centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 617

IMPLEMENTACIÓN DE SEGURIDAD SOBRE SUSE ENTERPRISE 12 SP3 LINUX (SERVIDOR INDEPENDIENTE)

ABRIL 2019

MINISTERIO DE DEFENSA

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: 083-19-155-8
Fecha de Edición: abril de 2019

La Jefatura de Servicios Técnicos y CIS del Ejército del Aire, junto con las empresas Sellcom Solutions y Sidertia Solutions S.L. han participado en la realización del presente documento, siendo esta última, la que ha realizado los anexos y la modificación del documento original.

PRÓLOGO

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

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

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

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

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

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

abril de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE SUSE ENTERPRISE 12 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 SUSE Linux Enterprise Server 12 SP3 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 SUSE Linux Enterprise Server 12 SP3 de la distribución, con la opción de instalación "Default system" 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 los entornos de escritorio GNOME o KDE, 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 "Default system" de SUSE Linux Enterprise Server 12 SP3 permite garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con SUSE Linux Enterprise Server 12. 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 SUSE Linux Enterprise Server 12 SP3. 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 SUSE Linux Enterprise Server 12 ya implementados que deseen crear una unidad o partición adicional cifrada.

c) AppArmor es una aplicación y herramienta de seguridad incluida en el paquete SUSE Enterprise Server Linux diseñada para proveer una protección de fácil uso para tus aplicaciones. AppArmor protege proactivamente el sistema operativo y las aplicaciones de amenazas externas o internas inclusive ataques "zeroday" implementando un buen funcionamiento e impidiendo inclusive fallos desconocidos de ser explotados. Las políticas de seguridad de AppArmor (Perfiles) definen que recursos del sistema y privilegios pueden acceder las aplicaciones. AppArmor incluye perfiles predeterminados que usan una combinación de análisis estático avanzado y herramientas basadas en aprendizaje; por esta razón pueden colocarse en las aplicaciones más complejas en cuestión de horas.

d) AppArmor está formado por:

   i. Un módulo de kernel comunicado con el kernel de SUSE Enterprise Server Linux que implementa los perfiles de seguridad.

   ii. Un conjunto de perfiles de AppArmor para numerosos programas que se comunican con SUSE Enterprise Server Linux.

   iii. Herramientas para crear y operar nuevos perfiles.

   iv. Una interfaz de usuario YaST para operar reportes y notificaciones de eventos de seguridad.

   v. Documentación acerca de las herramientas.

e) 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.

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE SUSE LINUX ENTERPRISE SERVER 12 PARA ENS

1. APLICACIÓN DE MEDIDAS EN SUSE LINUX ENTERPRISE SERVER 12

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de servidores con SUSE Linux Enterprise Server 12 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.

Nota: Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará usó de la aplicación de medidas de seguridad descritas en el "ANEXO A.5 CATEGORÍA ALTA / DIFUSIÓN LIMITADA".

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

a) Aplicación de seguridad en servidores independientes, donde se realizará la ejecución de aplicaciones o el tratamiento de información sujetos al RD 3/2010 y se encontraran implementados con SUSE Linux Enterprise Server 12.

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 SUSE Linux Enterprise Server 12, 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 (apartado SECURITY POLICY) 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 SUSE Linux Enterprise Server 12 vienen implementadas por el propio Sistema Operativo a través del software AppArmor. 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 las categorías 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 las diferentes categorías 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 a la categoría exigida. Así en la categoría básica se prima la comodidad y en la categoría alta 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 SUSE Linux Enterprise Server 12, 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 SUSE Linux Enterprise Server 12. 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 SUSE Linux Enterprise Server 12 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, SUSE Linux Enterprise Server 12 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 las diferentes categorías 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://www.suse.com/documentation/sles-15/book_sle_admin/data/sec_adm_sudo_usage.html

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 - DL, 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 categorías, 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.

SUSE Linux Enterprise Server 12 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, 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 de la categoría 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 – DL 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.

SUSE Linux Enterprise Server 12 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 de la categoría 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.

SUSE Linux Enterprise Server 12 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.

