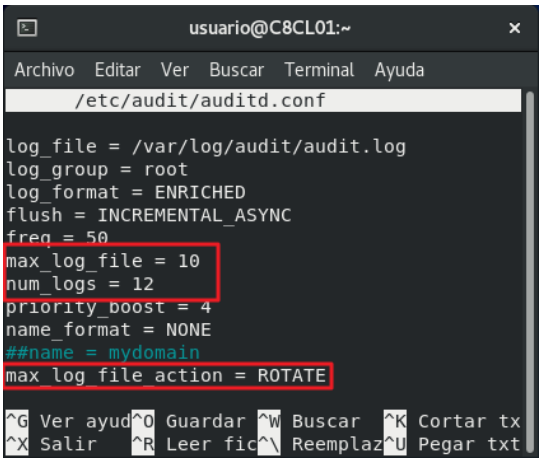
2.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

Paso	Descripción
26.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “**Terminal**”. Ejecute el comando “**cd /**” y pulse la tecla “Enter”.
27.	En la versión 8 de CentOS no se proporciona el conjunto de herramientas “yum-utils” de forma nativa con la instalación “servidor con GUI”, no obstante, puede instalarla de forma manual o mediante los medios proporcionados por el propio CentOS. El script que se ejecutará en el paso siguiente, comprobará e instalará si es necesario los paquetes requeridos. Compruebe que tiene correctamente configurado un repositorio oficial de CentOS o uno propio de su organización y acceso al mismo antes de continuar.
28.	Se procederá a eliminar los antiguos kernel, los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**

Paso	Descripción
29.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso2_paquetes_huerfanos.sh**  Pulse "Enter" para comenzar la ejecución del script. El script iniciará un proceso de desinstalación de dichos paquetes, para ello instalará la herramienta "yum-utils". No pulse ninguna tecla ni cierra la ventana hasta que finalice con un mensaje en pantalla de **"¡Listo!"**. **Nota:** Si el script detectara algún paquete candidato para su desinstalación, una vez finalice el proceso, se recomienda volver al punto 26 de este apartado para revisar los servicios y volver a ejecutar el script, para eliminar posibles paquetes huérfanos.

3. CONFIGURACIÓN DE REGISTROS DE ACTIVIDAD

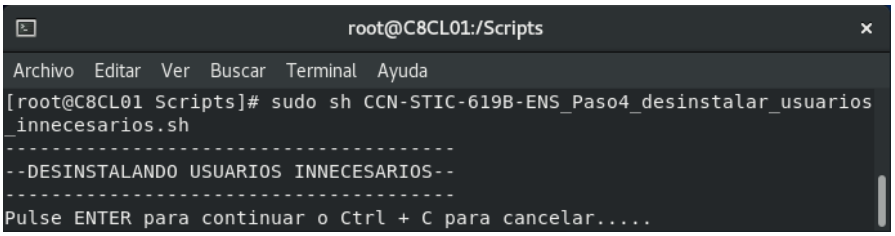
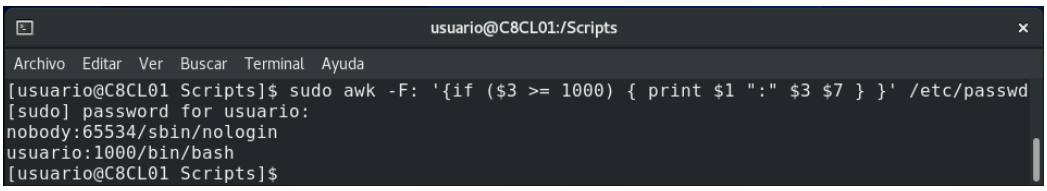
Paso	Descripción
30.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
31.	Se procede a configurar la herramienta Audit, se añadirán reglas para la correcta auditoría del sistema, así como la modificación de su fichero de configuración. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**
32.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso3_reglas_audit.sh** 

Paso	Descripción
33.	El script finalizará mostrando las reglas creadas. Si el sistema indicara lo contrario vuelva ejecute de nuevo el script. **Nota:** El script añade los parámetros necesarios al fichero de configuración **"/etc/audit/audit.conf"** para que se generen máximo 12 archivos de logs con una capacidad máxima por archivo de 10Mb, lo que crea un total de 120Mb. Cuando alcance el límite, los ficheros de logs rotarán gracias al parámetro **"max_log_file_action = ROTATE"**.
34.	Ajuste esta configuración con los parámetros necesarios para su organización. Para ello ejecute el siguiente comando. **$ sudo nano /etc/audit/auditd.conf**
35.	Modifique los parámetros marcados según las necesidades de su organización.  **Nota:** Para la modificación del fichero con el editor "nano" deberá navegar por el fichero mediante las flechas del teclado y modificar los datos eliminando o añadiendo las partes necesarias. Para guardar, pulse la combinación de teclas "Crtl + o" y luego "Enter" y para salir pulse la combinación de teclas "Crtl + x". Si requiere mas información sobre la utilización del editor "nano" diríjase a la siguiente URL: https://www.nano-editor.org/dist/v2.1/nano.html

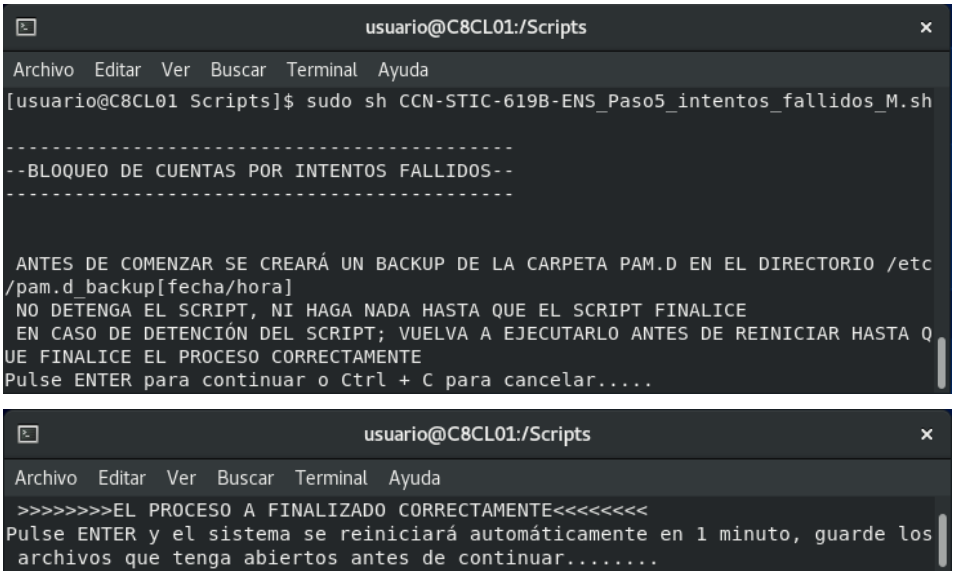
4. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

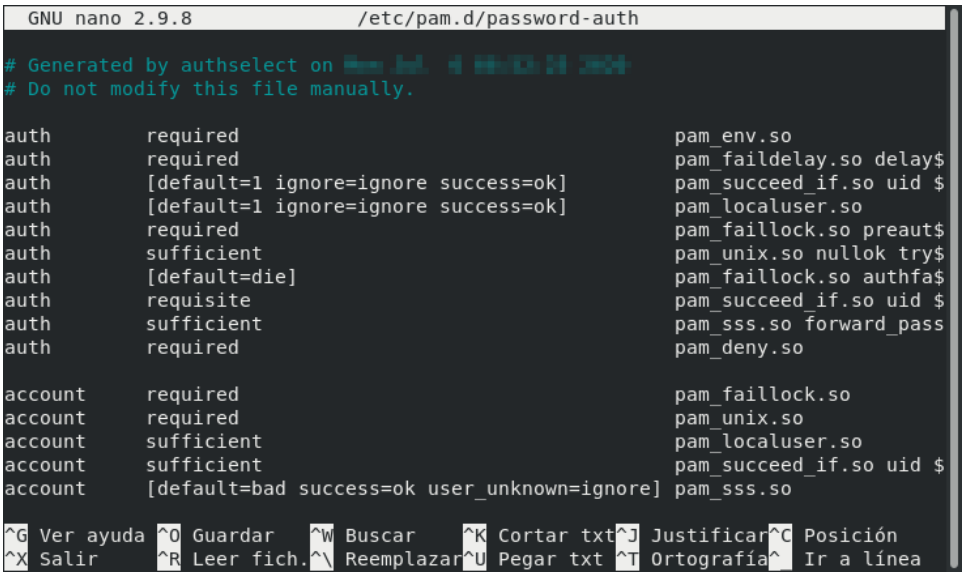
4.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

Paso	Descripción
36.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
37.	Se va a proceder a eliminar los usuarios creados por defecto en la instalación y que son innecesarios. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**

Paso	Descripción
38.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso4_desinstalar_usuarios_innecesarios.sh**  El script iniciará un proceso que deshabilitará los usuarios innecesarios, y corregirá las shells predeterminadas en caso de no ser las correctas. No pulse ninguna tecla ni cierre la ventana hasta que el proceso finalice. Ignore los mensajes de pantalla.
39.	Si ha detectado que en la actualidad está habilitado un usuario que ya no tiene necesidad de acceder al sistema puede usar el siguiente comando (**sin comillas**), siendo **NOMBREDELUSUARIO** el nombre del usuario candidato para su eliminación. **$ sudo userdel -r "NOMBREDELUSUARIO".**
40.	Ahora compruebe las "shells" predeterminadas de los usuarios con UID por encima del número 1000 (usuarios normales del sistema) Para ello ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd** Se mostrarán todos los usuarios y sus respectivas shells. Compruebe que todas las shells de usuario coinciden con "**/bin/bash**".  **Nota:** Como se puede observar puede aparecer el usuario nobody con uid:65534 y como excepción se deberá conservar su shell. Por defecto, los directorios compartidos NFS cambian el usuario root (superusuario) por el usuario nfsnobody, una cuenta de usuario sin privilegios. De esta forma, todos los archivos creados por root son propiedad del usuario nfsnobody, lo que previene la carga de programas con la configuración del bit setuid. En Centos 8 el usuario "nobody" sustituye a "nfsnobody" para los siguientes grupos y usuarios: - El par de usuarios nobody y grupos con el ID de 99. - El par de usuario nfsnobody y grupo con el ID de 65534, que también es el ID de desbordamiento predeterminado del núcleo. Este cambio reduce la confusión sobre los archivos que son propiedad de NFS nobody pero no tienen nada que ver con NFS.
41.	Cuando finalice todas las tareas reinicie el sistema.

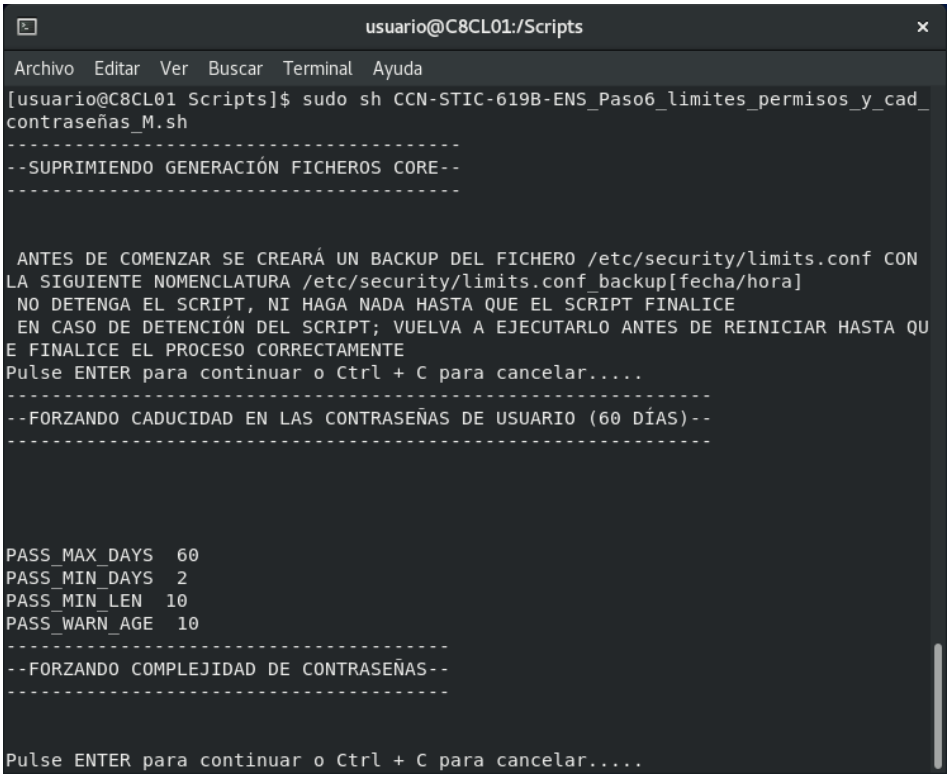
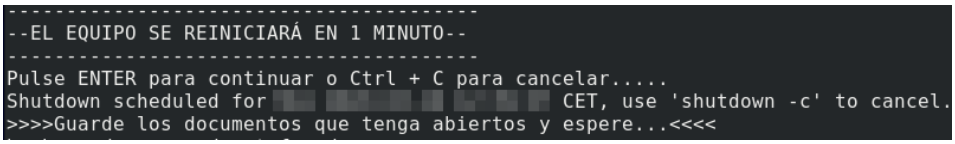
4.2. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS

Paso	Descripción
42.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
43.	Se procederá a configurar el bloqueo de cuentas por intentos fallidos, por medio del módulo "pam_faillock.so". Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente script. **$ sudo sh CCN-STIC-619B-ENS_Paso5_intentos_fallidos_M.sh**
44.	El script alertará de la creación de una copia de seguridad de la configuración de los ficheros incluidos en /etc/pam.d/. El script añadirá una configuración que cumpla con los mínimos requisitos de seguridad. Al finalizar el proceso el sistema se reiniciará para aplicar la configuración.  **Nota:** Si el script se detuviera o no terminara correctamente, deberá restaurar la copia de seguridad creada e iniciar el script de nuevo, por el contrario, es posible que el sistema no pueda iniciarse correctamente.

Paso	Descripción
45.	Si quisiera editar los ficheros con las necesidades de seguridad requeridos por su organización, ejecute los siguientes comandos. **$ sudo nano /etc/pam.d/password-auth** **$ sudo nano /etc/pam.d/ system-auth**  **Nota:** Hay que tener en consideración que el script aplica configuración sobre los ficheros por defecto de instalación. Por tanto, si existieran configuraciones previas a la ejecución del script, deberá adaptar éste o los ficheros a las necesidades específicas de su organización. No modifique estos ficheros de configuración si no conoce el funcionamiento de los módulos "pam.d", podría provocar que el sistema no iniciara correctamente.
46.	Si ha realizado modificaciones o ha detenido el reinicio automático, reinicie manualmente el sistema para que los cambios queden aplicados.

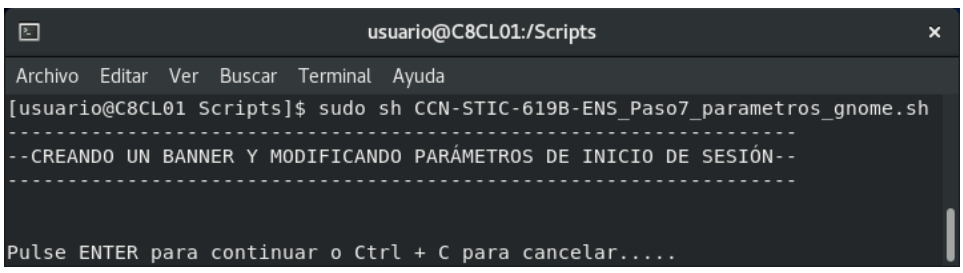
4.3. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

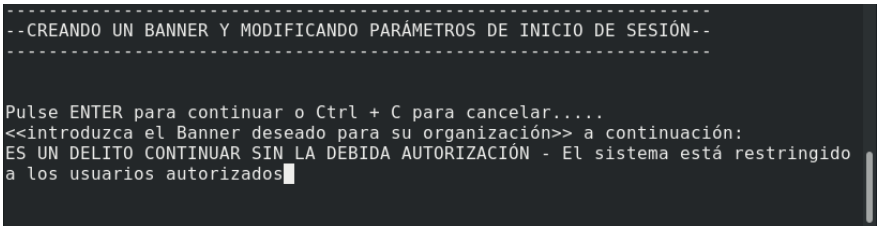
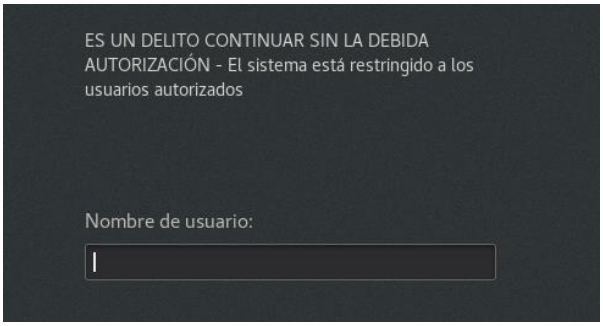
Paso	Descripción
47.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".

Paso	Descripción
48.	Antes de comenzar este paso, asegúrese de haber cerrado y guardado las aplicaciones y los documentos importantes. Se va a proceder a limitar los recursos disponibles para los usuarios, en particular limitar los "**volcados de núcleo** (core dumps)". Así mismo se forzará la caducidad de contraseñas para los nuevos usuarios y los ya existentes, la complejidad y los permisos en los directorios "/home" de cada usuario. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente script. **$ sudo sh CCN-STIC-619B-ENS_Paso6_limites_permisos_y_cad_contraseñas_M.sh**  Cuando finalice el script, saldrá un mensaje advirtiendo que el sistema se reiniciará en 1 minuto. Espere y cierre las aplicaciones que tenga abiertas. 

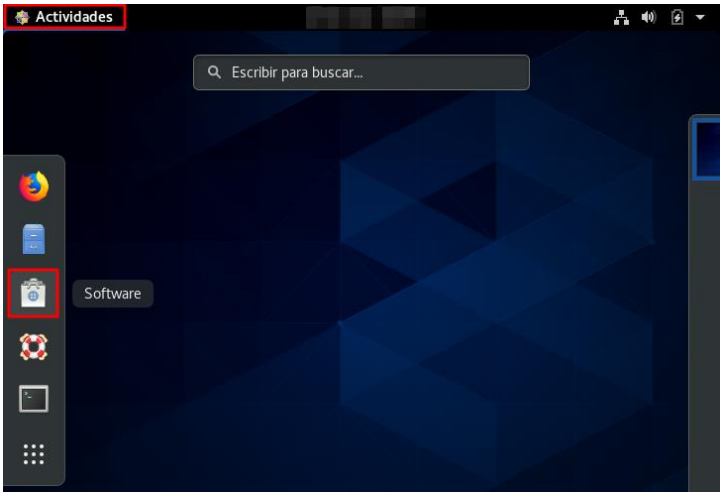
Paso	Descripción
49.	Cuando reinicie el sistema e inicie sesión, aparecerá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos. 
50.	Le pedirá la contraseña actual de nuevo y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.

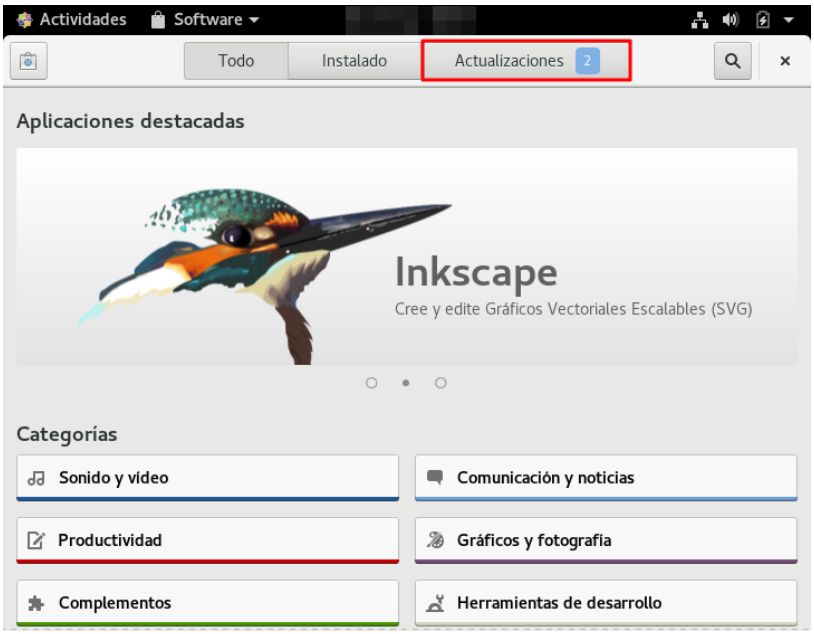
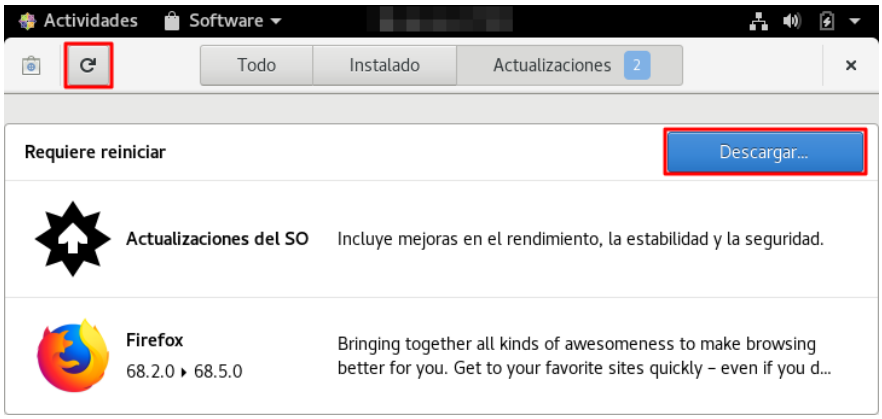
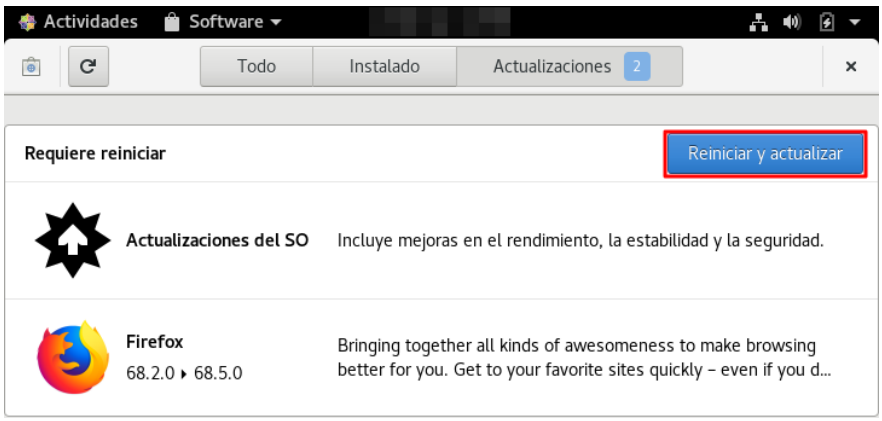
4.4. CONFIGURACIÓN SEGURA DE GNOME

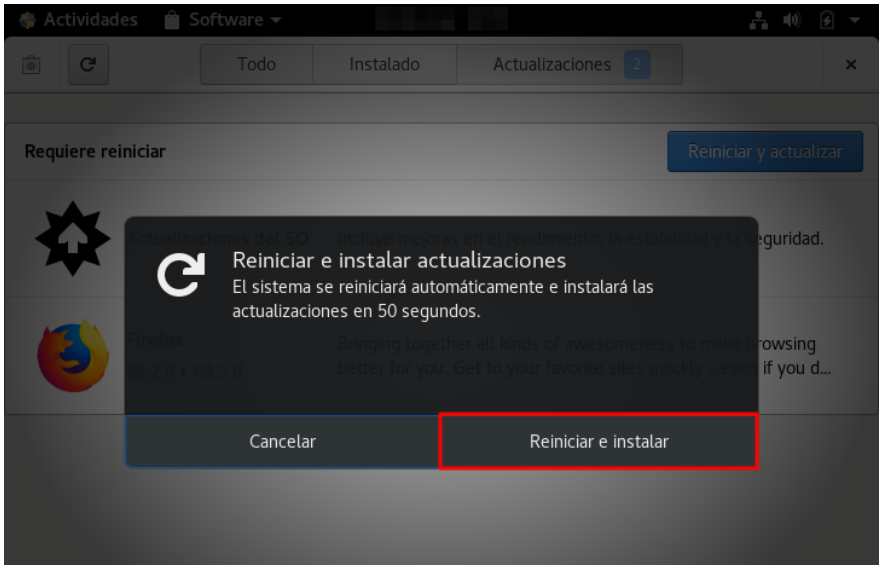
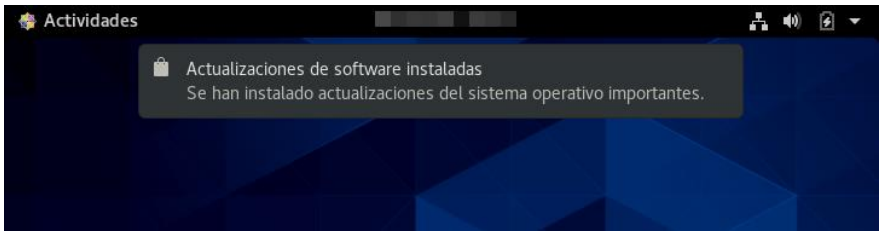
Paso	Descripción
51.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
52.	Se va a proceder a configurar parámetros de seguridad en el escritorio Gnome. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso7_parametros_gnome.sh** 

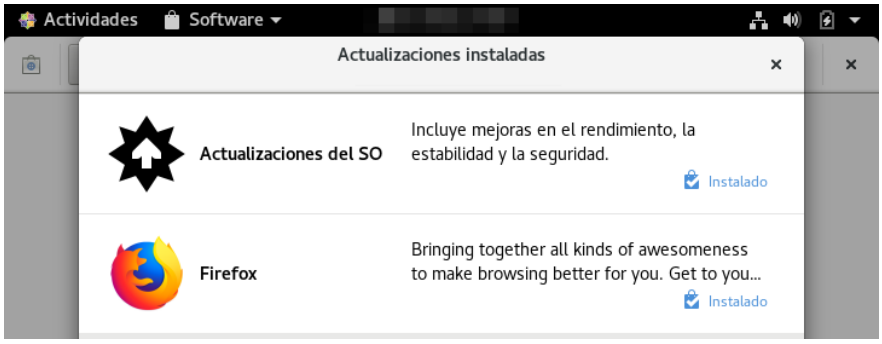
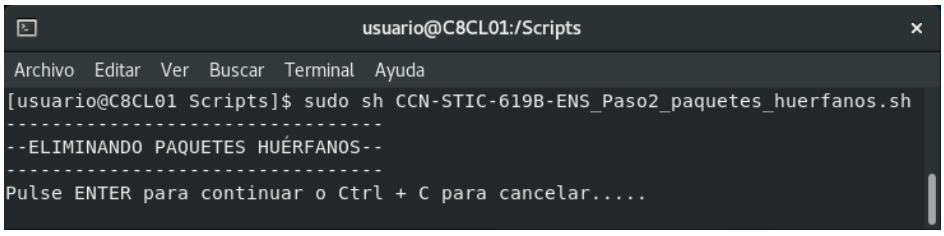
Paso	Descripción
53.	Introduzca el Banner deseado acorde con su organización. 
54.	El script iniciará un proceso que modificará la pantalla de inicio de CentOS 8 Linux para que aparezca un mensaje disuasorio (banner) al inicio y solicite usuario y contraseña. Así mismo se configurará un tiempo mínimo de bloqueo según requisitos de seguridad.  **Nota:** CentOS 8 Linux presenta mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

5. APLICACIÓN DE ACTUALIZACIONES

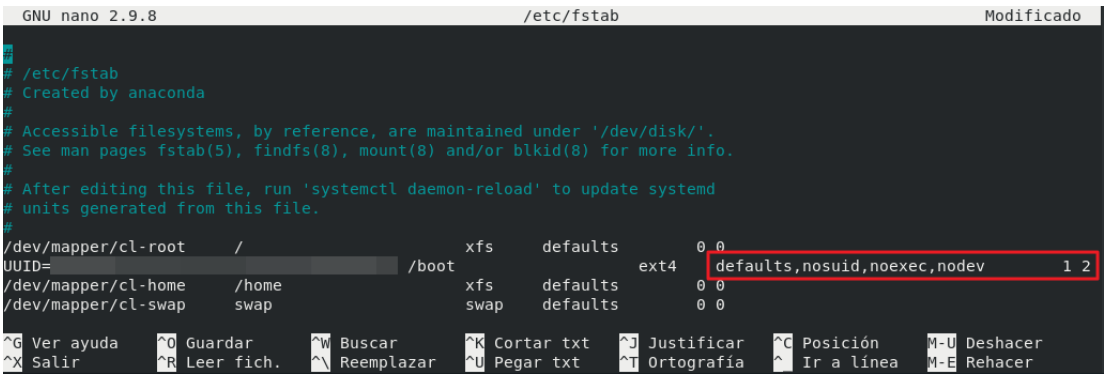
Paso	Descripción
55.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a “**Software**”. 

Paso	Descripción
56.	Una vez iniciada la aplicación, pulse sobre la pestaña “Actualizaciones”. 
57.	pulse sobre el botón de la flecha. ⟳ Comprobará si hay más actualizaciones; cuando finalice pulse en el botón “Descargar…”. 
58.	Cuando las actualizaciones se descarguen pulse “Reiniciar y Actualizar”- 

Paso	Descripción
59.	Confirme el reinicio en el botón 
60.	El sistema se reiniciará y comenzará a instalar las actualizaciones.  El proceso puede durar varios minutos, no presione ninguna tecla hasta que el proceso de actualización finalice.
61.	Cuando finalice, aparecerá la pantalla de inicio de CentOS 8. Inicie sesión y le saldrá un mensaje en el escritorio que le notificará las actualizaciones instaladas. 

Paso	Descripción
62.	Si presiona sobre el mensaje, aparecerán todas las aplicaciones que han sido actualizadas para su comprobación. 
63.	Cuando termine de revisar, cierre la ventana y su sistema estará actualizado. 
64.	Una vez finalizada la actualización, vuelva a ejecutar el script "CCN-STIC-619B-ENS_Paso2_paquetes_huerfanos.sh" del punto "2.2COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS". Para ello diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "Terminal". Ejecute el comando "**cd /**" y pulse la tecla "**Enter**". Diríjase a la carpeta "**/Scripts**" y ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso2_paquetes_huerfanos.sh**  El script iniciará un proceso de desinstalación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice con un mensaje en pantalla de "¡Listo!".
65.	Reinicie el sistema para finalizar el proceso.

6. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

Paso	Descripción
66.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
67.	Ejecute el siguiente comando e introduzca la contraseña si se le solicita. **$ sudo nano /etc/fstab**
68.	Edite el fichero de configuración con el editor de textos "nano", modificando los permisos de la partición "/boot" para que el resultado sea similar al de la imagen (defaults,nosuid,noexec,nodev 1 2).  **Nota:** Para la modificación del fichero con el editor "nano" deberá navegar por el fichero mediante las flechas del teclado y modificar los datos eliminando o añadiendo las partes necesarias. Para guardar, pulse la combinación de teclas "Crtl + o" y luego "Enter" y para salir pulse la combinación de teclas "Crtl + x". Si requiere mas información sobre la utilización del editor "nano" diríjase a la siguiente URL: https://www.nano-editor.org/dist/v2.1/nano.html
69.	Cuando finalice de editar, pulse la combinación de teclas "Crtl + o" y luego "Enter" para guardar y la combinación de teclas "Crtl + x" para salir. Elimine el directorio "/Scripts" y todo su contenido. **Nota:** Debe tener en consideración, que para realizar actualizaciones del kernel es posible que deba restablecer los valores de la partición "/boot" a defaults y posteriormente cuando la actualización finalice, revertirlos a los establecidos por esta guía.

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE CLIENTE CENTOS 8 PARA LA CATEGORÍA MEDIA

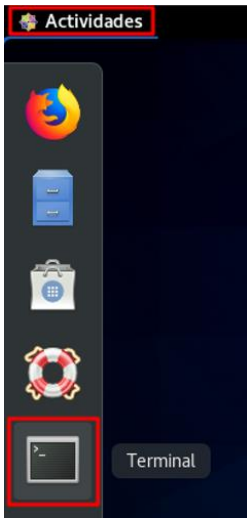
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.4.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES CENTOS 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

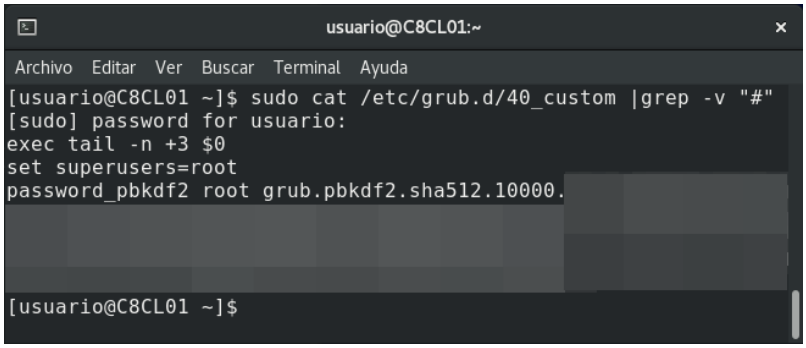
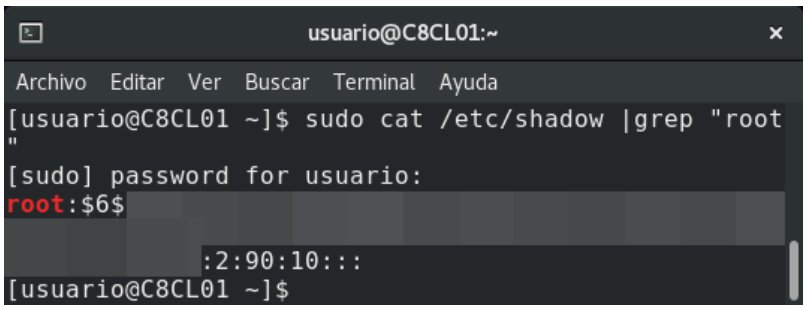
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes CentOS 8 independientes con implementación de seguridad en la categoría media del ENS.

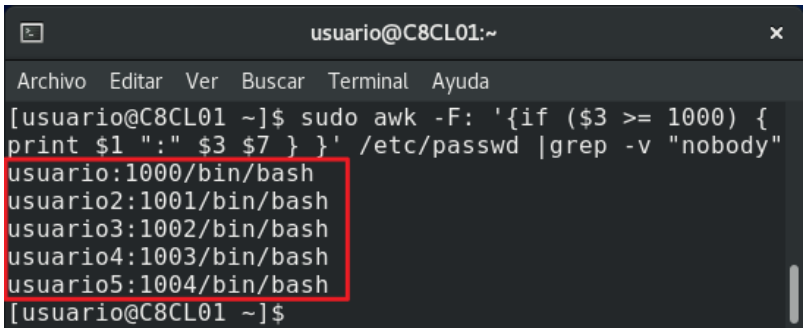
Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas que se utilizarán son las siguientes:

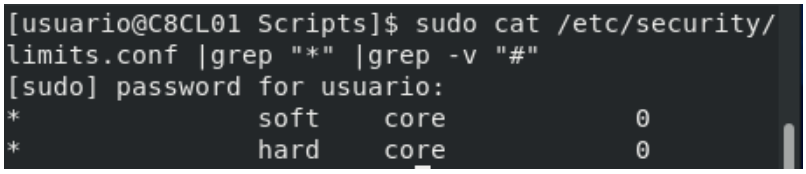
a) Terminal de Linux

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de root. Cree la carpeta "Scripts" en "/" y copie el contenido del nivel de seguridad "MEDIA" correspondiente al directorio "Scripts/ENS_MEDIA" asociado a esta guía en la ruta "/Scripts".
2. Inicie la Terminal de Linux.		Ejecute la "Terminal", para ello diríjase a la barra de tareas superior, pulse sobre "Actividades" y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen. 

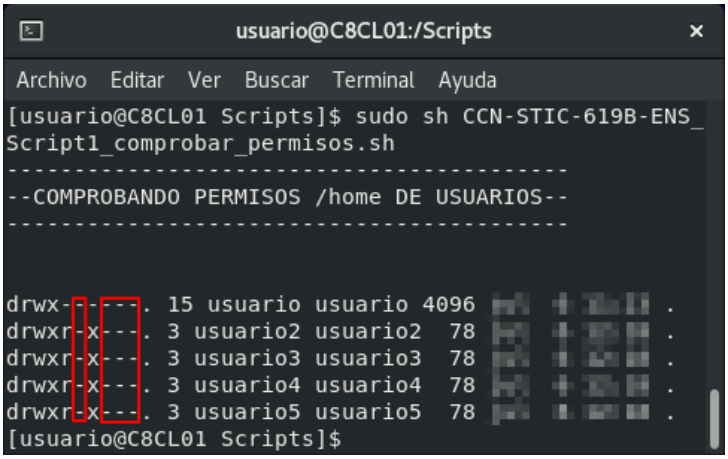
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que grub tiene contraseña configurada y root como único usuario de modificación.		En la "Terminal" ejecute el siguiente comando. **$ sudo cat /etc/grub.d/40_custom |grep -v "#"**  **Nota:** Fíjese en las letras y números que están situadas después de "password_pbkdf2 root grub.pbkdf2.sha512.". Pueden ser diferentes dependiendo del usuario, ya que se trata de un hash generado a partir de la contraseña dada al ejecutar el script.
4. Contraseña de root segura.		Abra la Terminal y ejecute el siguiente comando. **$ sudo cat /etc/shadow |grep "root"**  Fíjese que el inicio del hash de la contraseña de "root" comienza por "**6**", esto le indicará en qué tipo de hash está la contraseña de "root", en este caso es SHA-512, (Secure Hash Algorithm) y por lo tanto tiene 86 caracteres en total. Fíjese adicionalmente en que el final de la configuración termina por "**:2:90:10:::**" indicando que se ha configurado correctamente la caducidad de la cuenta.
5. Búsqueda de usuarios sin contraseña.		Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1** **Nota:** Si la configuración es correcta, no deberá mostrar ningún resultado la salida del comando.

Comprobación	OK/NOK	Cómo hacerlo
6. Búsqueda de usuarios con UID 0.		Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1 |grep -v "root"** **Nota:** Si la configuración es correcta, no deberá mostrar ningún resultado la salida del comando.
7. Servicios innecesarios		Abra la Terminal y ejecute el siguiente comando. **$ sudo systemctl list-unit-files --type=service**  UNIT FILE STATE accounts-daemon.service enabled alsa-restore.service static alsa-state.service static anaconda-direct.service static anaconda-nm-config.service static anaconda-noshell.service static anaconda-pre.service static anaconda-shell@.service static anaconda-sshd.service static anaconda-tmux@.service static anaconda.service static arp-ethers.service disabled atd.service enabled auditd.service enabled autovt@.service enabled avahi-daemon.service enabled lines 1-17 Revise que los servicios activos al iniciar el sistema son los correctos para su organización.
8. Comprobación de usuarios y shells predeterminadas.		Ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $7 } }' /etc/passwd \|grep -v "nobody"**  usuario@C8CL01:~ Archivo Editar Ver Buscar Terminal Ayuda [usuario@C8CL01 ~]$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd \|grep -v "nobody" usuario:1000/bin/bash usuario2:1001/bin/bash usuario3:1002/bin/bash usuario4:1003/bin/bash usuario5:1004/bin/bash [usuario@C8CL01 ~]$ Compruebe si los usuarios que se muestran son los más adecuados para su organización y que están correctas las shells predeterminadas.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Comprobación de registros de actividad</td><td></td><td>Primero se va a comprobar el fichero de configuración, con los parámetros definidos por esta guía.
Ejecute los siguientes comandos.
$ sudo cat /etc/audit/auditd.conf |grep "max_log_file ="
$ sudo cat /etc/audit/auditd.conf |grep "num_logs ="
$ sudo cat /etc/audit/auditd.conf |grep "max_log_file_action ="
$ sudo ls -laR /etc/audit/auditd.conf | cut -d' ' -f1
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>max_log_file</td><td>10</td><td></td></tr>
<tr><td>num_logs</td><td>12</td><td></td></tr>
<tr><td>max_log_file_action</td><td>ROTATE</td><td></td></tr>
<tr><td>/etc/audit/auditd.conf</td><td>-rw-r-----.</td><td></td></tr>
</table></td></tr>
<tr><td>10. Parámetros de bloqueo de cuenta.</td><td></td><td>Se va a comprobar los ficheros de configuración, con los parámetros definidos por esta guía.
– /etc/pam.d/password-auth
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/password-auth |grep "auth" |grep "pam_faillock.so" |grep "deny="
$ sudo cat /etc/pam.d/password-auth |grep "auth" |grep "unlock_time"
$ sudo cat /etc/pam.d/password-auth |grep "account" |grep "pam_faillock.so"
$ sudo cat /etc/pam.d/password-auth |grep "pam_pwhistory" |grep "remember"
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>deny</td><td>8</td><td></td></tr>
<tr><td>unlock_time</td><td>3600</td><td></td></tr>
<tr><td>pam_faillock.so</td><td>Existe</td><td></td></tr>
<tr><td>remember</td><td>25</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>– /etc/pam.d/system-auth
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/system-auth |grep "auth" |grep "pam_faillock.so" |grep "deny="
$ sudo cat /etc/pam.d/system-auth |grep "auth" |grep "unlock_time"
$ sudo cat /etc/pam.d/system-auth |grep "account" |grep "pam_faillock.so"
$ sudo cat /etc/pam.d/system-auth |grep "pam_pwhistory" |grep "remember"</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>deny</td><td>8</td><td></td></tr>
<tr><td>unlock_time</td><td>3600</td><td></td></tr>
<tr><td>pam_faillock.so</td><td>Existe</td><td></td></tr>
<tr><td>remember</td><td>25</td><td></td></tr>
</table></td></tr>
<tr><td>11. Configuración de los volcados de núcleo (core dumps)</td><td></td><td>Ejecute el siguiente comando.
$ sudo cat /etc/security/limits.conf |grep "*" |grep -v "#"
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Soft core</td><td>0</td><td></td></tr>
<tr><td>Hard core</td><td>0</td><td></td></tr>
</table></td></tr>
<tr><td>12. Banner disuasorio.</td><td></td><td>Ejecute los siguientes comandos.
$ cat /etc/issue
$ cat /etc/issue.net
$ cat /etc/motd
Compruebe si se han configurado bien los mensajes disuasorios (banners).</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>13. Verifique la directiva de caducidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MAX_DAYS"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MIN_DAYS"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MIN_LEN"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_WARN_AGE"
$ sudo cat /etc/login.defs |grep "UMASK"
$ sudo cat /etc/login.defs |grep "ENCRYPT_METHOD"
Compruebe si se han configurado bien los siguientes valores.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>PASS_MAX_DAYS</td><td>60</td><td></td></tr>
<tr><td>PASS_MIN_DAYS</td><td>2</td><td></td></tr>
<tr><td>PASS_MIN_LEN</td><td>10</td><td></td></tr>
<tr><td>PASS_WARN_AGE</td><td>10</td><td></td></tr>
<tr><td>UMASK</td><td>027</td><td></td></tr>
<tr><td>ENCRYPT_METHOD</td><td>SHA512</td><td></td></tr>
</table></td></tr>
<tr><td>14. Verifique la directiva de complejidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/security/pwquality.conf |grep "minlen ="
$ sudo cat /etc/security/pwquality.conf |grep "dcredit ="
$ sudo cat /etc/security/pwquality.conf |grep "ucredit ="
$ sudo cat /etc/security/pwquality.conf |grep "lcredit ="
Compruebe si se han configurado bien los siguientes valores.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>minlen</td><td>10</td><td></td></tr>
<tr><td>dcredit</td><td>-1</td><td></td></tr>
<tr><td>ucredit</td><td>-1</td><td></td></tr>
<tr><td>lcredit</td><td>-1</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>Se va a proceder a revisar los permisos de la ruta “/home” de casa usuario del sistema.
Para ello diríjase a la carpeta “Scripts”.
$ cd /Scripts
Ejecute el siguiente comando.
$ sudo sh CCN-STIC-619B-ENS_Script1_comprobar_permisos.sh
El script mostrará los permisos de las carpetas “/home” y se debe comprobar que coincidan las columnas marcadas se encuentren vacías.
 
</td></tr>
<tr><td>15.Configuración de Gnome</td><td></td><td>Se va a proceder a revisar los parámetros de configuración de Gnome.
Para ello ejecute los siguientes comandos.
$ cat /etc/dconf/db/gdm.d/01-banner-message
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>banner-message-enable</td><td>true</td><td></td></tr>
<tr><td>banner-message-text</td><td>“Texto elegido”</td><td></td></tr>
</table>
$ cat /etc/dconf/db/gdm.d/00-login-screen |grep "disable-user-list"
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>disable-user-list</td><td>true</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>

```
$ cat /etc/dconf/db/local.d/00-screensaver |grep "idle-delay=uint32"
$ cat /etc/dconf/db/local.d/00-screensaver |grep "lock-enabled"
$ cat /etc/dconf/db/local.d/00-screensaver |grep "lock-delay=uint32"
```

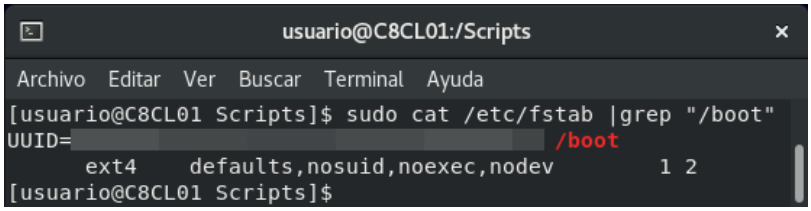
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>idle-delay=uint32</td><td>600</td><td></td></tr>
<tr><td>lock-enabled</td><td>true</td><td></td></tr>
<tr><td>lock-delay=uint32</td><td>0</td><td></td></tr>
</table>

```
$ cat /etc/dconf/db/local.d/03-privacy |grep "hide-identity"
$ cat /etc/dconf/db/local.d/03-privacy |grep "old-files-age"
$ cat /etc/dconf/db/local.d/03-privacy |grep "remember-recent-files"
$ cat /etc/dconf/db/local.d/03-privacy |grep "remove-old-temp-files"
```

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>hide-identity</td><td>true</td><td></td></tr>
<tr><td>old-files-age</td><td>0</td><td></td></tr>
<tr><td>remember-recent-files</td><td>false</td><td></td></tr>
<tr><td>remove-old-temp-files</td><td>true</td><td></td></tr>
</table>

</td></tr>
<tr><td>16. Permisos partición de inicio.</td><td></td><td>Compruebe que se han guardado los permisos en el fichero de configuración.

```
$ sudo cat /etc/fstab |grep "/boot"
```



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

ANEXO A.5. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.5.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES CENTOS 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 empleen clientes CentOS 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 aplicando seguridad cumpla con los requisitos para una red clasificada con grado de clasificación Difusión Limitada. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría alta o difusión limitada, deberá realizar las implementaciones según se referencian en el presente anexo.