SUSE Linux Enterprise Server 12 es un sistema de código libre con licencia 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 categorías. 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 SUSE Linux Enterprise Server 12. 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 SUSE Linux Enterprise Server, 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 SUSE Linux Enterprise Server ofrece ciclos de actualizaciones de 13 años (10 años de asistencia general y 3 años de asistencia extendida). No debe confundir no obstante dichas actualizaciones de funcionalidad con las actualizaciones tradicionales de seguridad, sin embargo, SUSE Linux Enterprise Server 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 la funcionalidad "zypper lp --category 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 zypper 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 SUSE Linux Enterprise Server 12 están preconfiguradas para utilizar tres de estos repositorios:

      – Base. Los paquetes que conforman un lanzamiento de SUSE Linux Enterprise Server, 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 SUSE Linux Enterprise Server, 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 SUSE Linux Enterprise Server 12.

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 SUSE Linux Enterprise Server 12 venga provisto de un Firewall y la opción de implementar SELinux, estos no cubren todo el espectro de protección frente a código dañino. Por ejemplo, sin una solución de administración central no tendrá la visibilidad para hacer 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 básicas, 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 - DL requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

SUSE Linux Enterprise Server 12, 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.

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

En las categorías medias y altas se deberán implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:

a) Determinar el período de retención de los registros.

b) Asegurar 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 dispuestos 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 - DL, 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 riesgos 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 de 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 categorías altas - DL de información en el RD 3/2010. SUSE Linux Enterprise Server en su versión 12 SP3 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 de 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.

https://www.suse.com/documentation/sles-12/book_security/data/ sec_security_firewall_suse.html

Nota: Aunque se proporciona una configuración base de SuSEFirewall2 de SUSE Linux Enterprise Server 12 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 una categoría alta - DL 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 SUSE LINUX ENTERPRISE SERVER 12

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
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 SUSE LINUX ENTERPRISE SERVER 12 por no cubrir este los

Control	Medida	Mecanismo de aplicación
		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. 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.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el 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
MP. EQ. 3	Protección de portátiles	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización, Se debe tomar en consideración que el cifrado proporcionado por SUSE LINUX ENTERPRISE SERVER 12 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 SUSE LINUX ENTERPRISE SERVER 12 por no cubrir éste los mínimos exigidos por el ENS para la confidencialidad de los datos.
MP. COM. 3	Protección del sistema mediante implementación de firewall.	Configuraciones adicionales descritas a través de la presente guía. Implementación de configuración de firewall a nivel local según el ANEXO A.6.1 de la presente guía.
MP. COM. 3	Protección de la autenticación.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
MP. SI. 2	Criptografía	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
MP. INFO. 3	Cifrado	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización

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

1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DEL GUI SUSE LINUX ENTERPRISE SERVER 12

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores SUSE Linux Enterprise Server 12 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.

Nota: Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará usó de la aplicación de medidas de seguridad descritas en el "ANEXO A.5 CATEGORÍA ALTA / DIFUSIÓN LIMITADA".

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 servidores SUSE Linux Enterprise Server 12, 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 SUSE Linux Enterprise Server 12 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 excepto el punto de montaje "/" que podrá encontrarse formateado en el sistema de archivos Btrfs.

b) El programa de instalación crea una propuesta para uno de los discos disponibles. Todas las propuestas contienen una partición raíz formateada con Btrfs (con las instantáneas habilitadas) y una partición de intercambio. Si ha seleccionado la función del sistema "Sistema por defecto", también se creará una partición de inicio formateada con XFS. En discos duros de menos de 20 GB, la propuesta no incluye una partición de inicio independiente. Si se detectan una o varias particiones de intercambio en los discos duros disponibles, serán las que se utilicen (en lugar de proponer una partición nueva al efecto).

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 SUSE Linux Enterprise Server 12 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 SUSE Linux Enterprise Server 12 no se requiere la existencia de particiones más allá de las que vienen por defecto, 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.