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

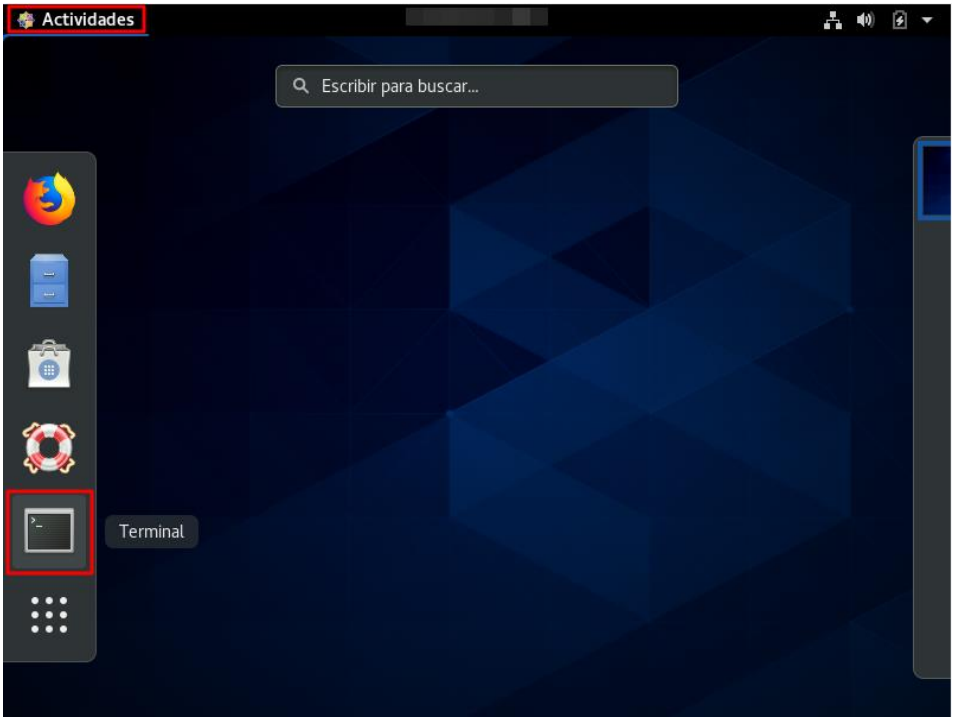
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Los pasos que se describen a continuación se realizarán en todos aquellos clientes CentOS 8, independientes a un dominio, que implementen servicios o información de categoría alta – DL y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

1. CONFIGURACIÓN SEGURA DEL ARRANQUE DEL SISTEMA

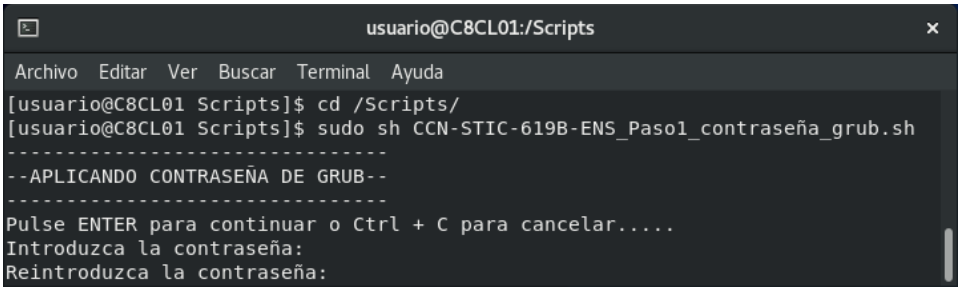
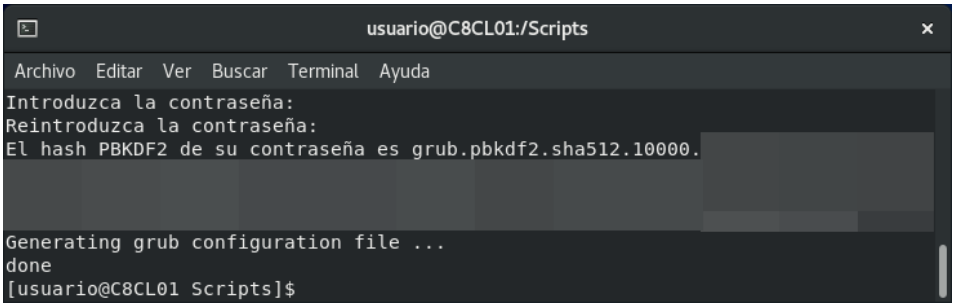
Antes de comenzar se tiene en cuenta que ha realizado los siguientes puntos.

Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Cree la carpeta “**Scripts**” en “**/**” y copie el contenido de la categoría de seguridad “ALTA-DL” correspondiente al directorio “Scripts/ENS_ALTA_DL” asociado a esta guía en la ruta “**/Scripts**”.

Paso	Descripción
4.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen. 
5.	Ejecute el comando “**cd /**” y pulse la tecla “Enter”.

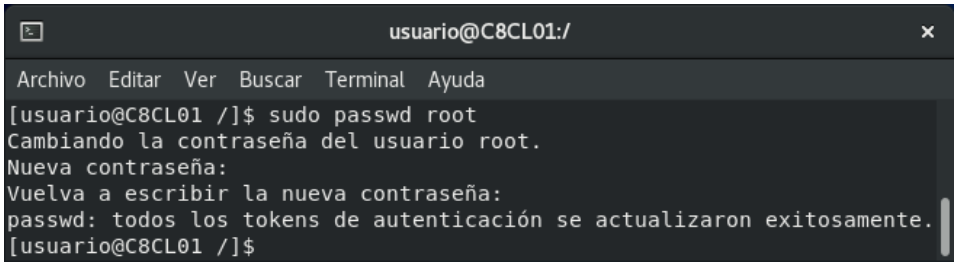
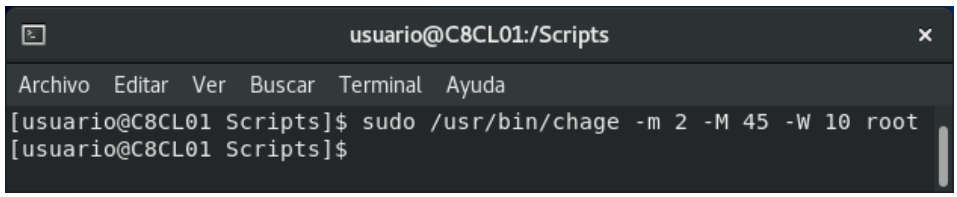
1.1. CONTRASEÑA DE GRUB

Paso	Descripción
6.	Se procede a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**

Paso	Descripción
7.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso1_contraseña_grub.sh** Pulse "Enter" para continuar. Introduzca la contraseña deseada.  **Nota**: Se generará automáticamente un hash con la contraseña elegida, ese hash no es necesario guardarlo, puesto que ya se ha copiado al fichero de grub. Es importante fijarse en que la última salida por pantalla sea un "done".  **Nota:** Si se introduce mal la contraseña y las contraseñas no coinciden, no se generará el hash, pero la configuración se exportará vacía al fichero de configuración de grub. Si sucede esto, repita el paso 6 desde el inicio antes de pasar al siguiente punto. Por defecto, el script configura el usuario "root" para iniciar la configuración de grub. Si por requisitos de su organización debe modificar el mismo, deberá adaptar el script a sus necesidades.
8.	No cierre la terminal entre pasos hasta que se le indique, para poder continuar con el proceso. A continuación, introduzca el siguiente comando y pulse "Enter". **$ clear** **Nota:** Deberá ejecutar este comando cuando requiera "limpiar" la "Terminal".

1.2. CONTRASEÑA SEGURA DE ROOT

Paso	Descripción
9.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
10.	Ejecute el siguiente comando. **$ sudo passwd root**

Paso	Descripción
11.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se mostrará en pantalla el siguiente comentario "Cambiando la contraseña del usuario root". Se pedirá la nueva contraseña y la confirmación de la misma. 
12.	Cuando el proceso haya terminado se mostrará el siguiente mensaje. "**passwd: todos los tokens de autenticación se actualizaron exitosamente**." Si no muestra ese mensaje, vuelva al paso 8 y repita la operación.
13.	Una vez actualizada la contraseña deberá adaptar la caducidad de la cuenta a los parámetros se seguridad requeridos, para ello ejecute el siguiente comando: **$ sudo /usr/bin/chage -m 2 -M 45 -W 10 root** 

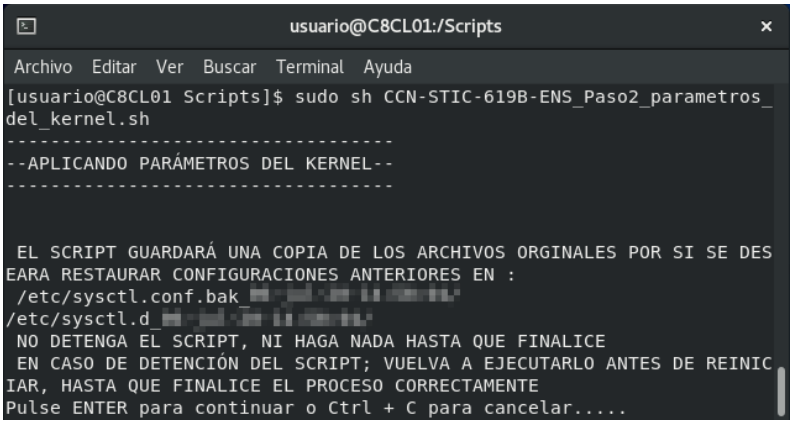
1.3. BÚSQUEDA DE CUENTAS SIN CONTRASEÑA

Paso	Descripción
14.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
15.	Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1**
16.	El comando no debería devolver ningún resultado por pantalla, si por el contrario, sale algún resultado, significaría que esos usuarios no tienen contraseña configurada y deben ser eliminados. **Nota:** Si no conoce el proceso de eliminación de usuarios vaya al punto "5.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS"

1.4. USUARIOS CON UID 0 QUE NO SEAN ROOT

Paso	Descripción
17.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
18.	Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1**
19.	El comando deberá devolver "root" como resultado por pantalla, si por el contrario, sale algún resultado que no sea root, significará que ese/esos usuario/s tienen "UID" 0 y por ende permisos demasiado elevados y deben ser eliminados. **Nota:** Si no conoce el proceso de eliminación de usuarios vaya al punto "5.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

2. FORTIFICACIÓN DE KERNEL

Paso	Descripción
20.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
21.	Se va a proceder a modificar parámetros del kernel, para ello se añadirán ciertas líneas comentadas **"#"** al fichero "/etc/sysctl.conf", además de la configuración predeterminada, para facilitar la adaptación a las necesidades de su organización.
22.	Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso2_parámetros_del_kernel.sh**
23.	El script alertará de la creación de una copia de seguridad del fichero "/etc/sysctl.conf" y de la carpeta "/etc/sysctl.d/" con una marca de tiempo, ya que el script añadirá una configuración que cumpla con los mínimos de seguridad. 

Paso	Descripción

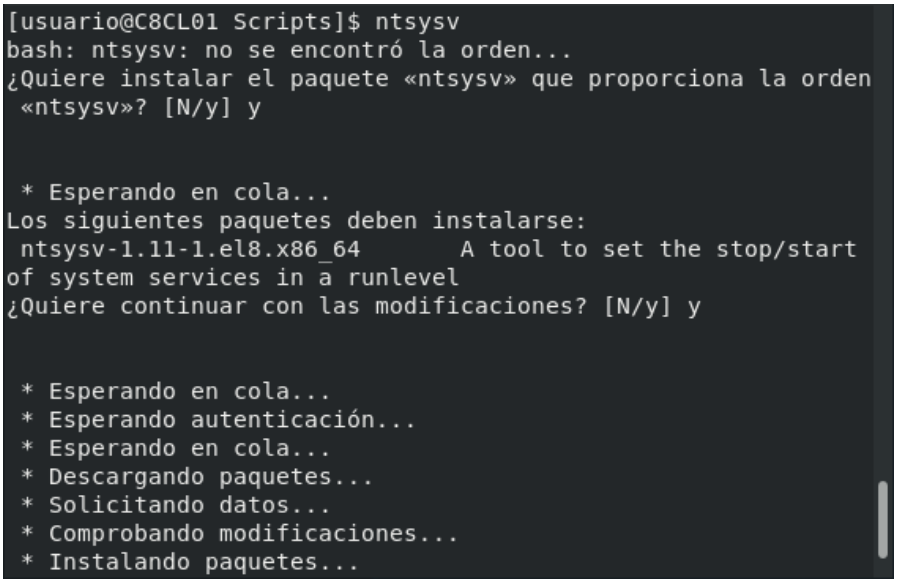
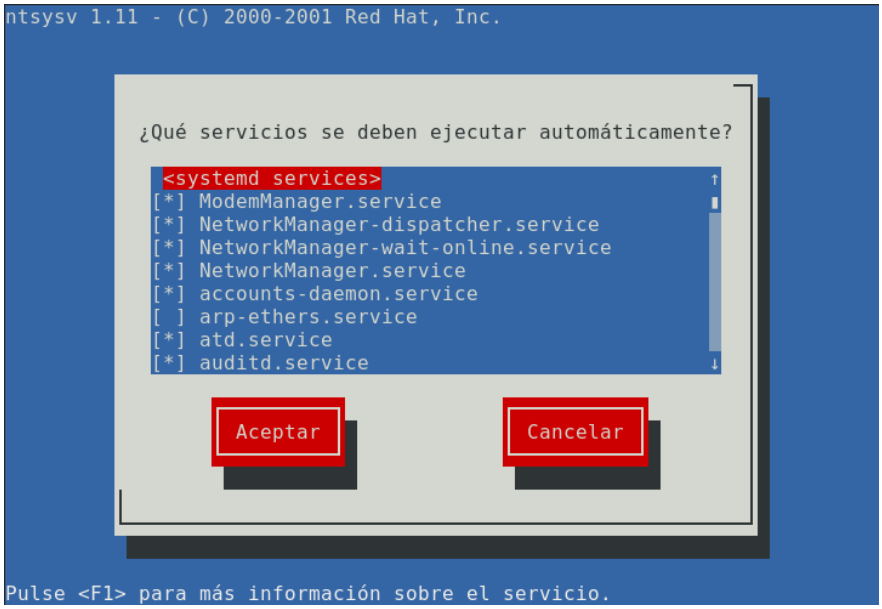
24.	Cuando la configuración predeterminada finalice, pulse “Enter” y se abrirá el fichero de configuración.
	
	`>>>>>>>>EL PROCESO A FINALIZADO<<<<<<<<`
	`Se mostrará el fichero /etc/sysctl.conf para su revisión pulse para continuar........`

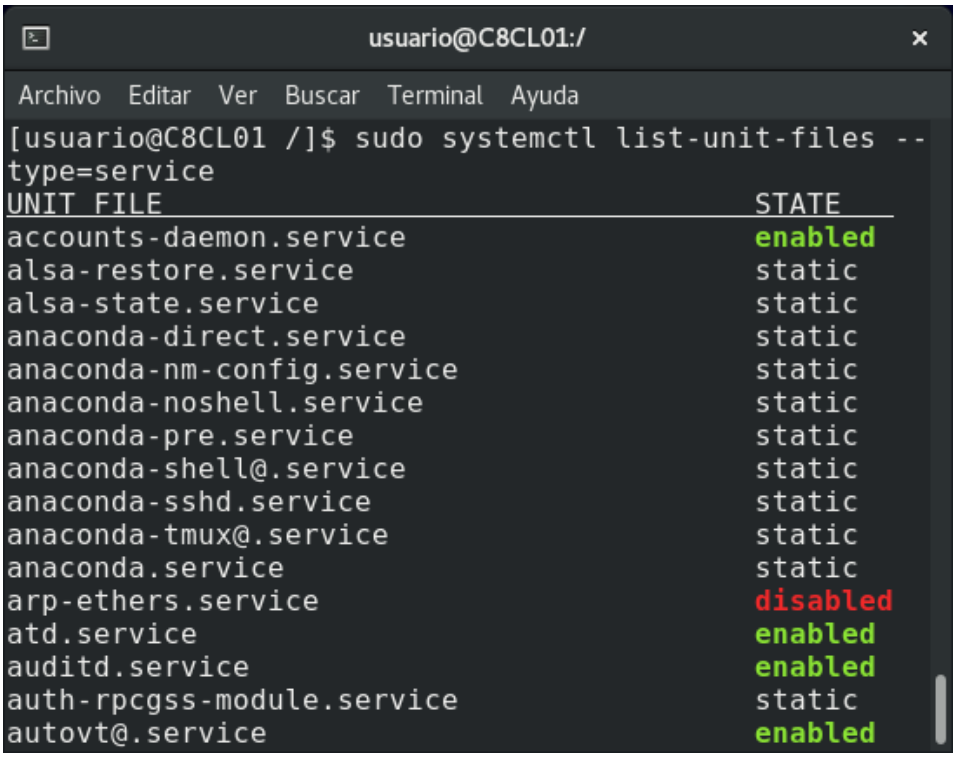
25.	Se puede observar que hay ciertos parámetros que no están actuando. Habilite, deshabilite o añada según las necesidades de su organización.
	
	usuario@C8CL01:/Scripts
	Archivo Editar Ver Buscar Terminal Ayuda
	`net.ipv4.conf.default.secure_redirects = 0`
	`net.ipv4.conf.all.secure_redirects = 0`
	`net.ipv4.conf.all.accept_source_route = 0`
	`net.ipv4.conf.default.accept_source_route = 0`
	`net.ipv4.conf.all.log_martians = 1`
	`net.ipv4.conf.default.log_martians = 1`
	`net.ipv4.icmp_ignore_bogus_error_responses = 1`
	`net.ipv4.icmp_echo_ignore_broadcasts = 1`
	`net.ipv4.tcp_syncookies = 1`
	`fs.suid_dumpable = 0`
	`net.ipv6.conf.default.accept_source_route = 0`
	`net.ipv6.conf.all.accept_source_route = 0`
	`net.ipv6.conf.all.accept_redirects = 0`
	`net.ipv6.conf.default.accept_ra = 0`
	`net.ipv6.conf.all.accept_ra = 0`
	`net.ipv6.conf.default.accept_redirects = 0`
	`# PARÁMETROS REVISABLES`
	`# ----------------------`
	
	Cuando llegue al final del documento el script informará que el equipo se va a reiniciar. Guarde los documentos que tenga abiertos y pulse “Enter” para reiniciar.

3. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

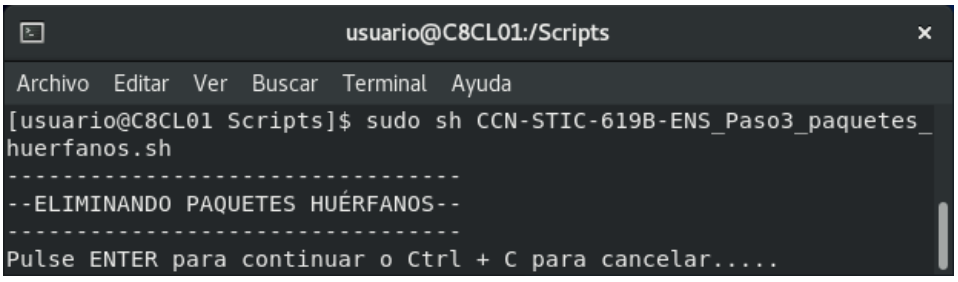
3.1. LIMITACIÓN DE SERVICIOS Y DEMONIOS

Paso	Descripción
26.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “**Terminal**”. Ejecute el comando “**cd /**” y pulse la tecla “Enter”.

Paso	Descripción
27.	En la versión 8 de CentOS no se proporciona la herramienta gráfica de configuración de servicios “ntsysv” de forma nativa con la instalación “servidor con GUI”, no obstante, puede instalarla de forma manual o mediante los medios proporcionados por el propio CentOS.  **Nota:** No es motivo de esta guía especificar las formas de instalación de la herramienta, sin embargo, se debe de tener en consideración que las fuentes de instalación de la misma sean fuentes oficiales y que la versión escogida sea la última recomendada por el fabricante.
28.	Se procede a deshabilitar servicios y demonios innecesarios. Si ha instalado la herramienta “ntsysv” en el punto anterior continúe con el siguiente punto, en caso contrario siga desde el punto 25.
29.	Ejecute el siguiente comando en la terminal. **$ sudo ntsysv** 

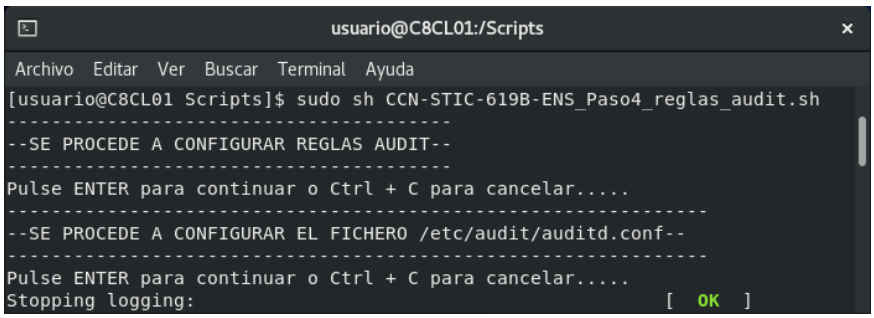
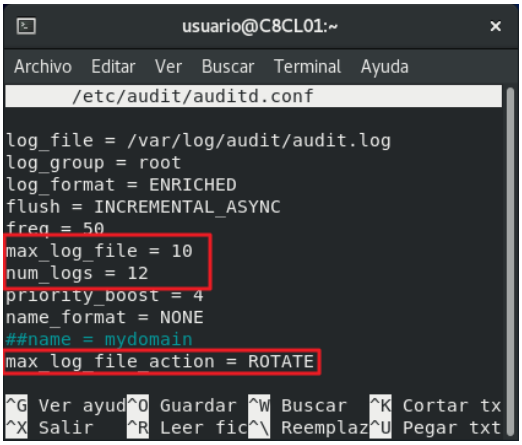
Paso	Descripción
30.	El funcionamiento de la herramienta es sencillo, los servicios con un asterisco serán los que estarán habilitados al inicio del sistema. Si quisiera deshabilitar algún servicio, basta con situarse encima del mismo con ayuda de los cursores del teclado y pulsar "**Espacio".** Cuando haya finalizado pulse la tecla **"Tab"** (tabulador) una vez para seleccionar **"Aceptar"** y a continuación pulse "Enter". Si por el contrario quisiera cancelar los cambios, pulse la tecla **"Tab"** dos veces para posicionarse encima del recuadro **"Cancelar"** y pulse "Enter".
31.	Deshabilite todos los servicios innecesarios y mantenga los mínimos necesarios para el correcto funcionamiento del sistema.
32.	Si por necesidades de su organización no cabe la posibilidad de instalación de la herramienta "ntsysv", deberá hacer uso de la terminal por medio de comandos de systemctl. Para revisar el estado del total de los servicios del sistema. Ejecute el siguiente comando. Introduzca la contraseña si se le solicita. **$ sudo systemctl list-unit-files --type=service**  **Nota:** Si necesita más información sobre la utilización de systemctl pude ver el siguiente enlace. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/managing-services-with-systemd_configuring-basic-system-settings

3.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

Paso	Descripción
33.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
34.	En la versión 8 de CentOS no se proporciona el conjunto de herramientas "yum-utils" de forma nativa con la instalación "servidor con GUI", no obstante, puede instalarla de forma manual o mediante los medios proporcionados por el propio CentOS. El script que se ejecutará en el paso siguiente, comprobará e instalará si es necesario los paquetes requeridos. Compruebe que tiene correctamente configurado un repositorio oficial de CentOS o uno propio de su organización y acceso al mismo antes de continuar.
35.	Se procederá a eliminar los antiguos kernel, los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso3_paquetes_huerfanos.sh**  Pulse "Enter" para comenzar la ejecución del script. El script iniciará un proceso de desinstalación de dichos paquetes, para ello instalará la herramienta "yum-utils" . No pulse ninguna tecla ni cierra la ventana hasta que finalice con un mensaje en pantalla de **"¡Listo!"**. **Nota:** Si el script detectara algún paquete candidato para su desinstalación, una vez finalice el proceso, se recomienda volver al punto 31 de este apartado para revisar los servicios y volver a ejecutar el script, para eliminar posibles paquetes huérfanos.

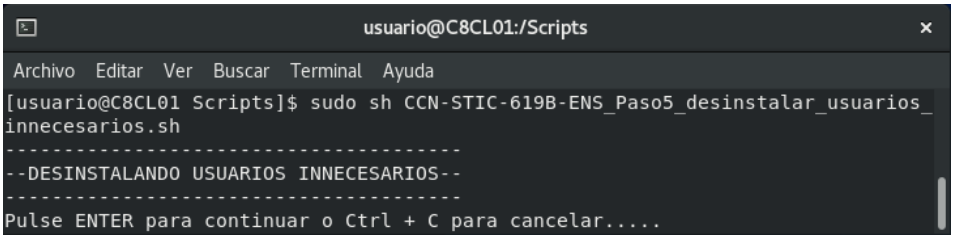
4. CONFIGURACIÓN Y PROTECCIÓN DE REGISTROS DE ACTIVIDAD

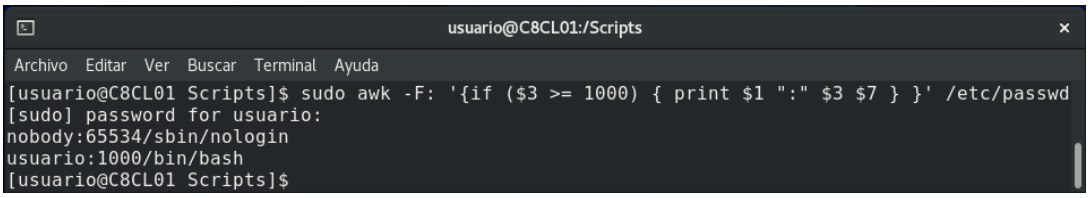
Paso	Descripción
36.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".