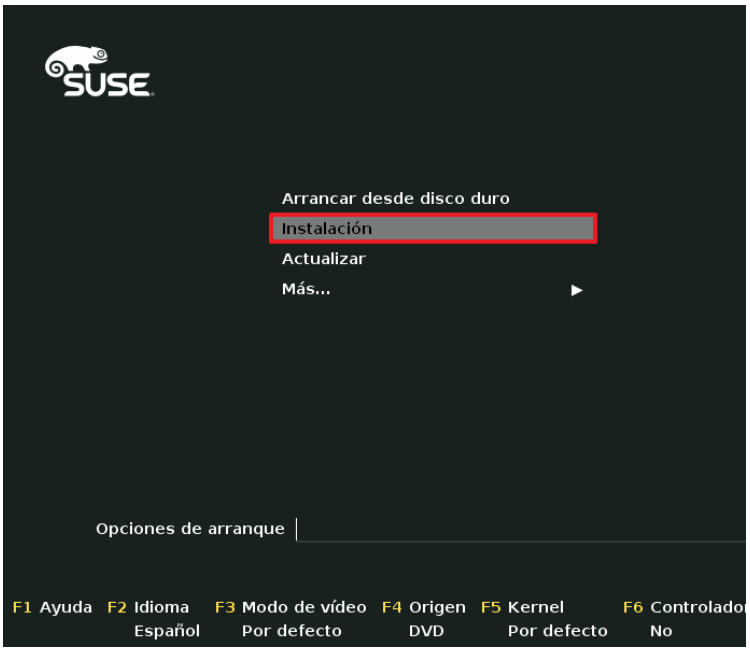
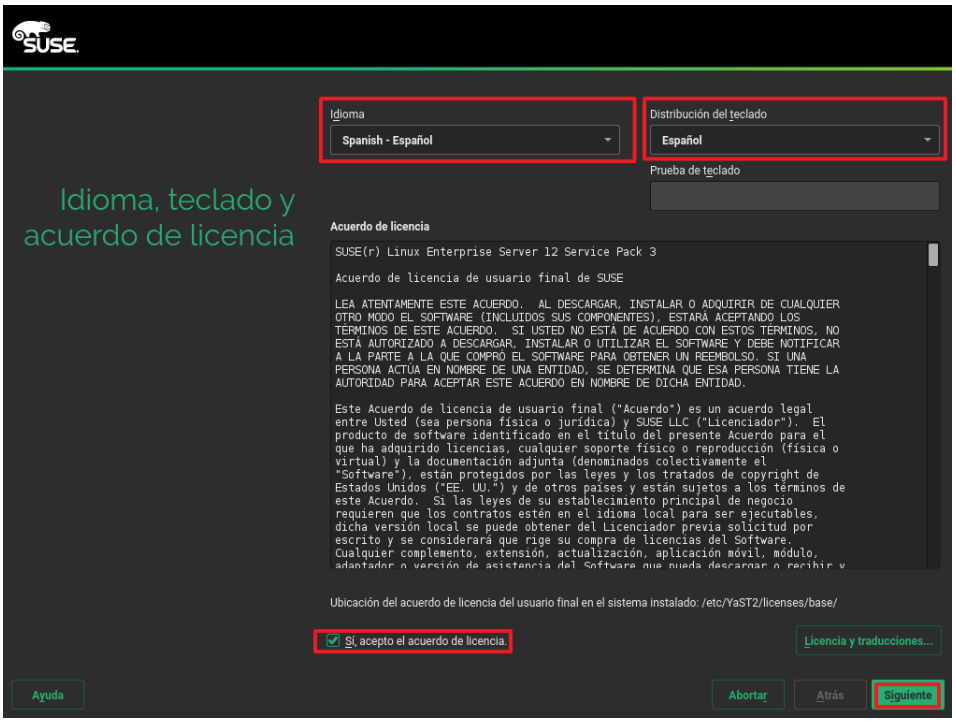
h) No instalar otros sistemas operativos en el equipo.

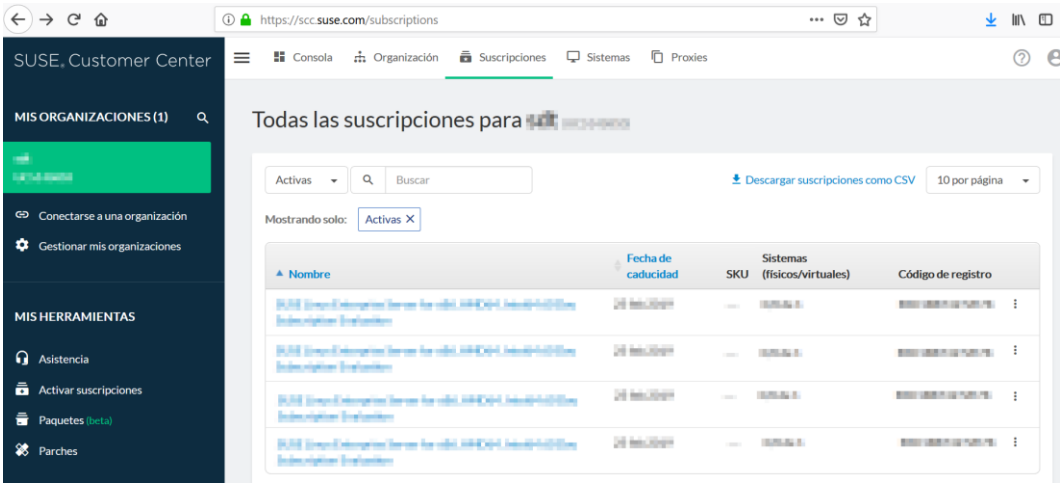
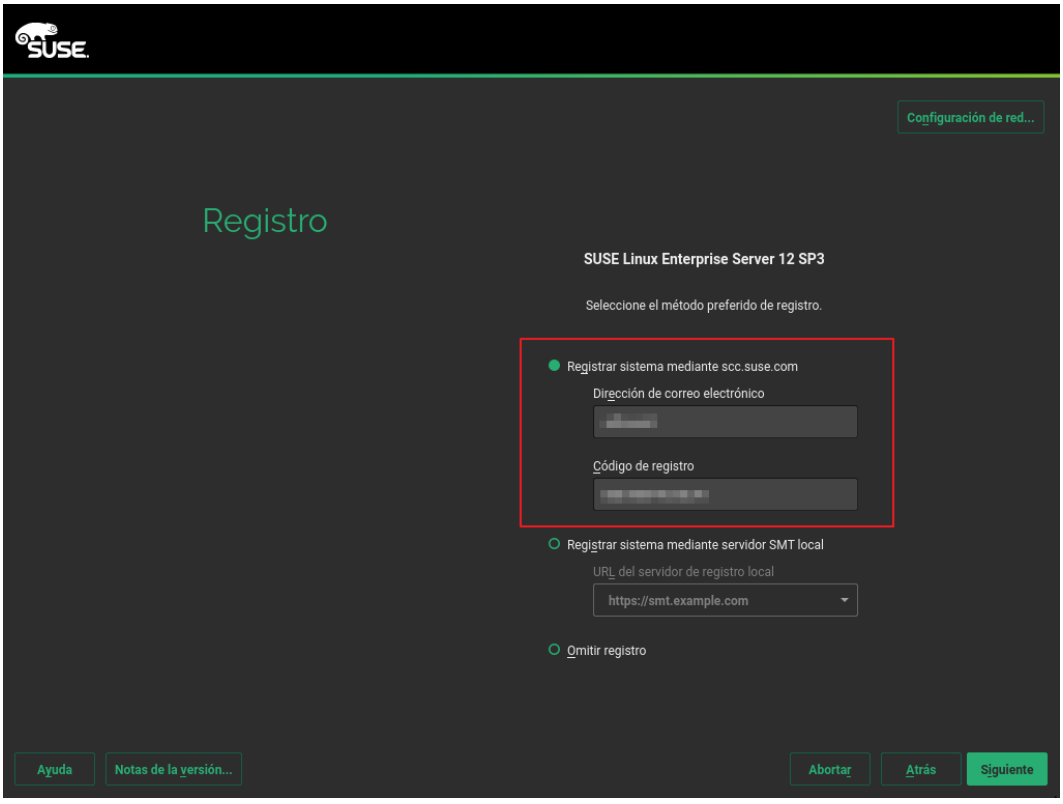
i) Asignar una contraseña compleja a la cuenta de usuario que se crea durante el proceso de instalación.