Paso	Descripción
37.	Se procede a configurar la herramienta Audit, se añadirán reglas para la correcta auditoría del sistema, así como la modificación de su fichero de configuración. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso4_reglas_audit.sh**  El script finalizará mostrando las reglas creadas. Si el sistema indicara lo contrario vuelva ejecute de nuevo el script. **Nota:** El script añade los parámetros necesarios al fichero de configuración **"/etc/audit/audit.conf"** para que se generen máximo 12 archivos de logs con una capacidad máxima por archivo de 10Mb, lo que crea un total de 120Mb. Cuando alcance el límite, los ficheros de logs rotarán gracias al parámetro **"max_log_file_action = ROTATE"**.
38.	Ajuste esta configuración con los parámetros necesarios para su organización. Para ello ejecute el siguiente comando. **$ sudo nano /etc/audit/auditd.conf**
39.	Modifique los parámetros marcados según las necesidades de su organización.  **Nota:** Para la modificación del fichero con el editor "nano" deberá navegar por el fichero mediante las flechas del teclado y modificar los datos eliminando o añadiendo las partes necesarias. Para guardar, pulse la combinación de teclas "Crtl + o" y luego "Enter" y para salir pulse la combinación de teclas "Crtl + x". Si requiere mas información sobre la utilización del editor "nano" diríjase a la siguiente URL: https://www.nano-editor.org/dist/v2.1/nano.html

5. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

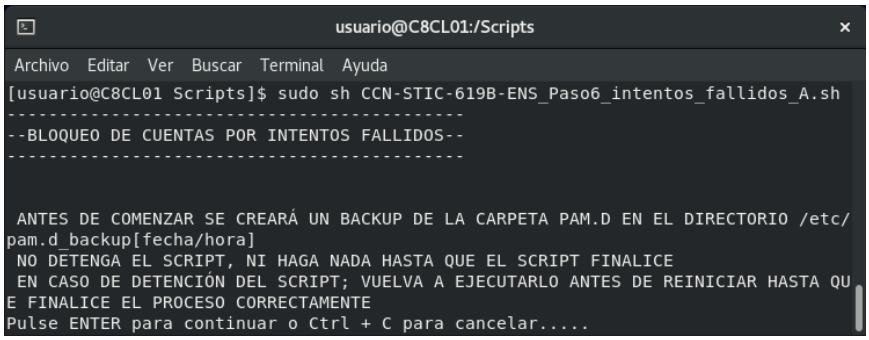
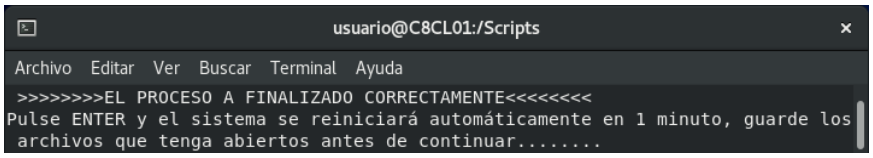
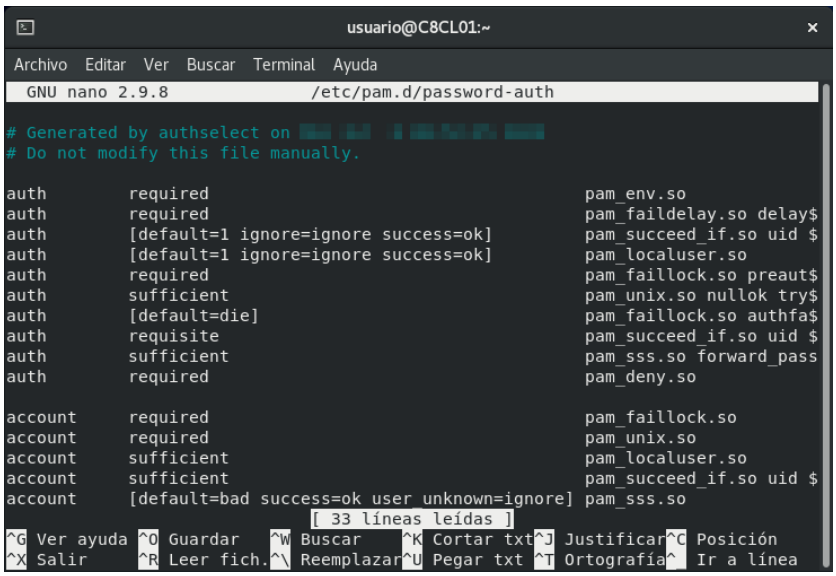
5.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

Paso	Descripción
40.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
41.	Se va a proceder a eliminar los usuarios creados por defecto en la instalación y que son innecesarios. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso5_desinstalar_usuarios_innecesarios.sh**  El script iniciará un proceso que deshabilitará los usuarios innecesarios, y corregirá las shells predeterminadas en caso de no ser las correctas. No pulse ninguna tecla ni cierre la ventana hasta que el proceso finalice. Ignore los mensajes de pantalla.
42.	Si ha detectado que en la actualidad está habilitado un usuario que ya no tiene necesidad de acceder al sistema puede usar el siguiente comando (**sin comillas**), siendo **NOMBREDELUSUARIO** el nombre del usuario candidato para su eliminación. **$ sudo userdel -r "NOMBREDELUSUARIO".**
43.	Ahora compruebe las "shells" predeterminadas de los usuarios con UID por encima del número 1000 (usuarios normales del sistema) Para ello ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd**

Paso	Descripción
44.	Se mostrarán todos los usuarios y sus respectivas shells. Compruebe que todas las shells de usuario coinciden con "**/bin/bash**".  **Nota:** Como se puede observar puede aparecer el usuario nobody con uid:65534 y como excepción se deberá conservar su shell. Por defecto, los directorios compartidos NFS cambian el usuario root (superusuario) por el usuario nfsnobody, una cuenta de usuario sin privilegios. De esta forma, todos los archivos creados por root son propiedad del usuario nfsnobody, lo que previene la carga de programas con la configuración del bit setuid. En Centos 8 el usuario "nobody" sustituye a "nfsnobody" para los siguientes grupos y usuarios: - El par de usuarios nobody y grupos con el ID de 99. - El par de usuario nfsnobody y grupo con el ID de 65534, que también es el ID de desbordamiento predeterminado del núcleo. Este cambio reduce la confusión sobre los archivos que son propiedad de NFS nobody pero no tienen nada que ver con NFS.
45.	Cuando finalice todas las tareas reinicie el sistema.

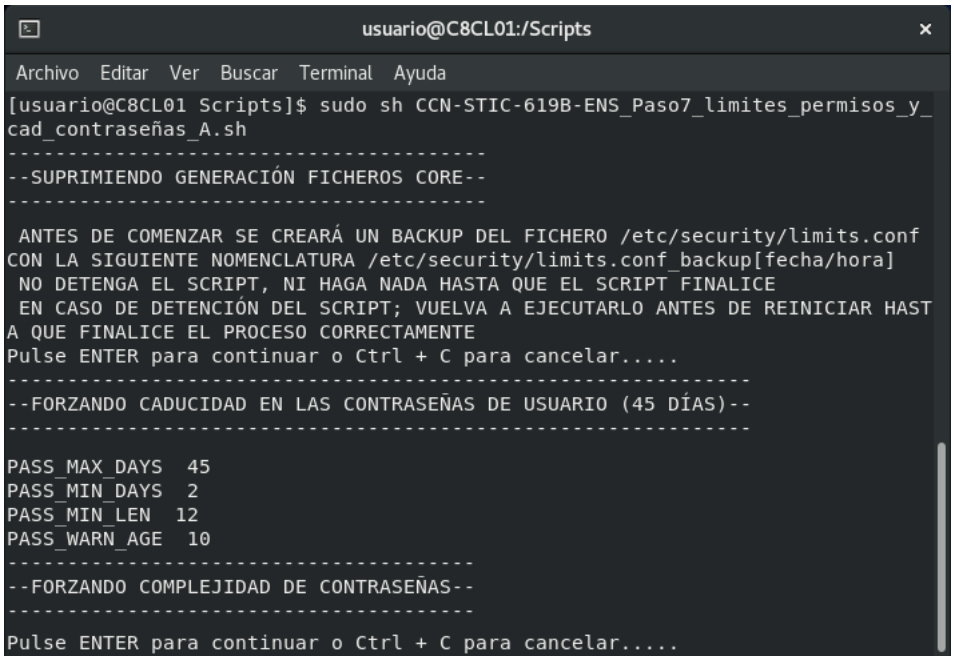
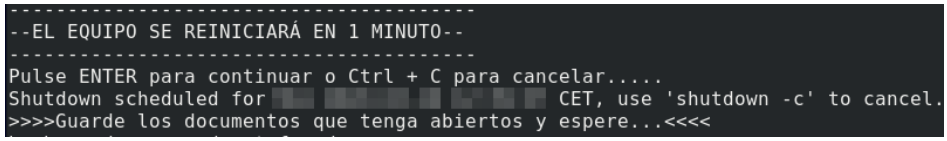
5.2. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS

Paso	Descripción
46.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
47.	Se procederá a configurar el bloqueo de cuentas por intentos fallidos, por medio del módulo "pam_faillock.so". Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente script. **$ sudo sh CCN-STIC-619B-ENS_Paso6_intentos_fallidos_A.sh**

Paso	Descripción
48.	El script alertará de la creación de una copia de seguridad de la configuración de los ficheros incluidos en /etc/pam.d/. El script añadirá una configuración que cumpla con los mínimos requisitos de seguridad. Al finalizar el proceso el sistema se reiniciará para aplicar la configuración.   **Nota:** Si el script se detuviera o no terminara correctamente, deberá restaurar la copia de seguridad creada e iniciar el script de nuevo, por el contrario, es posible que el sistema no pueda iniciarse correctamente.
49.	Si quisiera editar los ficheros con las necesidades de seguridad requeridos por su organización, ejecute los siguientes comandos. **$ sudo nano /etc/pam.d/password-auth** **$ sudo nano /etc/pam.d/ system-auth**  **Nota:** Hay que tener en consideración que el script aplica configuración sobre los ficheros por defecto de instalación. Por tanto, si existieran configuraciones previas a la ejecución del script, deberá adaptar éste o los ficheros a las necesidades específicas de su organización. No modifique estos ficheros de configuración si no conoce el funcionamiento de los módulos “pam.d”, podría provocar que el sistema no iniciara correctamente.

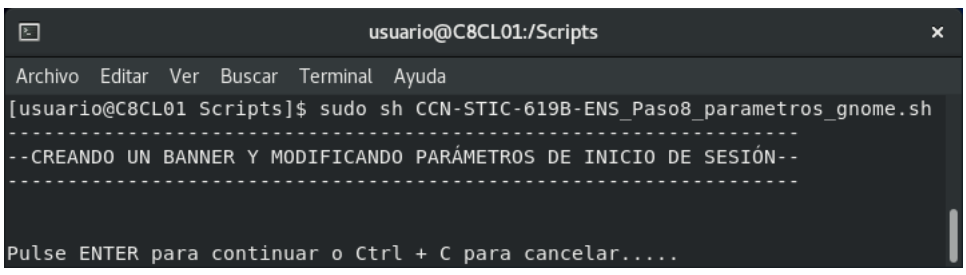
Paso	Descripción
50.	Si ha realizado modificaciones o ha detenido el reinicio automático, reinicie manualmente el sistema para que los cambios queden aplicados.

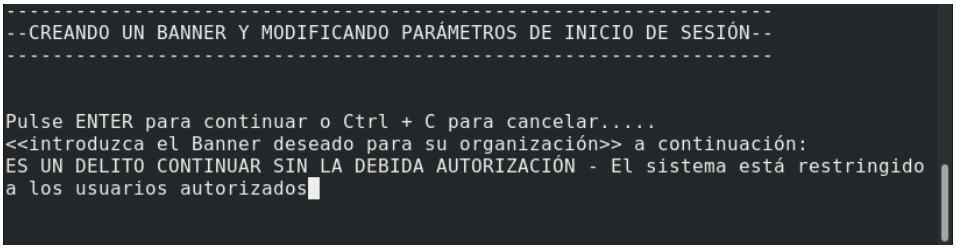
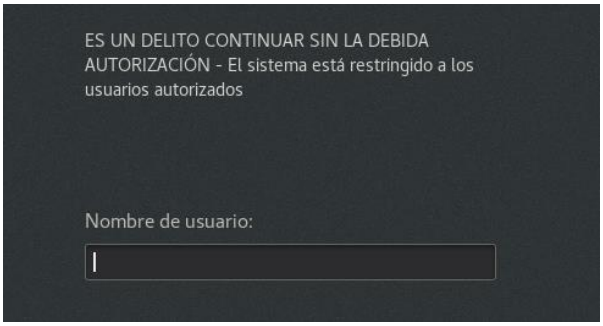
5.3. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

Paso	Descripción
51.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
52.	Antes de comenzar este paso, asegúrese de haber cerrado y guardado las aplicaciones y los documentos importantes. Se va a proceder a limitar los recursos disponibles para los usuarios, en particular limitar los "**volcados de núcleo** (core dumps)". Así mismo se forzará la caducidad de contraseñas para los nuevos usuarios y los ya existentes, la complejidad y los permisos en los directorios "/home" de cada usuario. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente script. **$ sudo sh CCN-STIC-619B-ENS_Paso7_limites_permisos_y_cad_contraseñas_A.sh**  Cuando finalice el script, saldrá un mensaje advirtiendo que el sistema se reiniciará en 1 minuto. Espere y cierre las aplicaciones que tenga abiertas. 

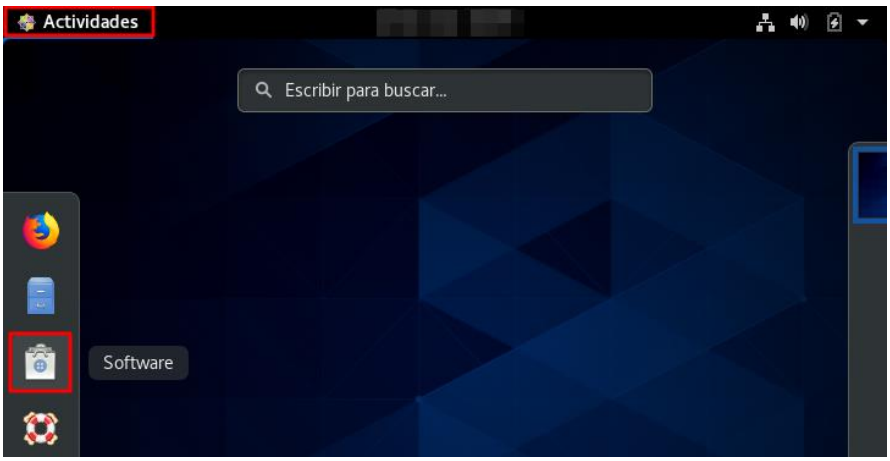
Paso	Descripción
53.	Cuando reinicie el sistema e inicie sesión, aparecerá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos. 
54.	Le pedirá la contraseña actual de nuevo y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.

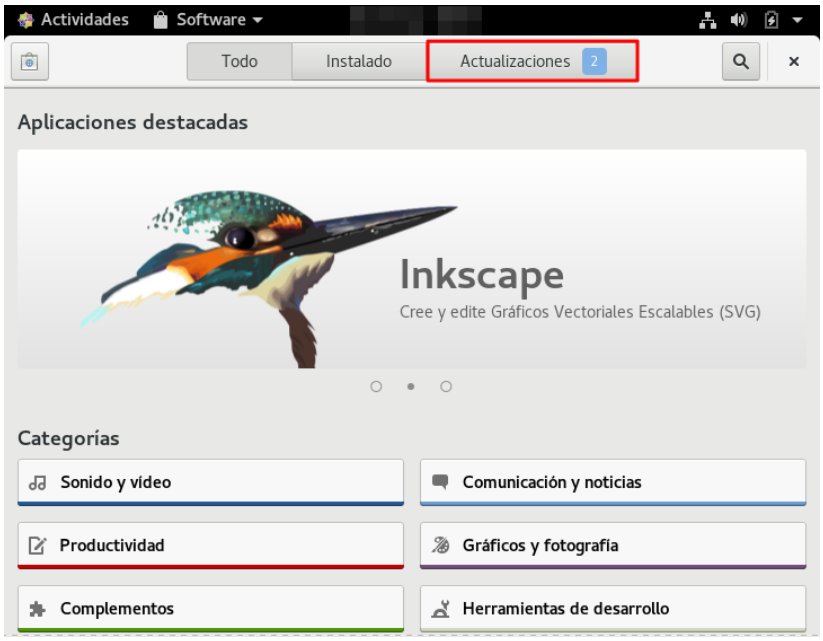
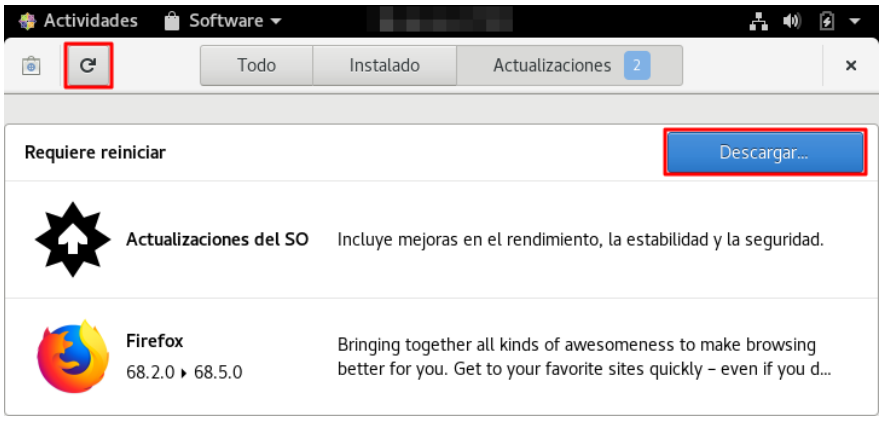
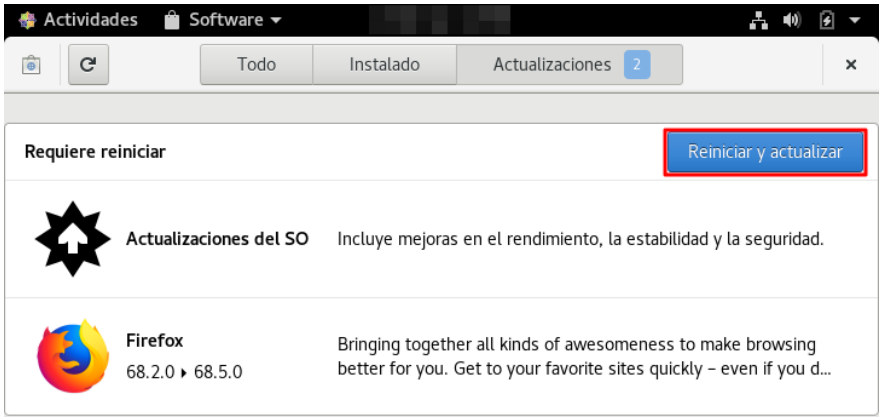
5.4. CONFIGURACIÓN SEGURA DE GNOME

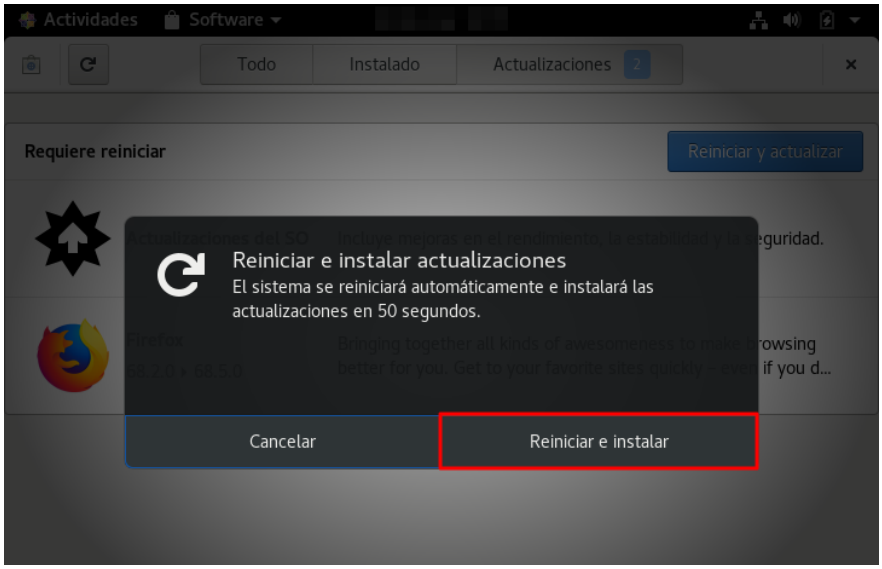
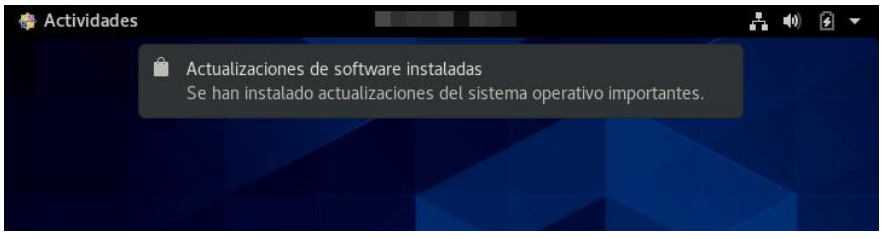
Paso	Descripción
55.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
56.	Se va a proceder a configurar parámetros de seguridad en el escritorio Gnome. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso8_parametros_gnome.sh** 

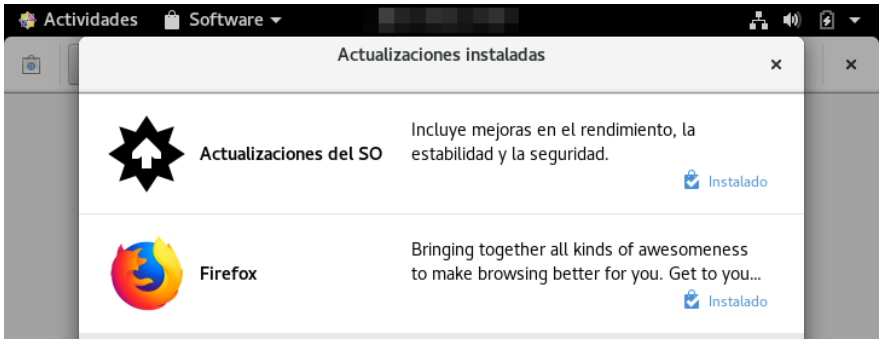
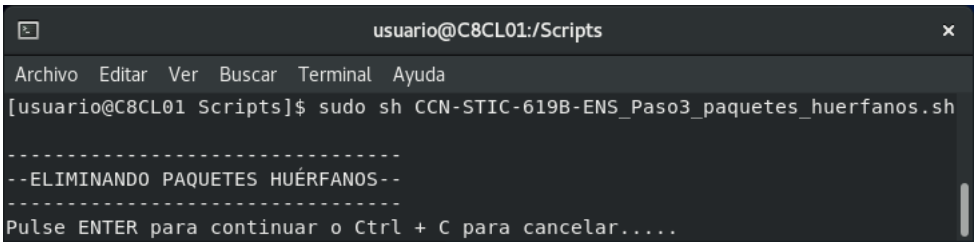
Paso	Descripción
57.	Introduzca el Banner deseado acorde con su organización. 
58.	El script iniciará un proceso que modificará la pantalla de inicio de CentOS 8 Linux para que aparezca un mensaje disuasorio (banner) al inicio y solicite usuario y contraseña. Así mismo se configurará un tiempo mínimo de bloqueo según requisitos de seguridad.  **Nota:** CentOS 8 Linux presenta mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

6. APLICACIÓN DE ACTUALIZACIONES

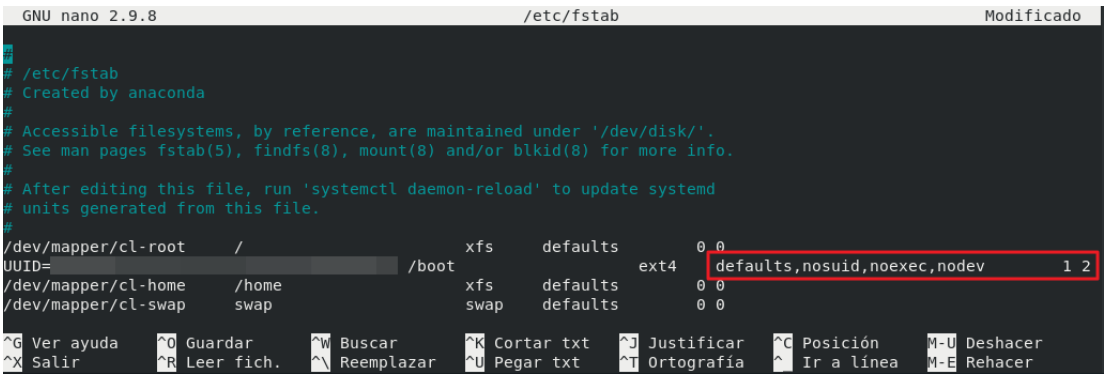
Paso	Descripción
59.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a “**Software**”. 

Paso	Descripción
60.	Una vez iniciada la aplicación, pulse sobre la pestaña “Actualizaciones”. 
61.	pulse sobre el botón de la flecha. ⟳ Comprobará si hay más actualizaciones; cuando finalice pulse en el botón “Descargar…”. 
62.	Cuando las actualizaciones se descarguen pulse “Reiniciar y Actualizar”- 

Paso	Descripción
63.	Confirme el reinicio en el botón 
64.	El sistema se reiniciará y comenzará a instalar las actualizaciones.  El proceso puede durar varios minutos, no presione ninguna tecla hasta que el proceso de actualización finalice.
65.	Cuando finalice, aparecerá la pantalla de inicio de CentOS 8. Inicie sesión y le saldrá un mensaje en el escritorio que le notificará las actualizaciones instaladas. 