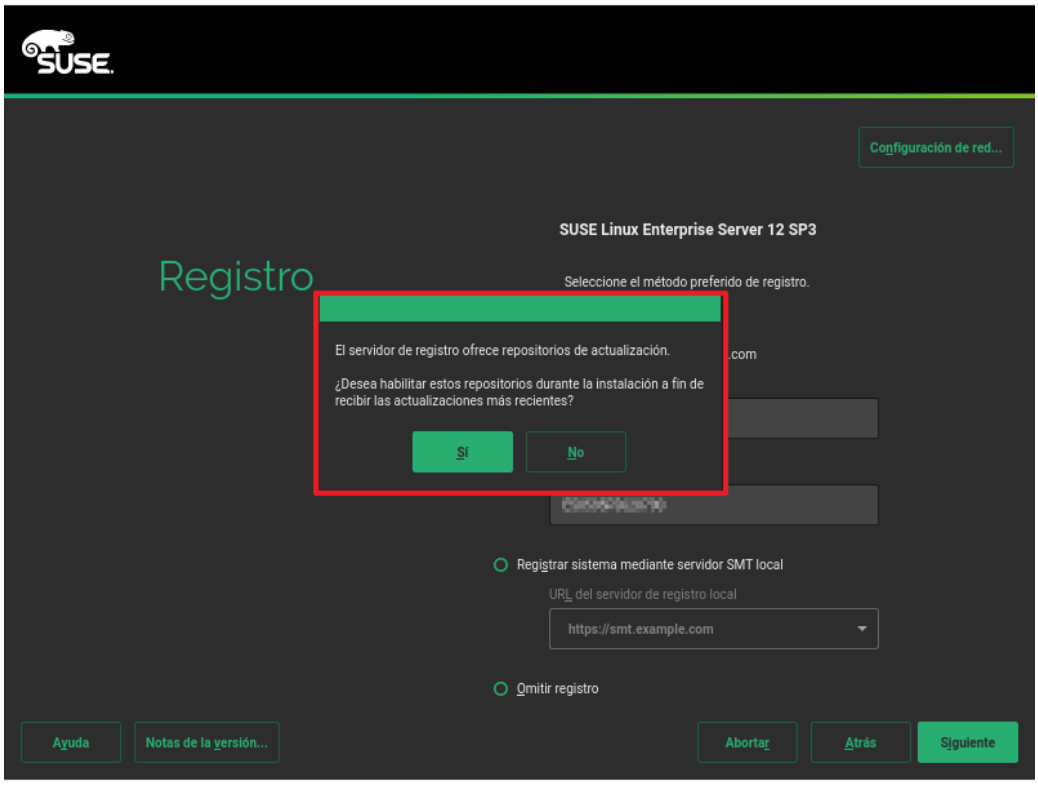
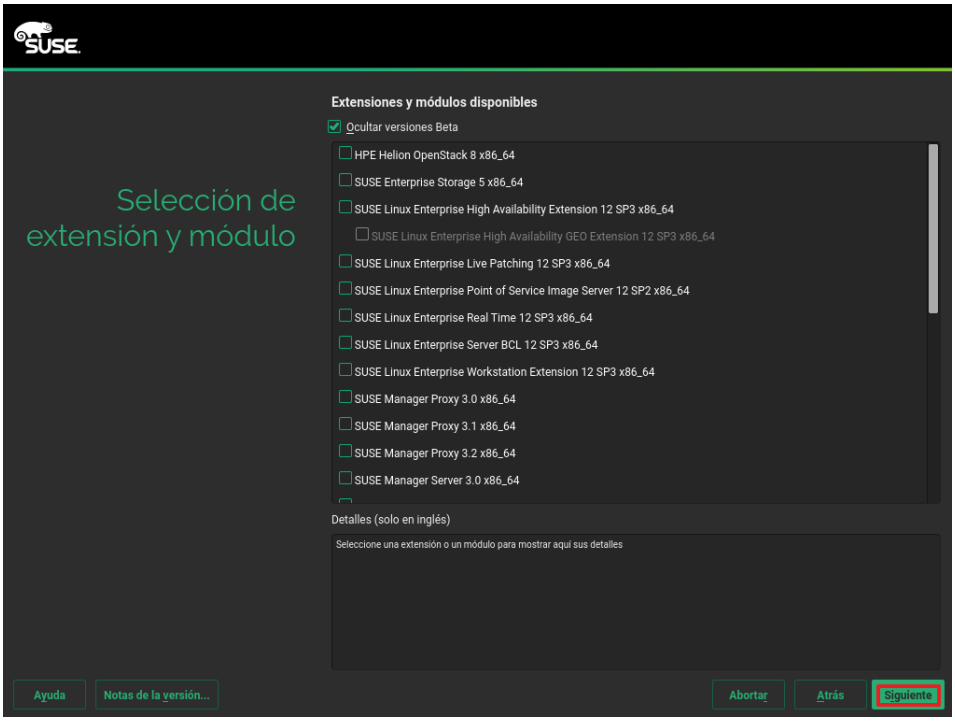
j) Una vez finalizada la instalación básica del sistema, asegurarse de que se instalan todas las actualizaciones de seguridad necesarias. Idealmente estas actualizaciones de seguridad se instalarán antes de conectar el equipo a la red o con el equipo conectado a una red segura.