Paso	Descripción
66.	Si presiona sobre el mensaje, aparecerán todas las aplicaciones que han sido actualizadas para su comprobación. 
67.	Cuando termine de revisar, cierre la ventana y su sistema estará actualizado. 
68.	Una vez finalizada la actualización, vuelva a ejecutar el script "CCN-STIC-619B-ENS_Paso3_paquetes_huerfanos.sh" del punto "3.2COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS". Para ello diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "Terminal". Ejecute el comando "**cd /**" y pulse la tecla "**Enter**". Diríjase a la carpeta "**/Scripts**" y ejecute el siguiente comando. **$ sudo sh CCN-STIC-619B-ENS_Paso3_paquetes_huerfanos.sh**  El script iniciará un proceso de desinstalación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice con un mensaje en pantalla de "¡Listo!".
69.	Reinicie el sistema para finalizar el proceso.

7. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

Paso	Descripción
70.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "**Terminal**". Ejecute el comando "**cd /**" y pulse la tecla "Enter".
71.	Ejecute el siguiente comando e introduzca la contraseña si se le solicita. **$ sudo nano /etc/fstab**
72.	Edite el fichero de configuración con el editor de textos "nano", modificando los permisos de la partición "/boot" para que el resultado sea similar al de la imagen (defaults,nosuid,noexec,nodev 1 2).  **Nota:** Para la modificación del fichero con el editor "nano" deberá navegar por el fichero mediante las flechas del teclado y modificar los datos eliminando o añadiendo las partes necesarias. Para guardar, pulse la combinación de teclas "Crtl + o" y luego "Enter" y para salir pulse la combinación de teclas "Crtl + x". Si requiere mas información sobre la utilización del editor "nano" diríjase a la siguiente URL: https://www.nano-editor.org/dist/v2.1/nano.html
73.	Cuando finalice de editar, pulse la combinación de teclas "Crtl + o" y luego "Enter" para guardar y la combinación de teclas "Crtl + x" para salir. Elimine el directorio "/Scripts" y todo su contenido. **Nota:** Debe tener en consideración, que para realizar actualizaciones del kernel es posible que deba restablecer los valores de la partición "/boot" a defaults y posteriormente cuando la actualización finalice, revertirlos a los establecidos por esta guía.

ANEXO A.5.2. LISTA DE COMPROBACIÓN DE CLIENTE CENTOS 7 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

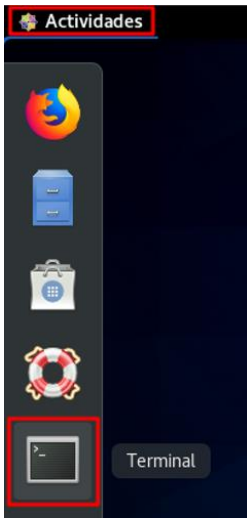
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.5.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES CENTOS 8 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

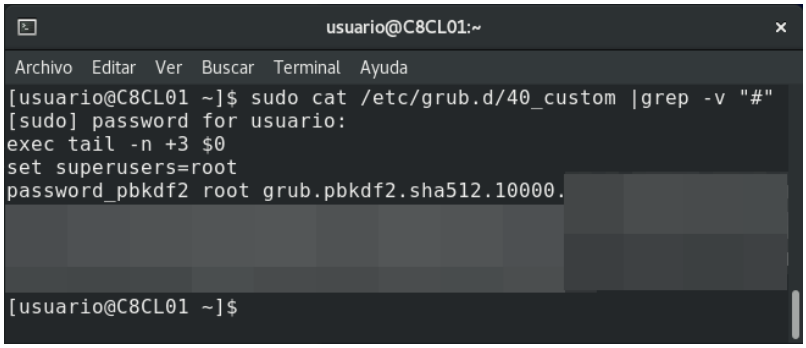
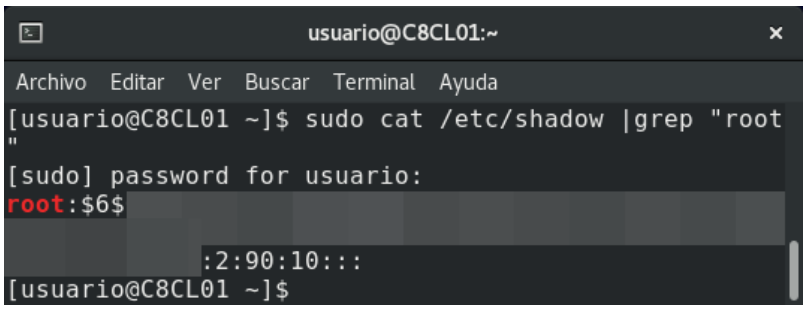
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes CentOS 8 independientes con implementación de seguridad en la categoría alta - DL del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas que se utilizarán son las siguientes:

a) Terminal de Linux

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de root. Cree la carpeta "Scripts" en "/" y copie el contenido del nivel de seguridad "ALTA" correspondiente al directorio "Scripts/ENS_ALTA" asociado a esta guía en la ruta "/Scripts".
2. Inicie la Terminal de Linux.		Ejecute la "Terminal", para ello diríjase a la barra de tareas superior, pulse sobre "Actividades" y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen. 

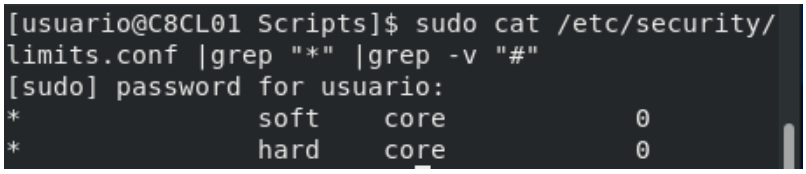
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que grub tiene contraseña configurada y root como único usuario de modificación.		En la "Terminal" ejecute el siguiente comando. **$ sudo cat /etc/grub.d/40_custom |grep -v "#"**  **Nota:** Fíjese en las letras y números que están situadas después de "password_pbkdf2 root grub.pbkdf2.sha512.". Pueden ser diferentes dependiendo del usuario, ya que se trata de un hash generado a partir de la contraseña dada al ejecutar el script.
4. Contraseña de root segura.		Abra la Terminal y ejecute el siguiente comando. **$ sudo cat /etc/shadow |grep "root"**  Fíjese que el inicio del hash de la contraseña de "root" comienza por "**6**", esto le indicará en qué tipo de hash está la contraseña de "root", en este caso es SHA-512, (Secure Hash Algorithm) y por lo tanto tiene 86 caracteres en total. Fíjese adicionalmente en que el final de la configuración termina por "**:2:90:10:::**" indicando que se ha configurado correctamente la caducidad de la cuenta.
5. Búsqueda de usuarios sin contraseña.		Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1** **Nota:** Si la configuración es correcta, no deberá mostrar ningún resultado la salida del comando.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>6. Búsqueda de usuarios con UID 0.</td><td></td><td>Ejecute el siguiente comando.
$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1 |grep -v "root"
Nota: Si la configuración es correcta, no deberá mostrar ningún resultado la salida del comando.</td></tr>
<tr><td>7. Verifique los parámetros del kernel.</td><td></td><td>Evitar modificación de tablas de encaminamiento ipv4.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.all.send_redirects ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.all.accept_redirects = "
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.default.accept_redirects ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.default.send_redirects ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.default.secure_redirects ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.all.secure_redirects ="</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.conf.all.send_redirects</td><td>0</td><td></td></tr>
<tr><td>net.ipv4.conf.all.accept_redirects</td><td>0</td><td></td></tr>
<tr><td>net.ipv4.conf.default.accept_redirects</td><td>0</td><td></td></tr>
<tr><td>net.ipv4.conf.default.send_redirects</td><td>0</td><td></td></tr>
<tr><td>net.ipv4.conf.default.secure_redirects</td><td>0</td><td></td></tr>
<tr><td>net.ipv4.conf.all.secure_redirects</td><td>0</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td><td>Evitar modificación de tablas de encaminamiento ipv6.
$ sudo cat /etc/sysctl.conf |grep "net.ipv6.conf.default.accept_source_route ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv6.conf.all.accept_source_route = "
$ sudo cat /etc/sysctl.conf |grep "net.ipv6.conf.all.accept_redirects = "
$ sudo cat /etc/sysctl.conf |grep "net.ipv6.conf.default.accept_ra = "
$ sudo cat /etc/sysctl.conf |grep "net.ipv6.conf.all.accept_ra = "
$ sudo cat /etc/sysctl.conf |grep "net.ipv6.conf.default.accept_redirects = "</td></tr>
</table>

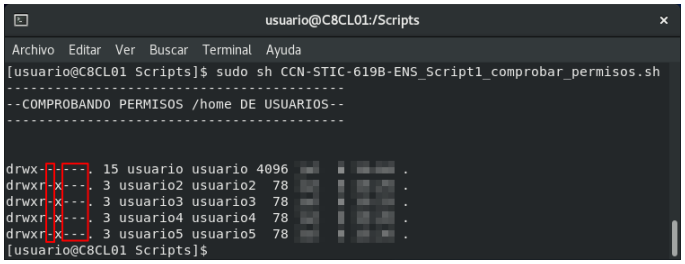
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv6.conf.default.accept_source_route</td><td>0</td><td></td></tr>
<tr><td>net.ipv6.conf.all.accept_source_route</td><td>0</td><td></td></tr>
<tr><td>net.ipv6.conf.all.accept_redirects</td><td>0</td><td></td></tr>
<tr><td>net.ipv6.conf.default.accept_ra</td><td>0</td><td></td></tr>
<tr><td>net.ipv6.conf.all.accept_ra</td><td>0</td><td></td></tr>
<tr><td>net.ipv6.conf.default.accept_redirects</td><td>0</td><td></td></tr>
<tr><td></td><td colspan="2">Deshabilitar el source routing.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.all.accept_source_route ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.default.accept_source_route ="</td></tr>
</table>
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.conf.all.accept_source_route</td><td>0</td><td></td></tr>
<tr><td>net.ipv4.conf.default.accept_source_route</td><td>0</td><td></td></tr>
<tr><td></td><td colspan="2">Activa los logs para paquetes anormales o excepcionales.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.all.log_martians ="
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.conf.default.log_martians ="</td></tr>
</table>
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.conf.all.log_martians</td><td>1</td><td></td></tr>
<tr><td>net.ipv4.conf.default.log_martians</td><td>1</td><td></td></tr>
<tr><td></td><td colspan="2">Ignorar peticiones broadcast.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.icmp_echo_ignore_broadcasts ="</td></tr>
</table>
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.icmp_echo_ignore_broadcasts</td><td>1</td><td></td></tr>
<tr><td></td><td colspan="2">Ignorar mensajes de error mal formados.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.icmp_ignore_bogus_error_responses ="</td></tr>
</table>
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.icmp_ignore_bogus_error_responses</td><td>1</td><td></td></tr>
<tr><td></td><td colspan="2">Protegerse ante ataques TCP-SYN.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.tcp_syncookies ="</td></tr>
</table>
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.tcp_syncookies</td><td>1</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>Bloqueo de core dumps de programas con SUID.
$ sudo cat /etc/sysctl.conf |grep "fs.suid_dumpable ="
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>fs.suid_dumpable</td><td>0</td><td></td></tr>
</table></td></tr>
<tr><td>8. Servicios innecesarios</td><td></td><td>Abra la Terminal y ejecute el siguiente comando.
$ sudo systemctl list-unit-files --type=service
<pre>UNIT FILE   STATE
accounts-daemon.service   enabled
alsa-restore.service   static
alsa-state.service   static
anaconda-direct.service   static
anaconda-nm-config.service   static
anaconda-noshell.service   static
anaconda-pre.service   static
anaconda-shell@.service   static
anaconda-sshd.service   static
anaconda-tmux@.service   static
anaconda.service   static
arp-ethers.service   disabled
atd.service   enabled
auditd.service   enabled
autovt@.service   enabled
avahi-daemon.service   enabled
lines 1-17</pre>
Revise que los servicios activos al iniciar el sistema son los correctos para su organización.</td></tr>
<tr><td>9. Comprobación de usuarios y shells predeterminadas.</td><td></td><td>Ejecute el siguiente comando.
$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $7 } }' /etc/passwd |grep -v "nobody"
<pre>usuario@C8CL01:~
Archivo Editar Ver Buscar Terminal Ayuda
[usuario@C8CL01 ~]$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd |grep -v "nobody"
usuario:1000/bin/bash
usuario2:1001/bin/bash
usuario3:1002/bin/bash
usuario4:1003/bin/bash
usuario5:1004/bin/bash
[usuario@C8CL01 ~]$</pre>
Compruebe si los usuarios que se muestran son los más adecuados para su organización y que están correctas las shells predeterminadas.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>10. Comprobación de registros de actividad</td><td></td><td>Primero se va a comprobar el fichero de configuración, con los parámetros definidos por esta guía.
Ejecute los siguientes comandos.
$ sudo cat /etc/audit/auditd.conf |grep "max_log_file ="
$ sudo cat /etc/audit/auditd.conf |grep "num_logs ="
$ sudo cat /etc/audit/auditd.conf |grep "max_log_file_action ="
$ sudo ls -laR /etc/audit/auditd.conf | cut -d' ' -f1</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>max_log_file</td><td>10</td><td></td></tr>
<tr><td>num_logs</td><td>12</td><td></td></tr>
<tr><td>max_log_file_action</td><td>ROTATE</td><td></td></tr>
<tr><td>/etc/audit/auditd.conf</td><td>-rw-r-----.</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td><td>Ejecute el siguiente comando y revise que las reglas de adaptan a las específicas para su organización.
$ sudo auditctl -l</td></tr>
<tr><td>11. Parámetros de bloqueo de cuenta.</td><td></td><td>Se va a comprobar los ficheros de configuración, con los parámetros definidos por esta guía.
– /etc/pam.d/password-auth
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/password-auth |grep "auth" |grep "pam_faillock.so" |grep "deny="
$ sudo cat /etc/pam.d/password-auth |grep "auth" |grep "unlock_time"
$ sudo cat /etc/pam.d/password-auth |grep "account" |grep "pam_faillock.so"
$ sudo cat /etc/pam.d/password-auth |grep "pam_pwhistory" |grep "remember"</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>deny</td><td>8</td><td></td></tr>
<tr><td>unlock_time</td><td>0</td><td></td></tr>
<tr><td>pam_faillock.so</td><td>Existe</td><td></td></tr>
<tr><td>remember</td><td>25</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>– /etc/pam.d/system-auth
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/system-auth |grep "auth" |grep "pam_faillock.so" |grep "deny="
$ sudo cat /etc/pam.d/system-auth |grep "auth" |grep "unlock_time"
$ sudo cat /etc/pam.d/system-auth |grep "account" |grep "pam_faillock.so"
$ sudo cat /etc/pam.d/system-auth |grep "pam_pwhistory" |grep "remember"</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>deny</td><td>8</td><td></td></tr>
<tr><td>unlock_time</td><td>3600</td><td></td></tr>
<tr><td>pam_faillock.so</td><td>Existe</td><td></td></tr>
<tr><td>remember</td><td>25</td><td></td></tr>
</table></td></tr>
<tr><td>12. Configuración de los volcados de núcleo (core dumps)</td><td></td><td>Ejecute el siguiente comando.
$ sudo cat /etc/security/limits.conf |grep "*" |grep -v "#"
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Soft core</td><td>0</td><td></td></tr>
<tr><td>Hard core</td><td>0</td><td></td></tr>
</table></td></tr>
<tr><td>13. Banner disuasorio.</td><td></td><td>Ejecute los siguientes comandos.
$ cat /etc/issue
$ cat /etc/issue.net
$ cat /etc/motd
Compruebe si se han configurado bien los mensajes disuasorios (banners).</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>14. Verifique la directiva de caducidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MAX_DAYS"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MIN_DAYS"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_MIN_LEN"
$ sudo cat /etc/login.defs |grep -v "#" |grep "PASS_WARN_AGE"
$ sudo cat /etc/login.defs |grep "UMASK"
$ sudo cat /etc/login.defs |grep "ENCRYPT_METHOD"
Compruebe si se han configurado bien los siguientes valores.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>PASS_MAX_DAYS</td><td>45</td><td></td></tr>
<tr><td>PASS_MIN_DAYS</td><td>2</td><td></td></tr>
<tr><td>PASS_MIN_LEN</td><td>12</td><td></td></tr>
<tr><td>PASS_WARN_AGE</td><td>10</td><td></td></tr>
<tr><td>UMASK</td><td>027</td><td></td></tr>
<tr><td>ENCRYPT_METHOD</td><td>SHA512</td><td></td></tr>
</table></td></tr>
<tr><td>15. Verifique la directiva de complejidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/security/pwquality.conf |grep "minlen ="
$ sudo cat /etc/security/pwquality.conf |grep "dcredit ="
$ sudo cat /etc/security/pwquality.conf |grep "ucredit ="
$ sudo cat /etc/security/pwquality.conf |grep "lcredit ="
Compruebe si se han configurado bien los siguientes valores.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>minlen</td><td>12</td><td></td></tr>
<tr><td>dcredit</td><td>-1</td><td></td></tr>
<tr><td>ucredit</td><td>-1</td><td></td></tr>
<tr><td>lcredit</td><td>-1</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>16.Comprobar permisos</td><td></td><td>Se va a proceder a revisar los permisos de la ruta “/home” de casa usuario del sistema.
Para ello diríjase a la carpeta “Scripts”.
$ cd /Scripts
Ejecute el siguiente comando.
$ sudo sh CCN-STIC-619B-ENS_Script1_comprobar_permisos.sh
El script mostrará los permisos de las carpetas “/home” y se debe comprobar que coincidan las columnas marcadas se encuentren vacías.
 
</td></tr>
<tr><td>17.Configuración de Gnome</td><td></td><td>Se va a proceder a revisar los parámetros de configuración de Gnome.
Para ello ejecute los siguientes comandos.
$ cat /etc/dconf/db/gdm.d/01-banner-message
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>banner-message-enable</td><td>true</td><td></td></tr>
<tr><td>banner-message-text</td><td>“Texto elegido”</td><td></td></tr>
</table>
$ cat /etc/dconf/db/gdm.d/00-login-screen |grep "disable-user-list"
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>disable-user-list</td><td>true</td><td></td></tr>
</table>
$ cat /etc/dconf/db/local.d/00-screensaver |grep "idle-delay=uint32"
$ cat /etc/dconf/db/local.d/00-screensaver |grep "lock-enabled"
$ cat /etc/dconf/db/local.d/00-screensaver |grep "lock-delay=uint32"
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>idle-delay=uint32</td><td>600</td><td></td></tr>
<tr><td>lock-enabled</td><td>true</td><td></td></tr>
<tr><td>lock-delay=uint32</td><td>0</td><td></td></tr>
</table></td></tr>
</table>

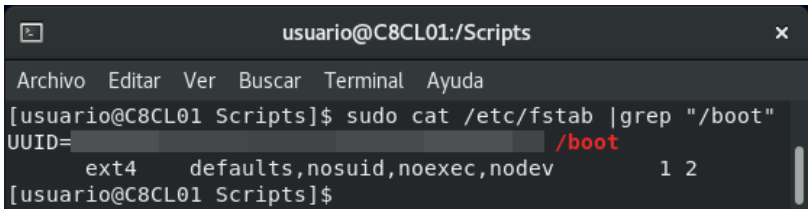
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>

```
$ cat /etc/dconf/db/local.d/03-privacy |grep "hide-identity"
$ cat /etc/dconf/db/local.d/03-privacy |grep "old-files-age"
$ cat /etc/dconf/db/local.d/03-privacy |grep "remember-recent-files"
$ cat /etc/dconf/db/local.d/03-privacy |grep "remove-old-temp-files"
```

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>hide-identity</td><td>true</td><td></td></tr>
<tr><td>old-files-age</td><td>0</td><td></td></tr>
<tr><td>remember-recent-files</td><td>false</td><td></td></tr>
<tr><td>remove-old-temp-files</td><td>true</td><td></td></tr>
</table>

</td></tr>
<tr><td>18. Permisos partición de inicio.</td><td></td><td>Compruebe que se han guardado los permisos en el fichero de configuración.

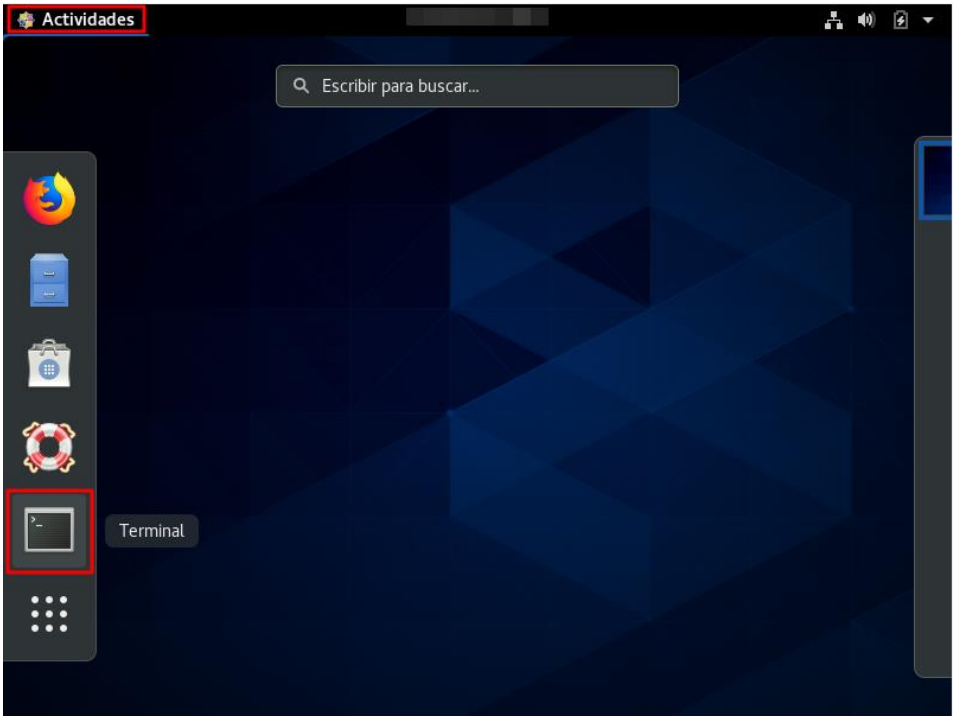
```
$ sudo cat /etc/fstab |grep "/boot"
```

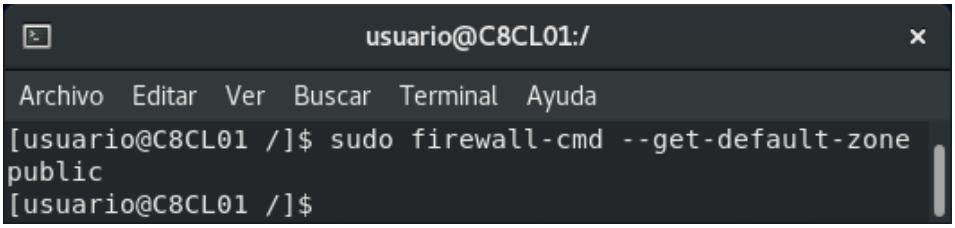
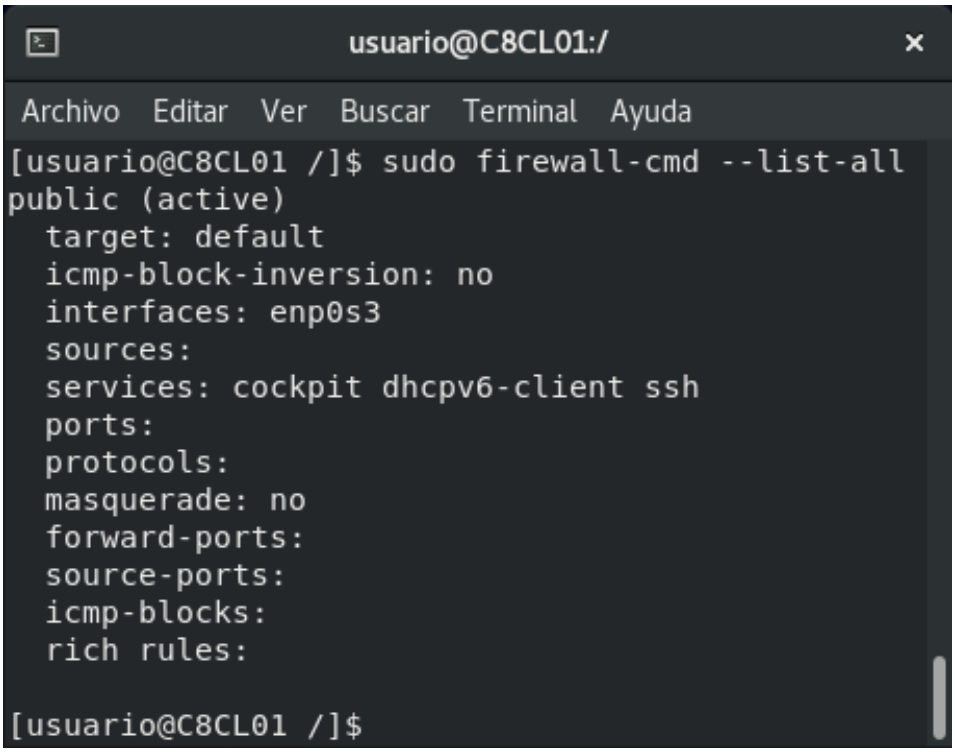


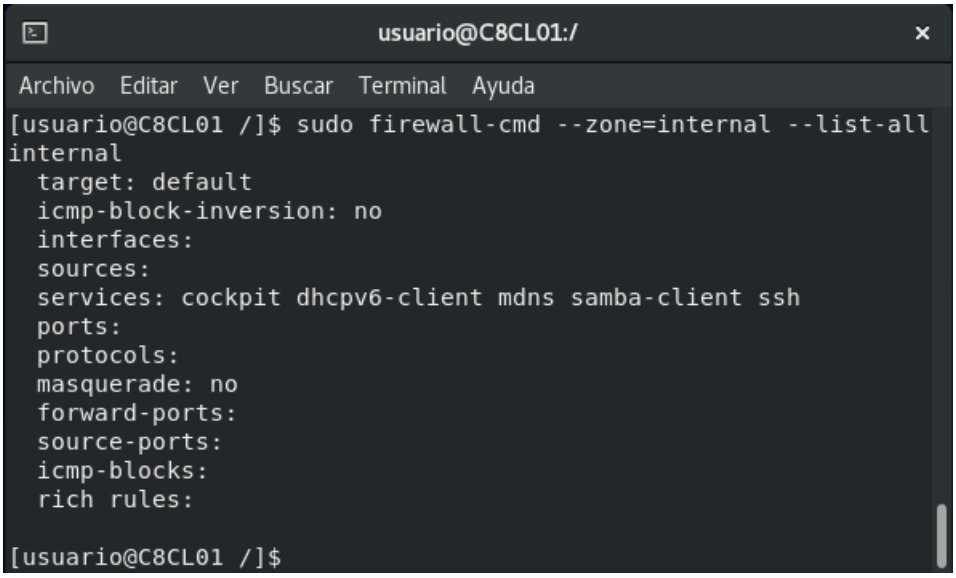
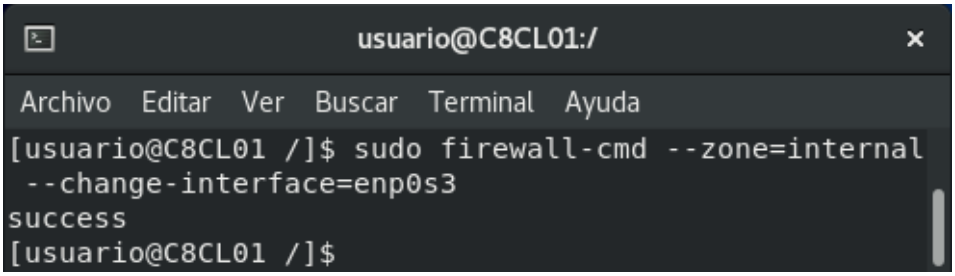
</td></tr>
</table>

ANEXO A.6. TAREAS ADICIONALES DE SEGURIDAD

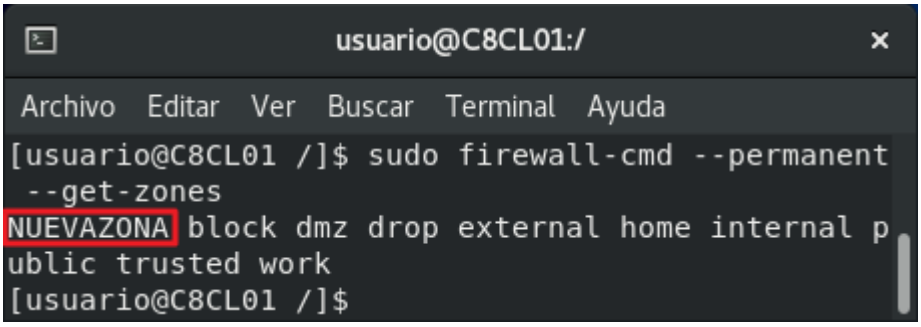
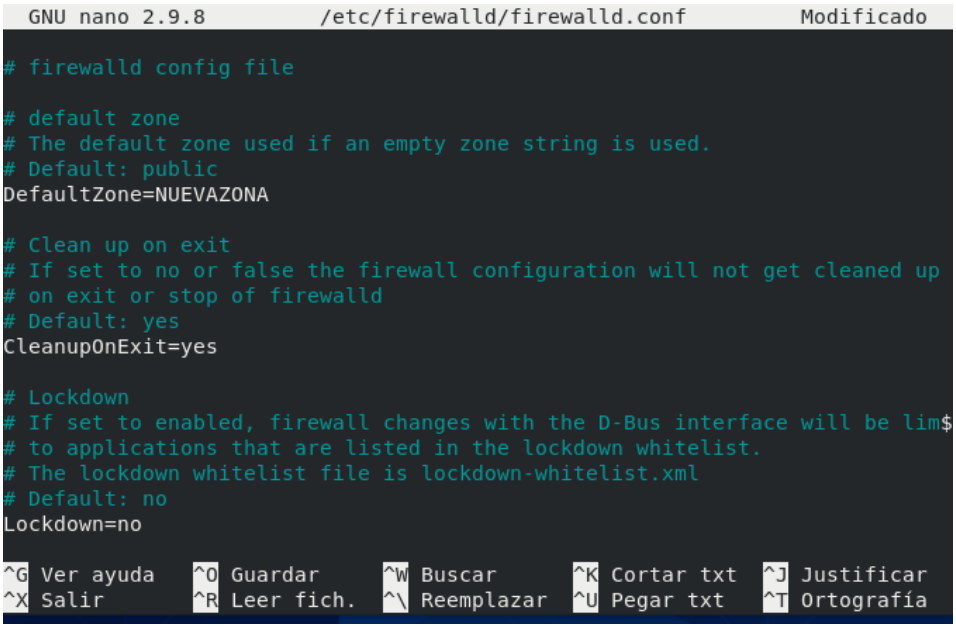
ANEXO A.6.1. PROTECCIÓN DE SERVICIOS DE RED. CONFIGURACIÓN DEL FIREWALL

Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".
3.	Diríjase a la barra de tareas superior, pulse sobre "Actividades" y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen. 
4.	Ejecute el comando "**cd /**" y pulse la tecla "Enter".
5.	Se procede a configurar el Firewall de CentOS 8. Para ello es importante que antes de crear las reglas y elegir la zona que más se adecue a su organización se active el servicio de Firewalld. Ejecute el siguiente comando. **$ sudo systemctl start firewalld.service** Compruebe su estado con siguiente comando. **$ sudo firewall-cmd --state** El comando devuelve por pantalla "running", si no es así vuelva al inicio del paso 2.

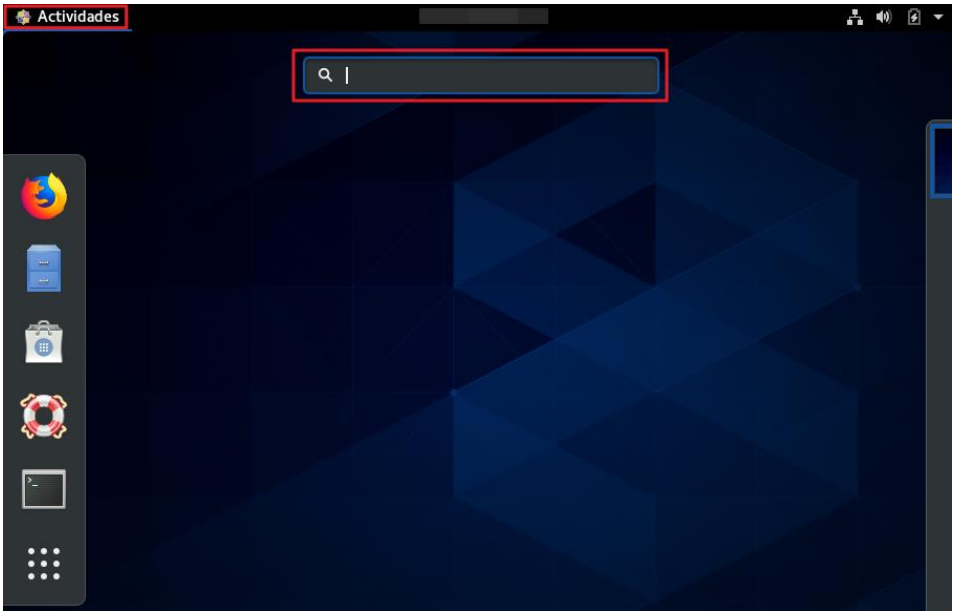
Paso	Descripción
6.	Para visualizar la zona actual en la cual se encuentra el equipo se usará el siguiente comando. **$ sudo firewall-cmd --get-default-zone** 
7.	Para conocer qué reglas están asociadas a dicha zona Se puede ejecutar el siguiente comando. **$ sudo firewall-cmd --list-all** 
8.	Se pueden verificar que zonas están disponibles para usar ingresando el siguiente comando. **$ sudo firewall-cmd --get-zones**

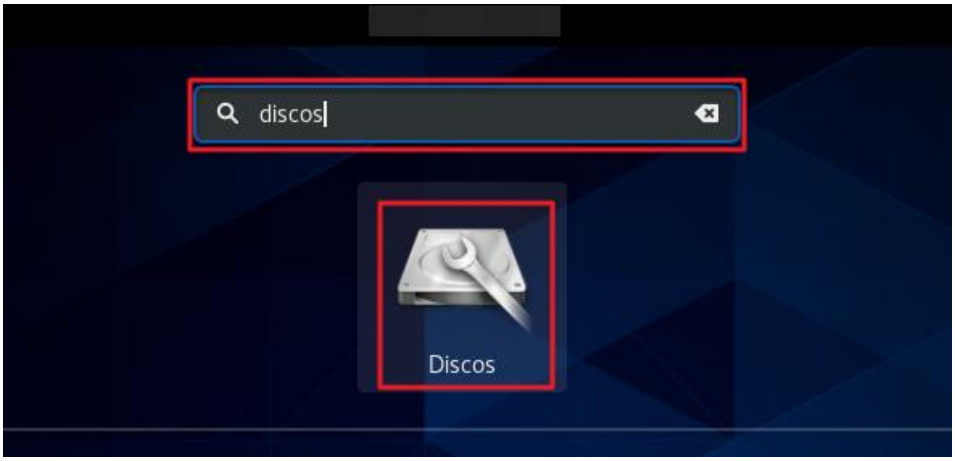
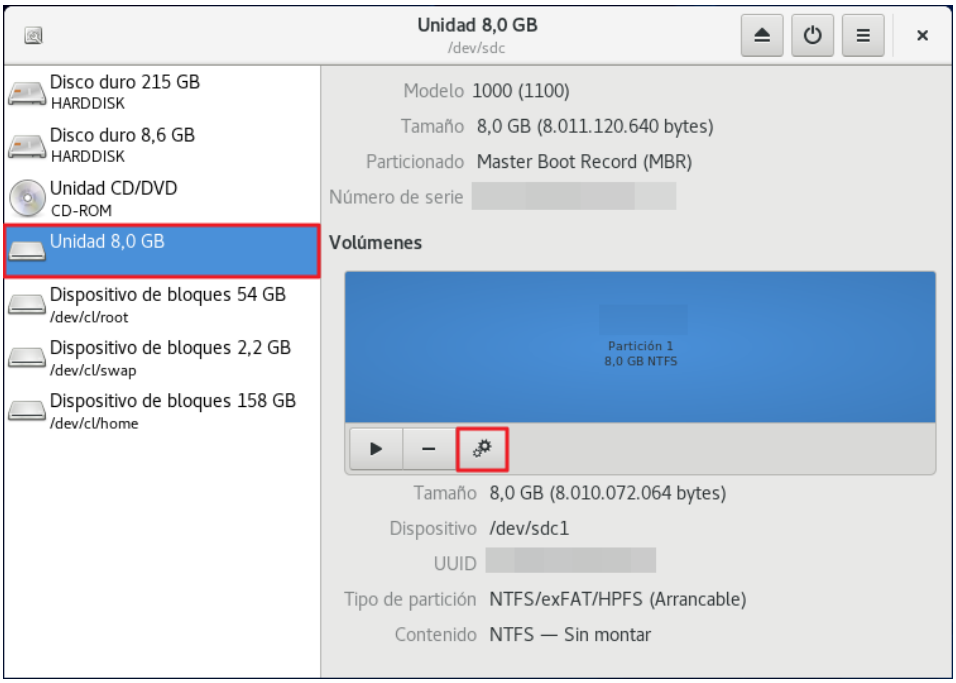
Paso	Descripción
9.	Para ver la configuración asociada a una zona y así elegir la zona que más interese a su organización se puede verificar usando el parámetro "**--zone**"; por ejemplo. **$ sudo firewall-cmd --zone=internal --list-all** 
10.	Es posible que en una sesión activa se desee asignar una zona específica a una interfaz de red del equipo, para ello asigne la zona "work" a la interfaz "enp0s3", por ejemplo. **$ sudo firewall-cmd --zone=work --change-interface=enp0s3** 
11.	Si quisiera que la zona perteneciera la esa interfaz de forma permanente ejecute el siguiente comando. **$ sudo firewall-cmd --zone=work --permanent --change-interface=enp0s3**
12.	Se pueden agregar excepciones al Firewall para que determinadas aplicaciones puedan ser ejecutadas de forma directa sin ningún problema, para ver los servicios disponibles en CentOS 8 Linux usa el siguiente comando. **$ sudo firewall-cmd --get-services**

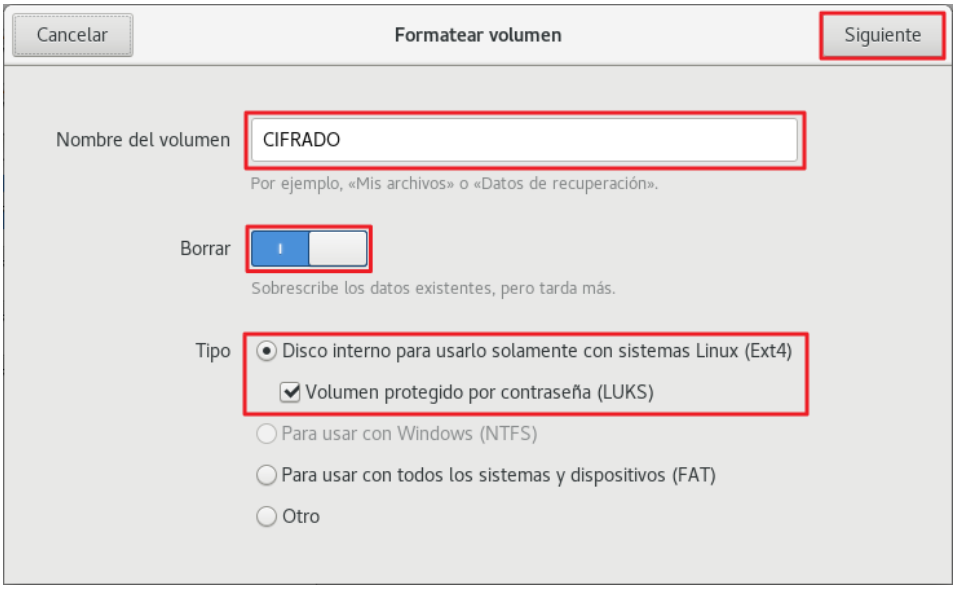
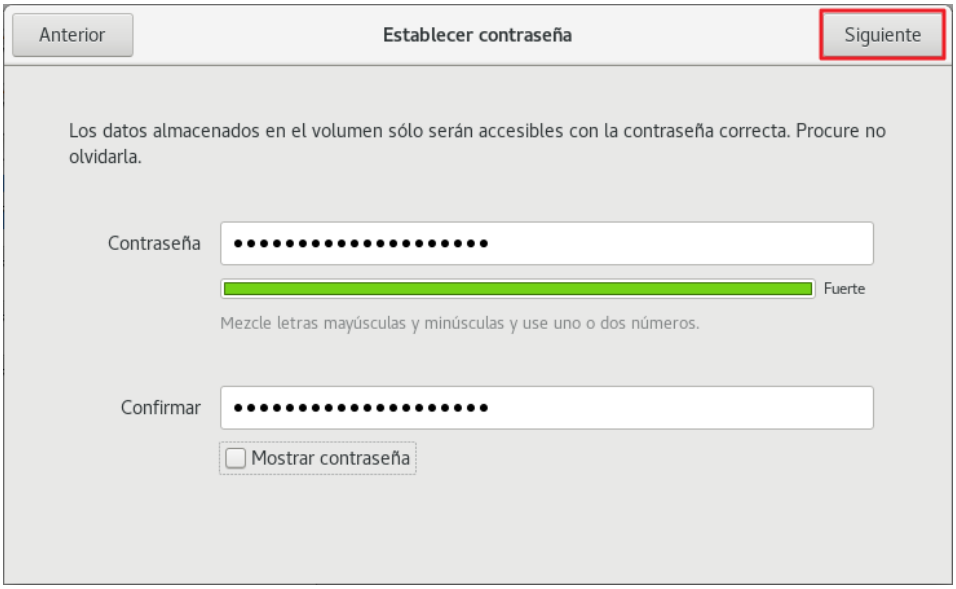
Paso	Descripción
13.	Para habilitar un servicio en una zona específica será necesario usar el parámetro "--add-service=" Por ejemplo, si desea agregar el servicio "https" en la zona publica se usará el siguiente comando. **$ sudo firewall-cmd --zone=public --add-service=https** **Nota:** Si por el contrario quisiera eliminar un servicio en una zona predeterminada, deberá ejecutar el siguiente comando. - $sudo firewall-cmd --zone=[**ZONA**] --remove-service=[**SERVICIO**] Por ejemplo, para deshabilitar el servicio de dhcp en ipv6 de la zona public, se realizaría con el siguiente comando. - $sudo firewall-cmd --zone=public --remove-service=dhcpv6
14.	Para comprobar los servicios permitidos en dicha zona, incluido el que se acaba de añadir, use el siguiente comando. **$ sudo firewall-cmd --zone=public --list-services** usuario@C8CL01:/ Archivo Editar Ver Buscar Terminal Ayuda [usuario@C8CL01 /]$ sudo firewall-cmd --zone=public --list-services cockpit dhcpv6-client https ssh [usuario@C8CL01 /]$
15.	Si quisiera que el servicio esté agregado a esa zona de forma permanente ejecute el siguiente comando. **$ sudo firewall-cmd --zone=public --permanent --add-service=https**
16.	Si, por el contrario, quisiera permitir un puerto en vez de un servicio la sintaxis del comando sería la siguiente, por ejemplo, para añadir el puerto 3500 del protocolo udp a la zona "internal". **$ sudo firewall-cmd --zone=internal --add-port=3500/udp**
17.	Para comprobar los puertos abiertos en una zona del firewall se usa el siguiente comando, por ejemplo, para ver los puertos abiertos en la zona "work". **$ sudo firewall-cmd --list-ports --zone=internal** usuario@C8CL01:/ Archivo Editar Ver Buscar Terminal Ayuda [usuario@C8CL01 /]$ sudo firewall-cmd --list-ports --zone=internal 3500/udp [usuario@C8CL01 /]$

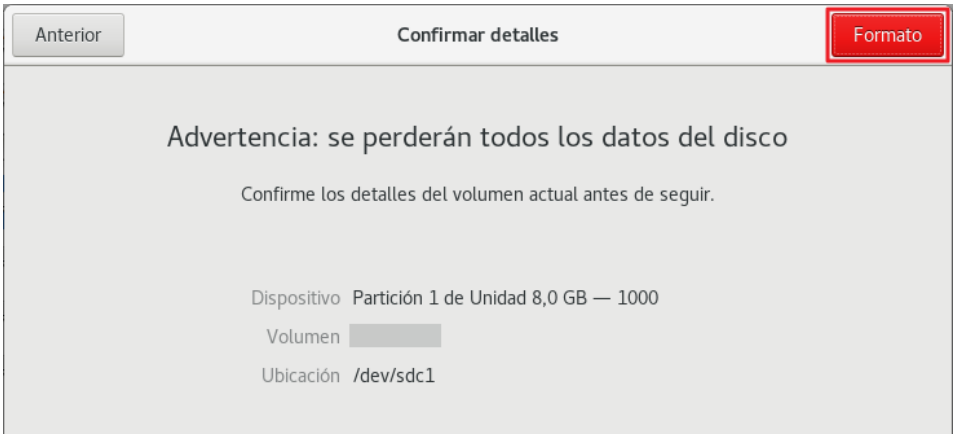
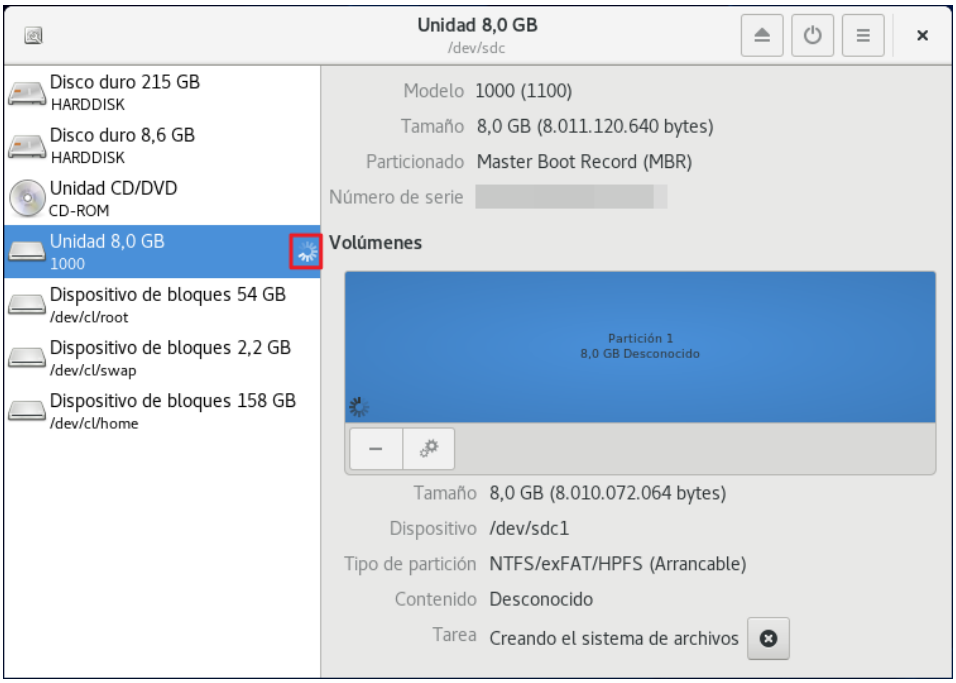
Paso	Descripción
18.	Se recomienda crear una zona propia de la que se tenga control total y pueda cubrir las necesidades de su organización Para ello ejecute el siguiente comando siendo “NUEVAZONA” el nombre de la zona que se elegirá. **$ sudo firewall-cmd --new-zone=[NUEVAZONA] --permanent --add-service=[SERVICIO]** Por ejemplo, se añade una zona y se permite un servicio. **$ sudo firewall-cmd --new-zone=NUEVAZONA --permanent --add-service=ssh**
19.	Para que la zona se refleje reinicie el Firewall con el siguiente comando. **$ sudo firewall-cmd --reload** Compruebe que está agregada correctamente. **$ sudo firewall-cmd --permanent --get-zones** 
20.	Por último, si quisiera realizar configuraciones adicionales o modificar la zona por defecto modifique los parámetros necesarios en el fichero de configuración de firewalld (/etc/firewalld/firewalld.conf). Para editar el fichero ejecute el siguiente comando. **$ sudo nano /etc/firewalld/firewalld.conf** 

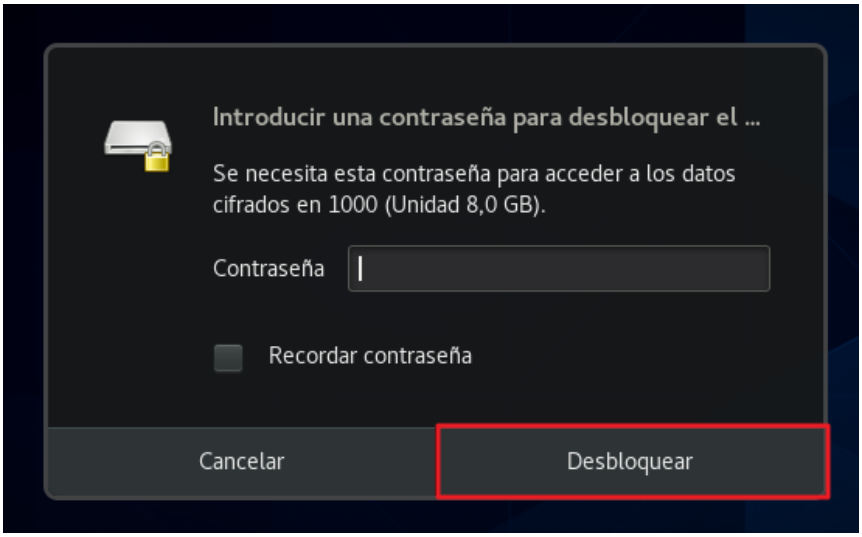
ANEXO A.6.2. PROTECCIÓN DEL DISCO. CIFRADO

Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".
3.	Este apartado es de aplicación para sistemas con particionado separado por puntos de montaje y para particiones independientes al sistema operativo por defecto como unidades extraíbles. Para particiones del sistema cifradas se recomienda realizar el cifrado en el momento de la instalación. **Nota:** Por defecto la instalación de CentOS 8 Linux crea cuatro particiones - **/dev/mapper/cl-root**, montada en la raíz del sistema "**/**". - **UUID=XXXXXXX-XXXX-XXXX-XXXXXXX,** montada en "/boot" - **/dev/mapper/cl-home,** montada en "**/home**". - **/dev/centos/cl-swap**, sin punto de montaje. Se recomienda cifrar las particiones sensibles del Sistema operativo y la partición "/home" de los usuarios, pero al no estar separadas en particiones independientes por defecto en la instalación, se mostrará un ejemplo de cómo cifrar una partición ajena a las mencionadas con LUKS. Hay que tener en consideración que el proceso de cifrado de una partición con LUKS, provoca la pérdida total de la información contenida en esa partición.
4.	Diríjase a la barra de tareas superior, pulse en Actividades y pulse sobre la barra de búsqueda central. 