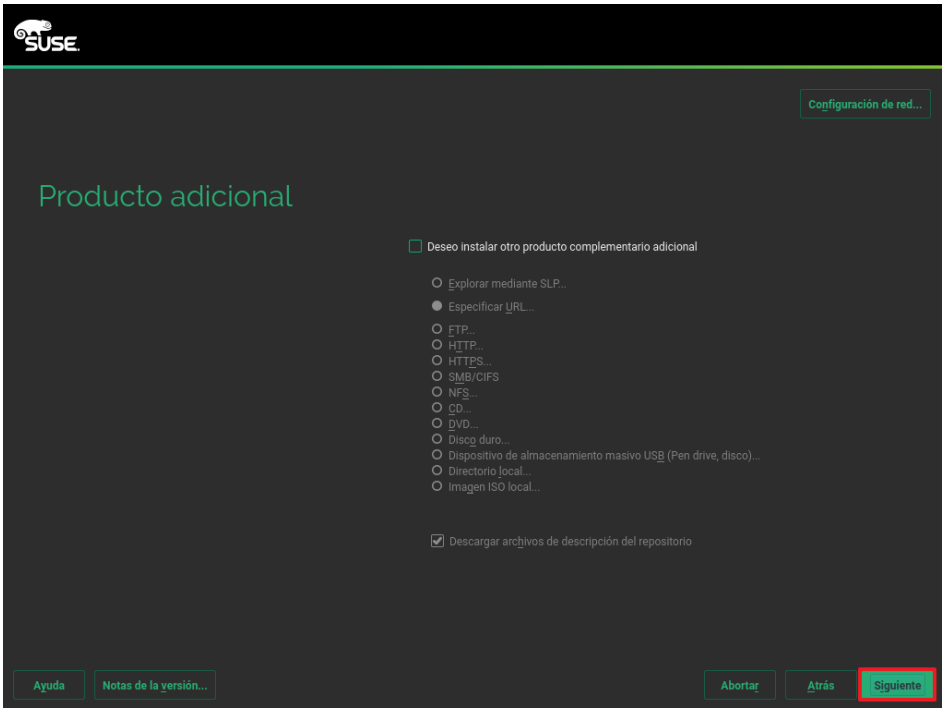
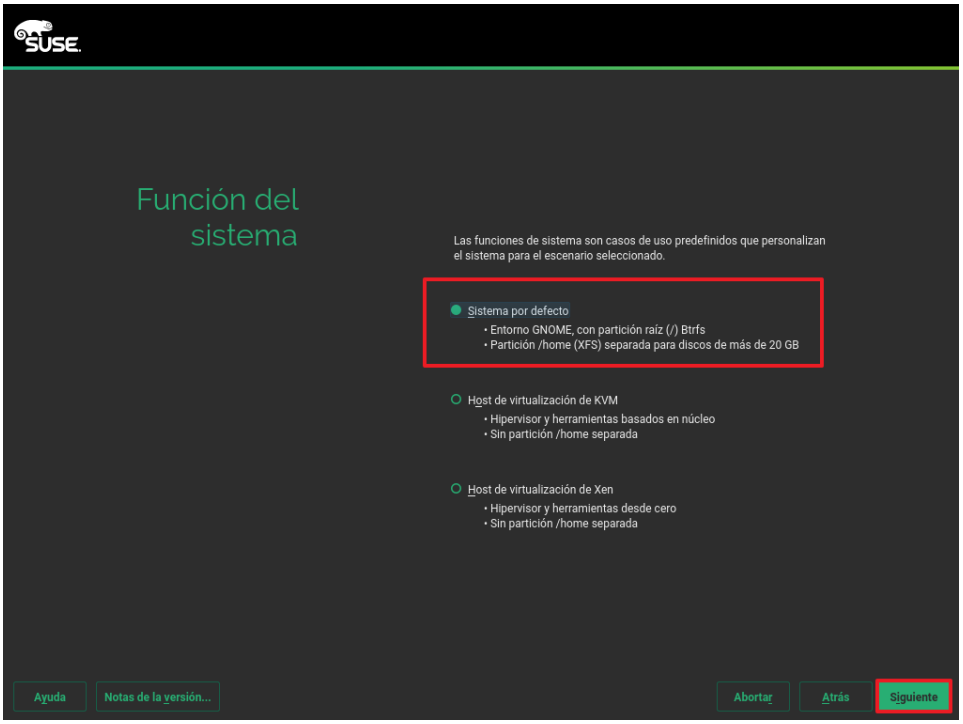
El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación.