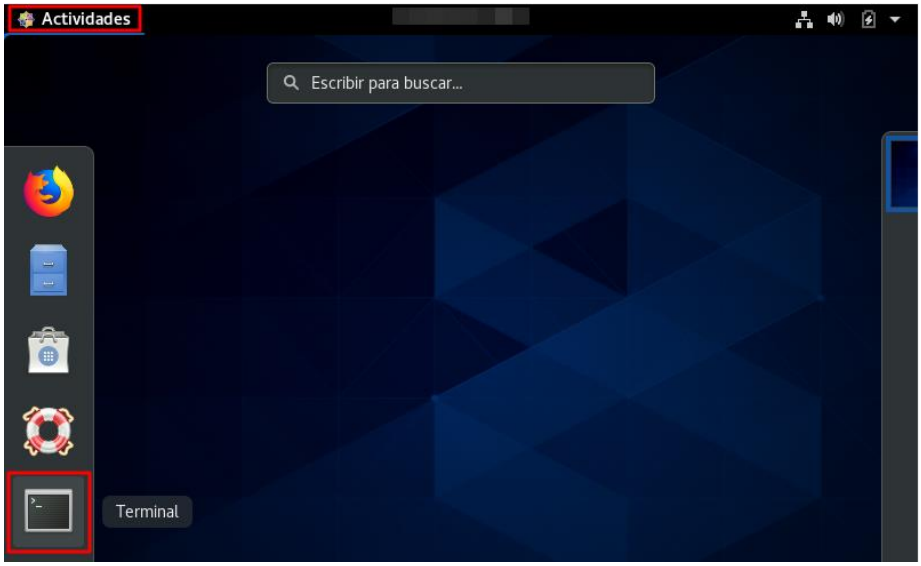
Paso	Descripción
5.	Escriba “discos” en el recuadro de búsqueda y posteriormente pulse sobre el icono de “Discos”. 
6.	Seleccione el disco que desee cifrar y pulse en el icono de los engranajes seleccionando “Formatear partición…”. En este caso se seleccionará un dispositivo extraíble. 

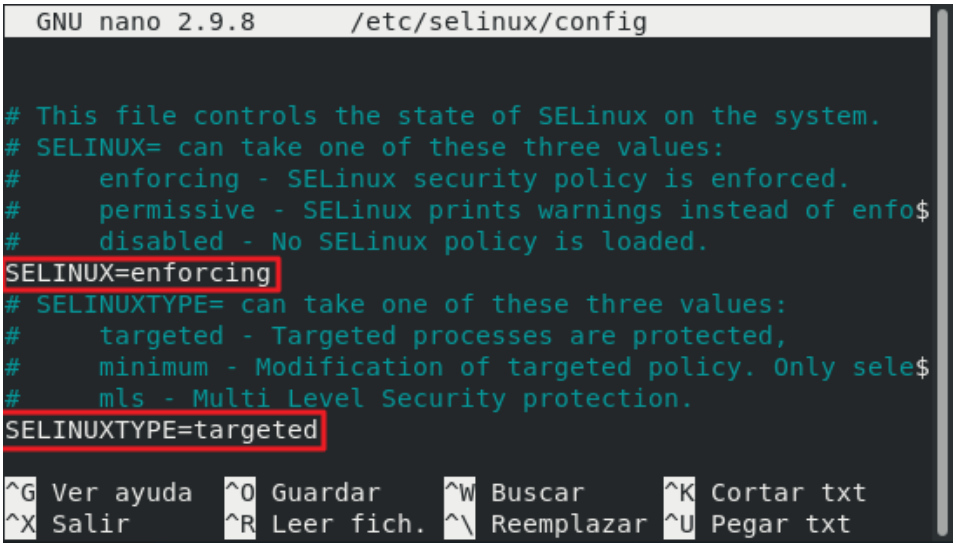
Paso	Descripción
7.	Indique el nombre del volumen, pulse sobre el interruptor “Borrar” y en el apartado Tipo, seleccione “Disco interno para usarlo solamente con sistemas Linux (ext4)” y marque la casilla “Volumen protegido por contraseña (LUKS). Posteriormente pulse “Siguiente”. 
8.	Introduzca la contraseña en el recuadro “Contraseña” y vuelva a repetirla en el recuadro “Confirmar”. Posteriormente pulse “Siguiente”. 

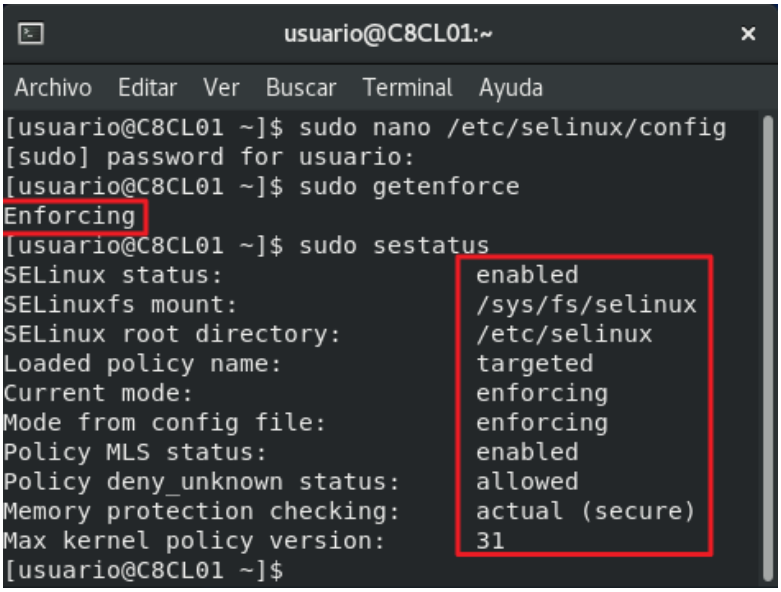
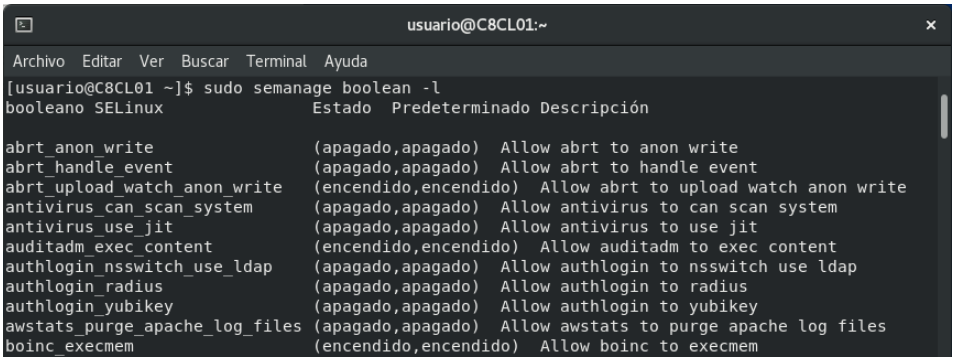
Paso	Descripción
9.	El sistema le advertirá de la pérdida total de la información en la unidad. Si todo es correcto pulse el botón rojo “Formato” para continuar. 
10.	La herramienta comenzará con la creación del sistema de archivos y la encriptación de la unidad, no toque nada hasta que la ruleta situada a la derecha de la unidad desaparezca. Es posible que tarde varios minutos. 
11.	Una vez finalice, extraiga con seguridad la unidad e introdúzcala en el sistema nuevamente.

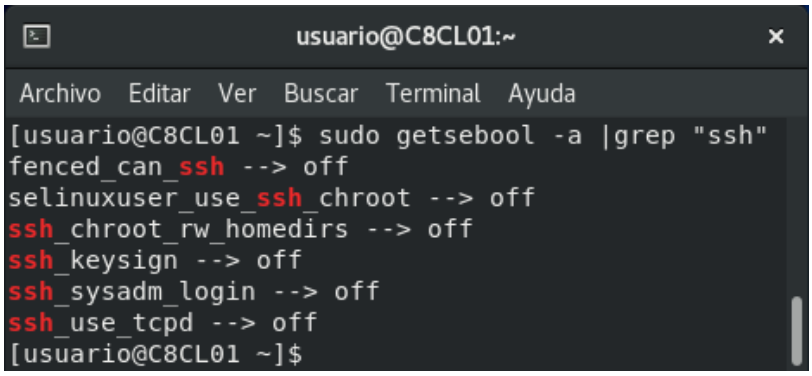
Paso	Descripción
12.	Cada vez que introduzca el dispositivo, se le solicitará la contraseña configurada para desbloquear. Introduzca por tanto la contraseña y pulse el botón “Desbloquear”. 

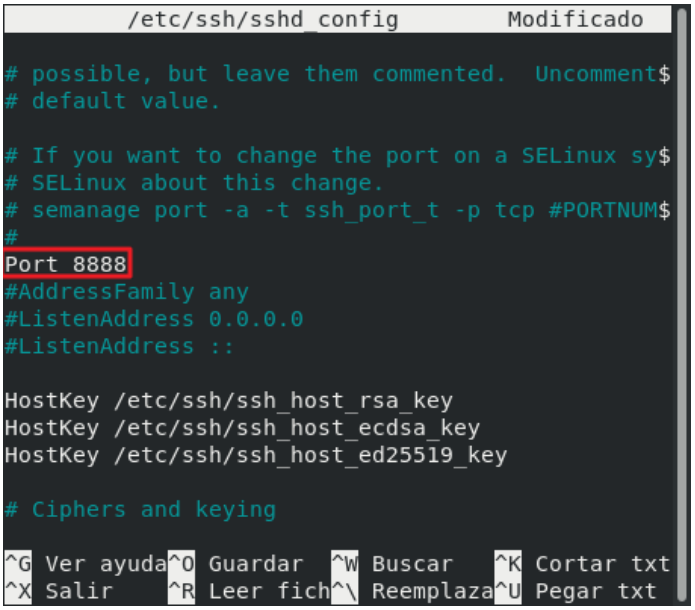
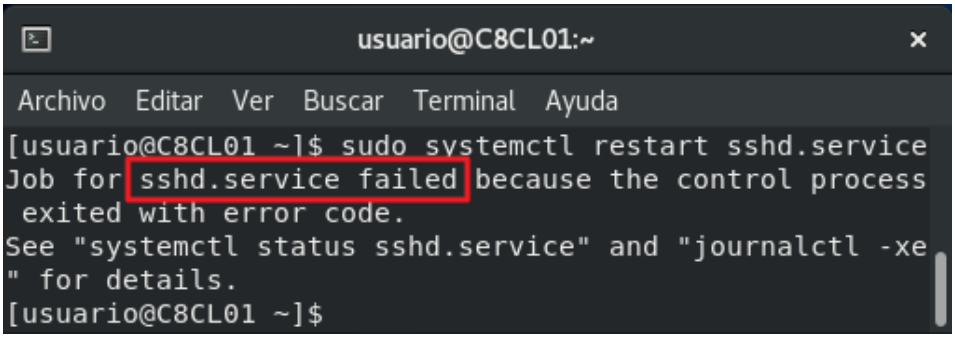
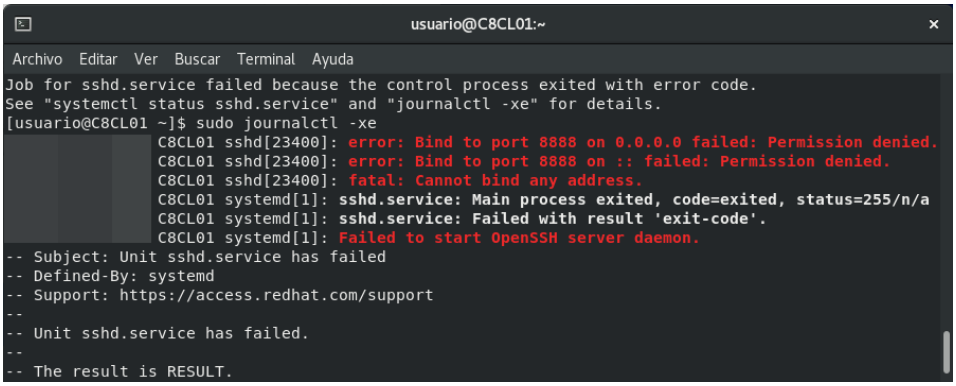
ANEXO A.6.3. CONFIGURACIÓN ADICIONAL DE SEGURIDAD - SELINUX

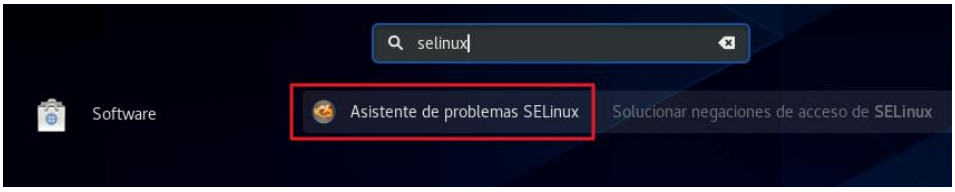
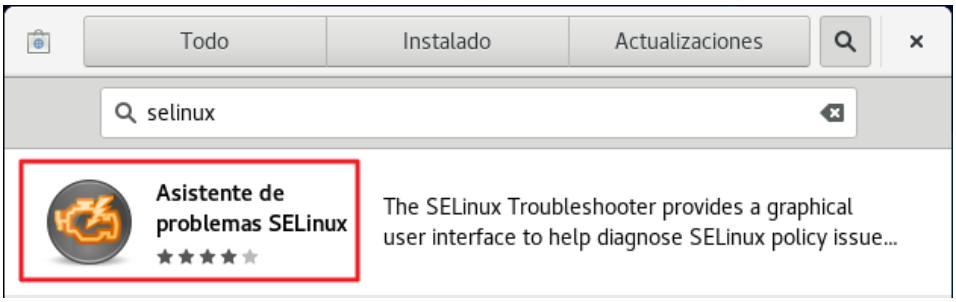
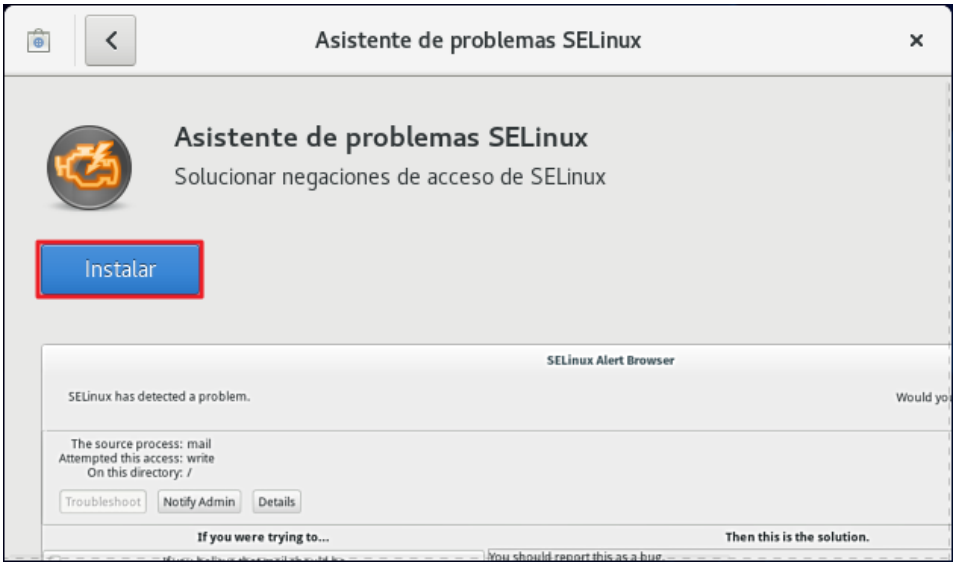
Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Se va a proceder a revisar el estado de SELinux, así como su configuración.
4.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen. 

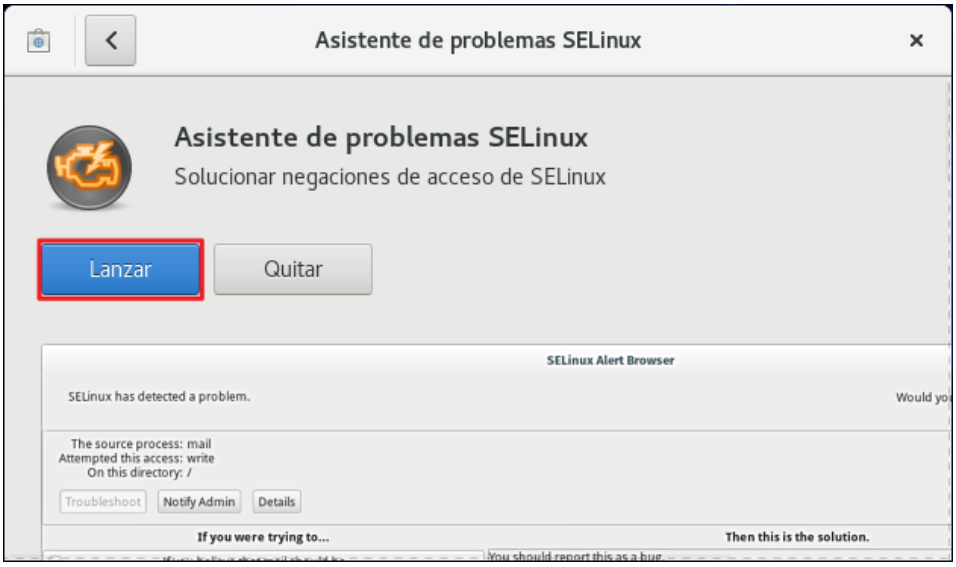
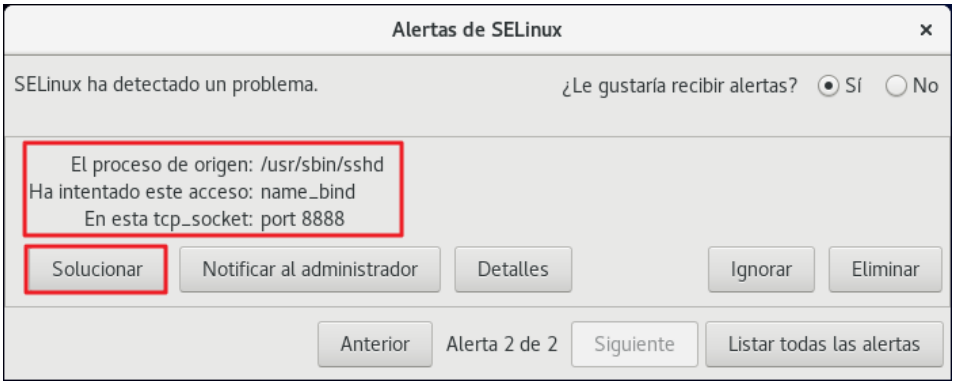
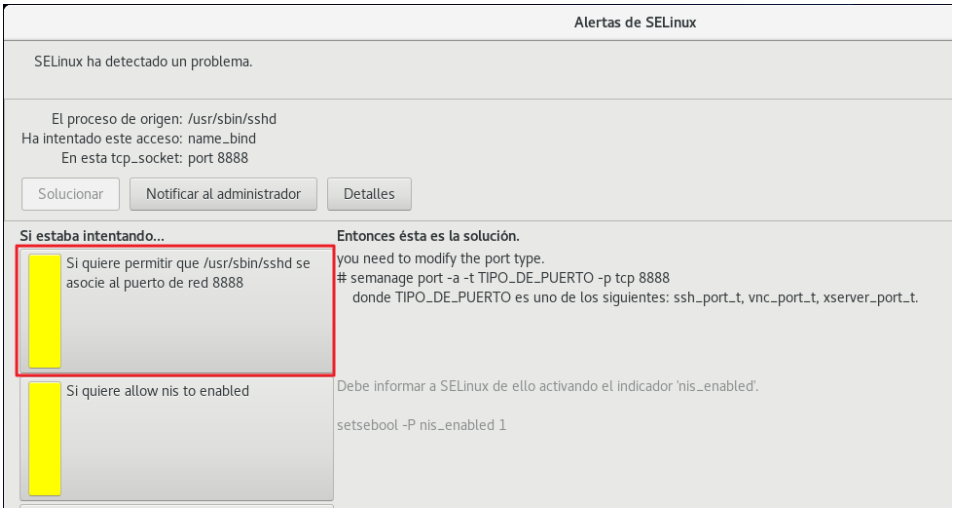
Paso	Descripción
5.	Ejecute el comando "**cd /**" y pulse la tecla "Enter".
6.	Se va a proceder a activar SELinux y configurarlo para que registre los eventos del sistema. Edite el fichero de configuración "/etc/selinux/config" y modifique los siguientes parámetros: SELINUX=Enforcing, SELINUXTYPE=targeted. **$ sudo nano /etc/selinux/config**  **Nota:** Se comentan a continuación algunos parámetros del fichero de configuración: - SELINUX=enforcing La opción SELINUX pone el modo en el que inicia SELinux. SELinux tiene tres modos: obligatorio (enforcing), permisivo (permissive) y deshabilitado (disabled). Cuando se usa modo obligatorio, la política de SELinux es aplicada y SELinux deniega el acceso basándose en las reglas de políticas de SELinux. Los mensajes de denegación se guardan. Cuando se usa modo permisivo, la política de SELinux no es obediente. Los mensajes son guardados. SELinux no deniega el acceso, pero se guardan las denegaciones de acciones que hubieran sido denegadas si SELinux estuviera en modo obediente. Cuando se usa el modo deshabilitado, SELinux está deshabilitado (el módulo de SELinux no se registra con el kernel de Linux). - SELINUXTYPE=targeted La opción SELINUXTYPE selecciona la política a usar por SELinux. La política Destinada es la predeterminada. Cambie esta opción si quiere usar la política MLS. Para usar la política MLS, instale el paquete selinux-policy-mls; configure SELINUXTYPE=mls en /etc/selinux/config; y reinicie su sistema.

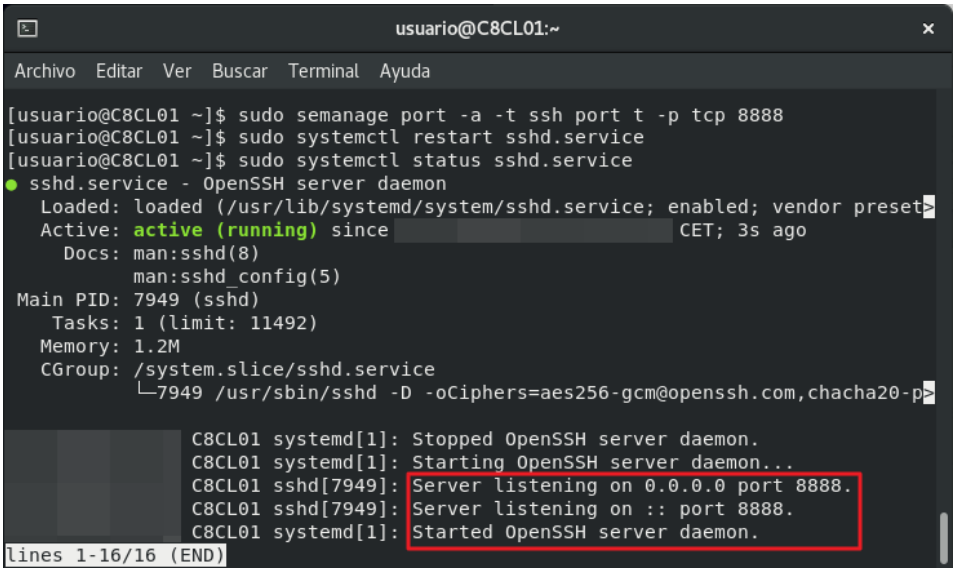
Paso	Descripción
7.	Para comprobar el estado de SELinux ejecute los siguientes comandos. **$ sudo getenforce** **$ sudo sestatus**  Compruebe que SELinux se encuentre configurado como “enforcing”, “enabled” y “targeted”. En caso contrario repita los pasos anteriores.
8.	Posteriormente se van a listar los booleanos activos y desactivados de SELinux. Revise los booleanos para configurarlos de la manera más conveniente a su organización, para ello ejecute el siguiente comando. **$ sudo semanage boolean -l**  **Nota:** Los booleanos permiten cambiar partes de la política de SELinux en tiempo de ejecución, sin ningún conocimiento sobre la escritura de políticas de SELinux. Esto permite cambios, como permitir el acceso de servicios a sistemas de archivo NFS, sin recargar o recompilar la política de SELinux. Ejecute el comando “getsebool [nombre-de-booleano]” para listar solamente el estado del booleano “[nombre-de-booleano]” sin descripción.

Paso	Descripción
9.	Se va a realizar un ejemplo para cambiar el puerto de escucha por defecto del servidor ssh y como configurarlo y permitirlo en SELinux. Se listan los booleanos pertenecientes a ssh con el siguiente comando. **$ sudo getsebool -a |grep "ssh"**  Habilite las políticas que más convengan a su organización. La sintaxis del comando sería la siguiente. **$ sudo setsebool [1|0] [booleano]** La sintaxis del comando para habilitar un booleano de manera permanente es la siguiente. **$ sudo setsebool -P [booleano] 1** **Nota:** A continuación, se describen una serie de políticas - Política fenced_can_ssh. Permite a usuarios con "chroot" poder ingresar también a través de SSH - Política selinuxuser_use_ssh_chroot. Se establece para usuarios confinados de SELinux (por ejemplo, guest_u, staff_u o user_u). - Política ssh_chroot_rw_homedirs. Habilita los atributos lectura y escritura de archivos en los directorios de inicio de los usuarios con chroot. - Política allow_ssh_keysign. Habilita el uso de firmas digitales. - Política ssh_sysadm_login. Habilita el acceso a usuarios con rol de administrador de sistema (contextos sysadm_r:sysadm_t). - Política ssh_use_tcpd. Habilita el uso de tcp Wrappers para el servidor ssh.

Paso	Descripción
10.	Se procede a cambiar el puerto predeterminado del servidor ssh y reiniciar el servicio. Ejecute los siguientes comandos. **$ sudo nano /etc/ssh/sshd_config**  Ahora reinicie el servicio y observe que se produce un error. **$ sudo systemctl restart sshd.service** 
11.	Revise journalctl para revisar los logs generados por el servicio. **$ sudo journalctl -xe** 

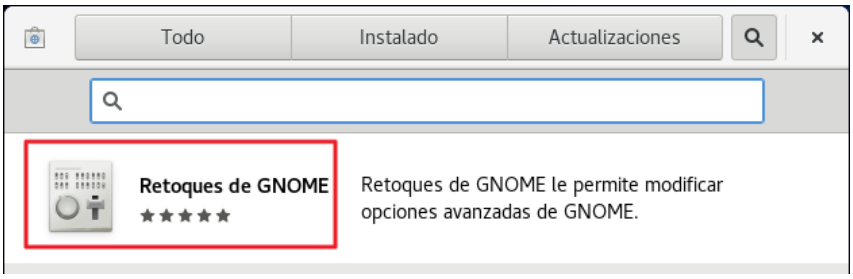
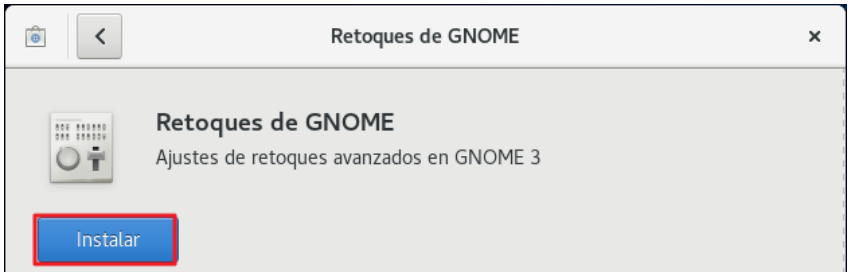
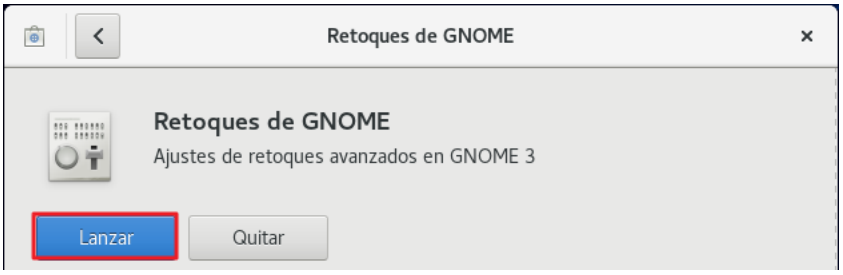
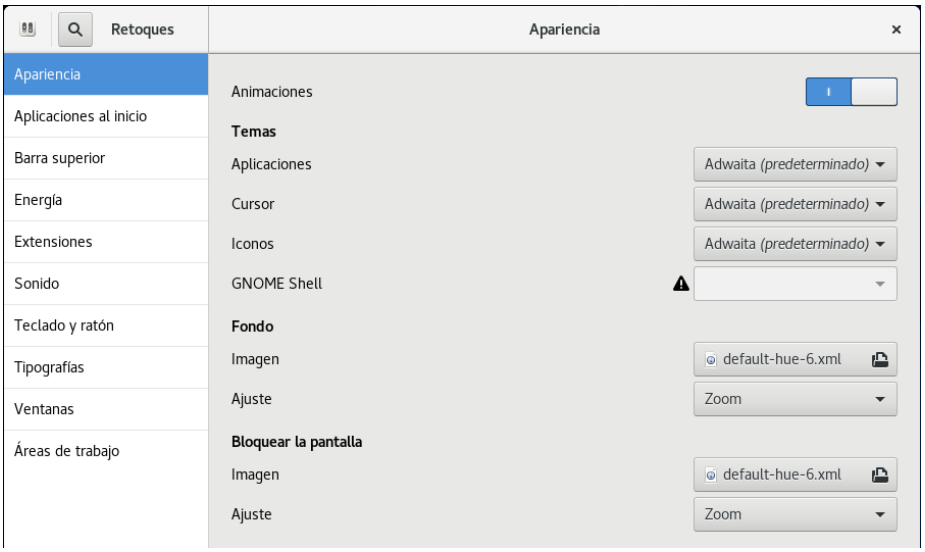
Paso	Descripción
12.	En este punto se recomienda instalar la herramienta gráfica “Asistente de problemas SELinux”. Para ello vaya a la barra superior de tareas, pulse sobre “Actividades” y en la barra de búsqueda escriba “selinux”. Pulse sobre el icono de “Asistente de problemas SELinux” para proceder a su instalación. 
13.	Se abrirá la herramienta “software” donde deberá pulsar nuevamente sobre el icono de “Asistente de problemas SELinux”. 
14.	Posteriormente pulse sobre el icono “Instalar”. 

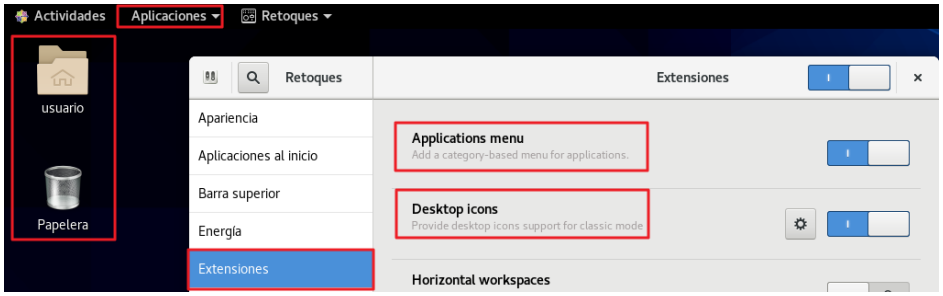
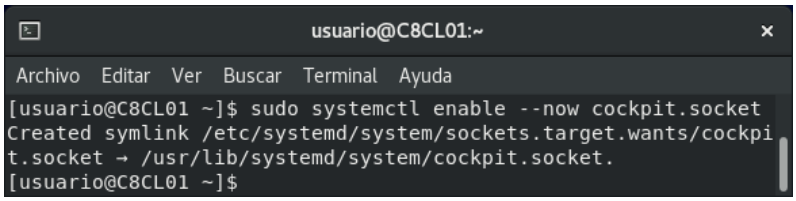
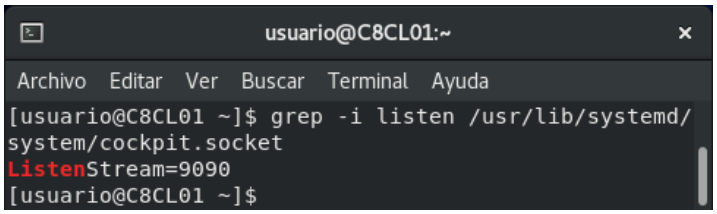
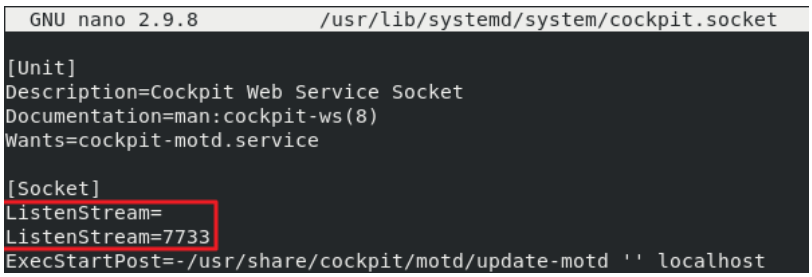
Paso	Descripción
15.	Cuando finalice, pulse sobre el icono “Lanzar”. 
16.	Si revisa las alertas, una de ellas será la referente al cambio de puerto de SSH. Pulse en el botón “Solucionar”. 
17.	Seleccione el apartado “Si quiere permitir que /usr/sbin/sshd se asocie al puerto de red 8888”. 

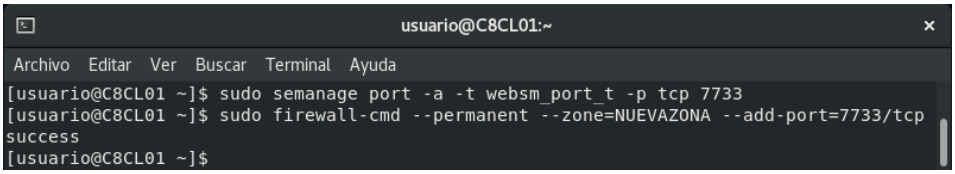
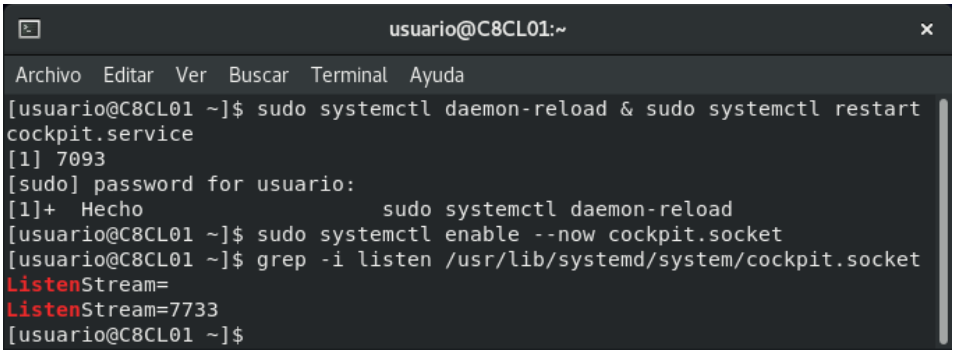
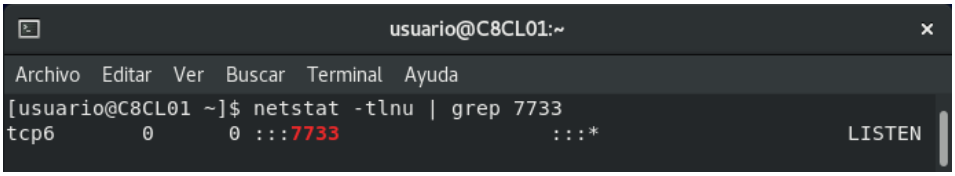
Paso	Descripción
18.	Ejecutaremos la solución que propone SELinux para asociar el puerto 8888 al demonio ssh. Para ello ejecute el siguiente comando. **$ sudo semanage port -a -t ssh_port_t -p tcp 8888** Compruebe que el servicio de ssh se activa permitiendo que la configuración del puerto predeterminado para el mismo sea el 8888. **$ sudo systemctl restart sshd.service** **$ sudo systemctl status sshd.service** 

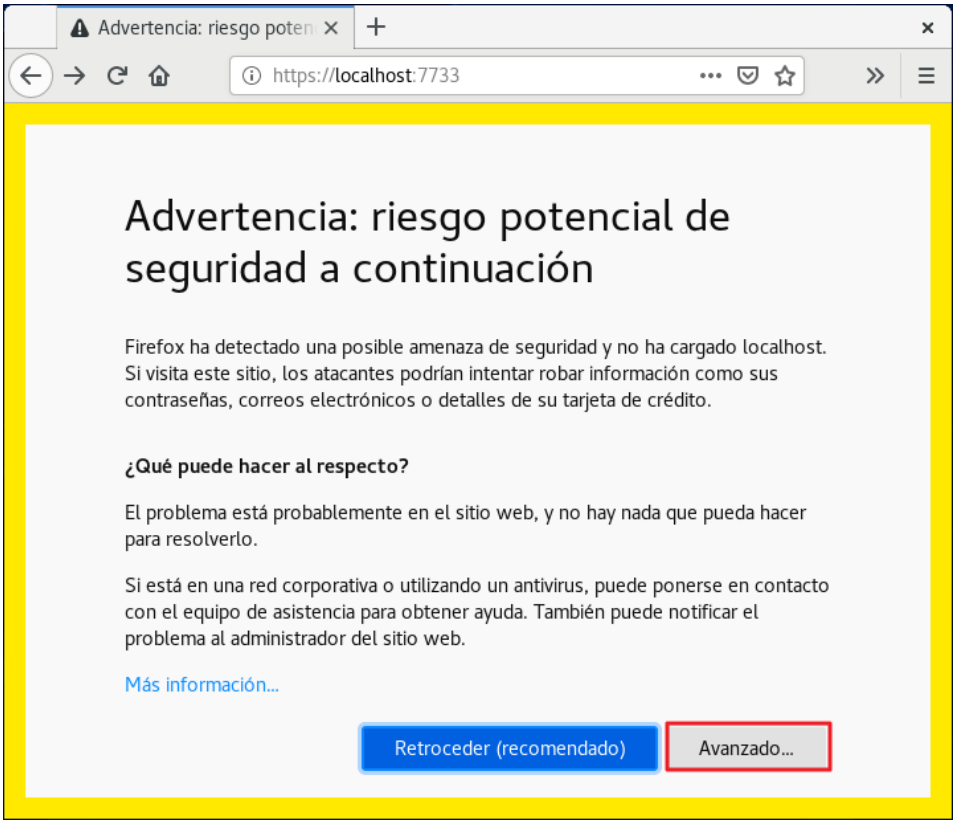
ANEXO A.6.4. INTERFAZ DE USUARIO E INTERFAZ WEB COCKPIT

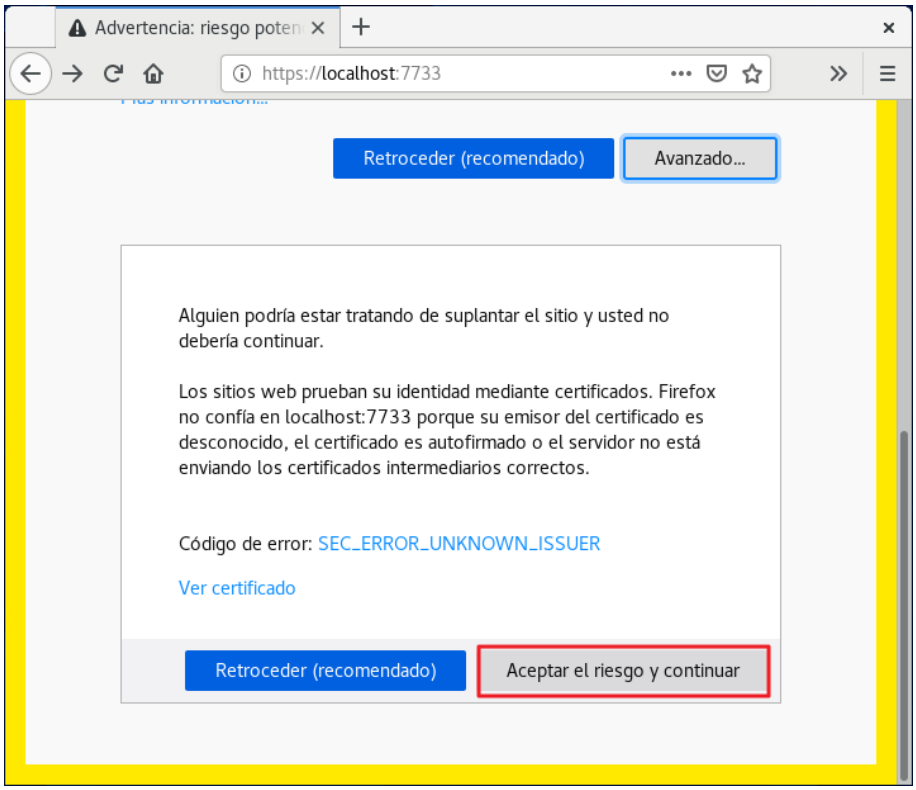
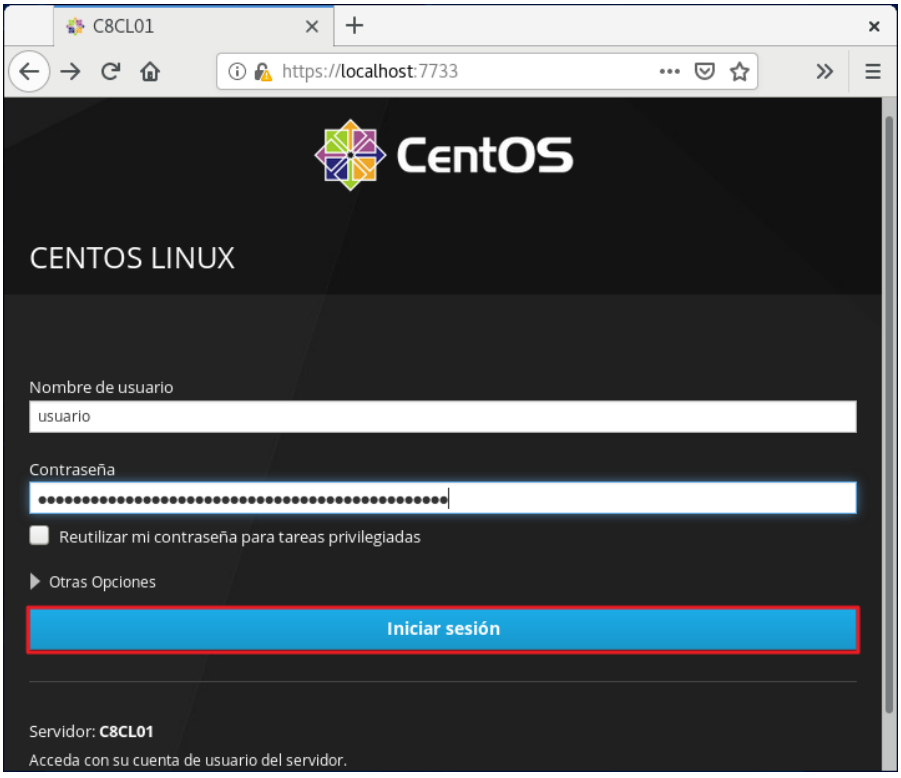
Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Este punto se centra en la modificación del interfaz de usuario por medio de la herramienta “Retoques de GNOME”.
4.	Se recomienda instalar la herramienta gráfica “Retoques de GNOME”. Para ello vaya a la barra superior de tareas, pulse sobre “Actividades” y en la barra de búsqueda escriba “retoques”. Pulse sobre el icono de “Retoques de GNOME” para proceder a su instalación. 

Paso	Descripción
5.	Se abrirá la herramienta “software” donde deberá pulsar nuevamente sobre el icono de “Retoques de GNOME”. 
6.	Posteriormente pulse sobre el icono “Instalar”. 
7.	Cuando finalice, pulse sobre el icono “Lanzar”. 
8.	Se abrirá la herramienta de Apariencia de GNOME. Modifique la apariencia del escritorio acorde a las necesidades específicas de su organización.  **Nota:** Se recomienda deshabilitar toda funcionalidad innecesaria para su organización

Paso	Descripción
9.	Si se dirige al apartado “Extensiones” y habilita los interruptores correspondientes con “Applications menu” y “Desktop icons”, se facilitará el acceso a aplicaciones y los iconos del escritorio tal y como se mostraba en versiones anteriores de CentOS Linux. 
10.	Por último, se va a configurar el entorno web cockpit de forma segura. Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente a la terminal.
11.	Ejecute el siguiente comando para habilitar la funcionalidad cockpit. **$ sudo systemctl enable --now cockpit.socket** 
12.	Compruebe el puerto de escucha de cockpit por medio del siguiente comando. **$ grep -i listen /usr/lib/systemd/system/cockpit.socket** 
13.	Para modificar el puerto de escucha al que más convenga para su organización, ejecute el siguiente comando y edite el fichero “cockpit.socket”. Modifique el campo “ListenStream” por el valor correspondiente al nuevo puerto de escucha dejando el mismo parámetro justo encima sin valor, tal y como se muestra en la siguiente imagen. Cierre y guarde el fichero cuando finalice. **$ sudo nano /usr/lib/systemd/system/cockpit.socket** 

Paso	Descripción
14.	Ejecute los siguientes comandos para que SELinux y firewalld permitan el uso de ese puerto para el interfaz web. **$ sudo semanage port -a -t websm_port_t -p tcp [PUERTO ELEGIDO]** **$ sudo firewall-cmd --permanent --zone=[ZONA HABILITADA] --add-port=[PUERTO ELEGIDO]/[PROTOCOLO]** **$ sudo firewalld-cmd --reload** 
15.	Deberá reiniciar el demonio y comprobar de nuevo el puerto de escucha. Para ello ejecute los siguientes comandos. Introduzca la contraseña si se le solicita. **$ sudo systemctl daemon-reload & sudo systemctl restart cockpit.service** **$ sudo systemctl enable --now cockpit.socket** **$ grep -i listen /usr/lib/systemd/system/cockpit.socket** 
16.	Compruebe que el puerto se encuentra correctamente a la escucha por medio del siguiente comando. **$ netstat -tlnu | grep [PUERTO ELEGIDO]**  **Nota:** Si el puerto que ha elegido no se encuentra a la escucha y por tanto no se muestran resultados por pantalla cuando se ejecuta el comando, vuelva a reiniciar el servicio por medio del siguiente comando. - sudo systemctl restart cockpit.service

Paso	Descripción
17.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente al navegador “Firefox”, tal y como se muestra en la imagen. 
18.	Diríjase a la siguiente URL https://localhost:[PUERTOELEGIDO]. Allí le advertirá de riesgo potencial de seguridad puesto que el certificado es autogenerado por el sistema operativo y no uno correctamente firmado por una entidad certificadora. Pulse en en botón “Avanzado…” para continuar.  **Nota:** Se recomienda la utilización de certificados correctamente emitidos desde una entidad certificadora de confianza.

Paso	Descripción
19.	Posteriormente en “Aceptar el riesgo y continuar”. 
20.	Se mostrará el interfaz de inicio de cockpit, donde deberá introducir las credenciales de su usuario y pulsar en el botón “Iniciar sesión”. 

Paso	Descripción
21.	Se mostrará el panel de cockpit para la administración y monitorización del sistema.