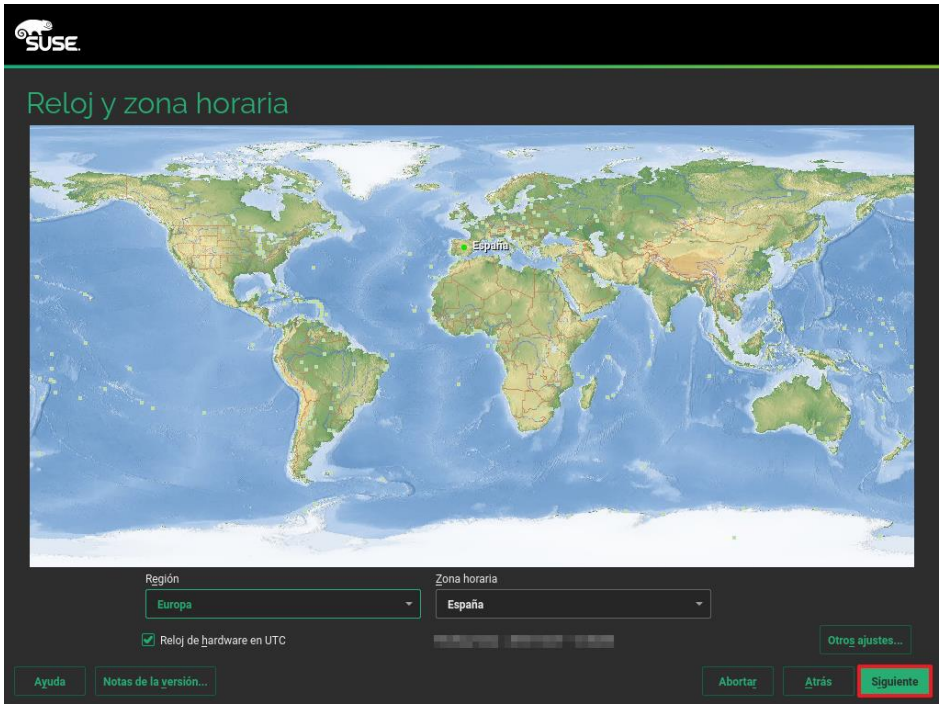
Paso	Descripción
1.	Introduzca el dispositivo USB o DVD de SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso y, si fuera necesario, reinicie la máquina para iniciar la instalación del sistema.
2.	Pulse “F2” para cambiar el idioma del menú de instalación y seleccione “Español”. 

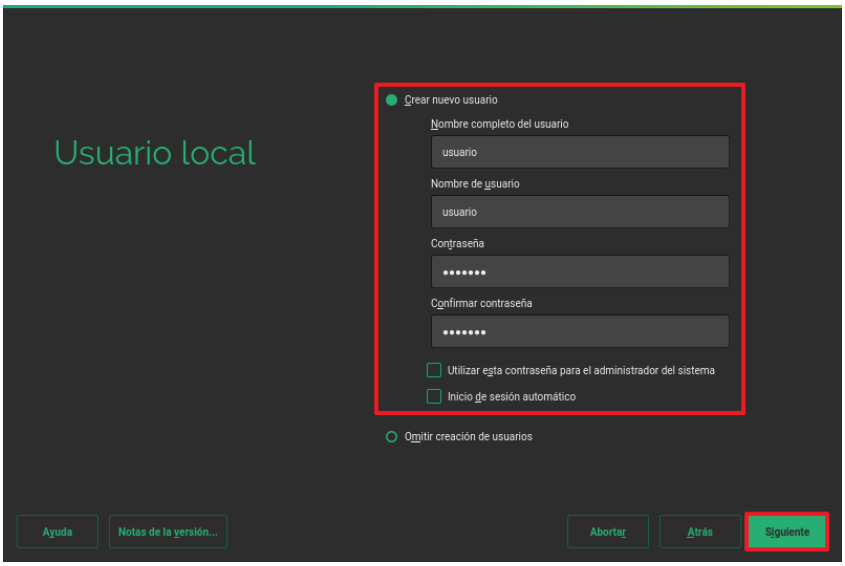
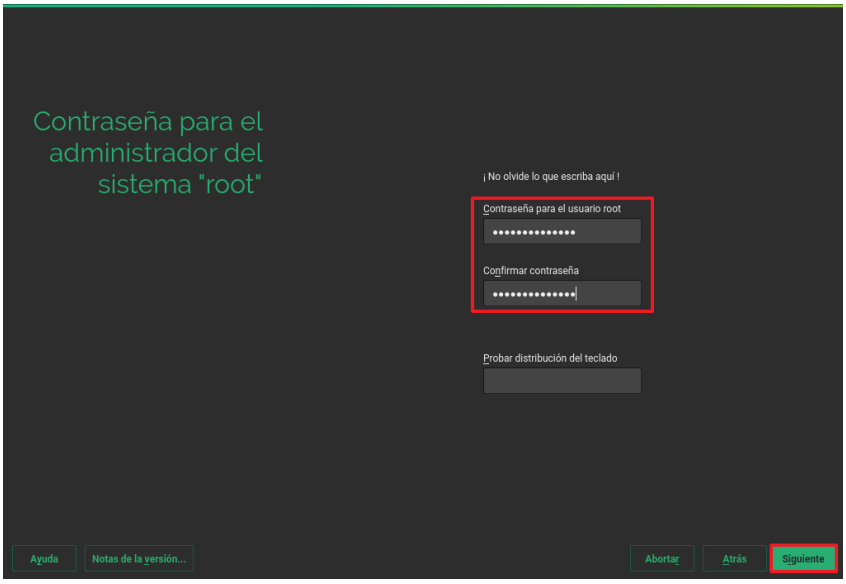
Paso	Descripción
3.	Cuando aparezca el menú de selección de inicio, pulse la tecla correspondiente a la flecha de dirección abajo, seleccione “Instalación” y pulse “Enter”. Si el equipo no se inicia desde el DVD revise los parámetros del BIOS.  **Nota:** No se debe pulsar ninguna tecla hasta que aparezca el menú de instalación. En caso contrario se podría iniciar la instalación sin modo gráfico. Si esto sucede, reinicie el ordenador y comience desde el paso 1.
4.	La instalación comenzará a actualizar el instalador, no pulse ninguna tecla hasta que aparezca el menú de selección de “idioma, teclado y acuerdo de licencia”. Seleccione idioma “Español”, acepte el acuerdo de licencia y pulse sobre el botón “Siguiente” para continuar. 

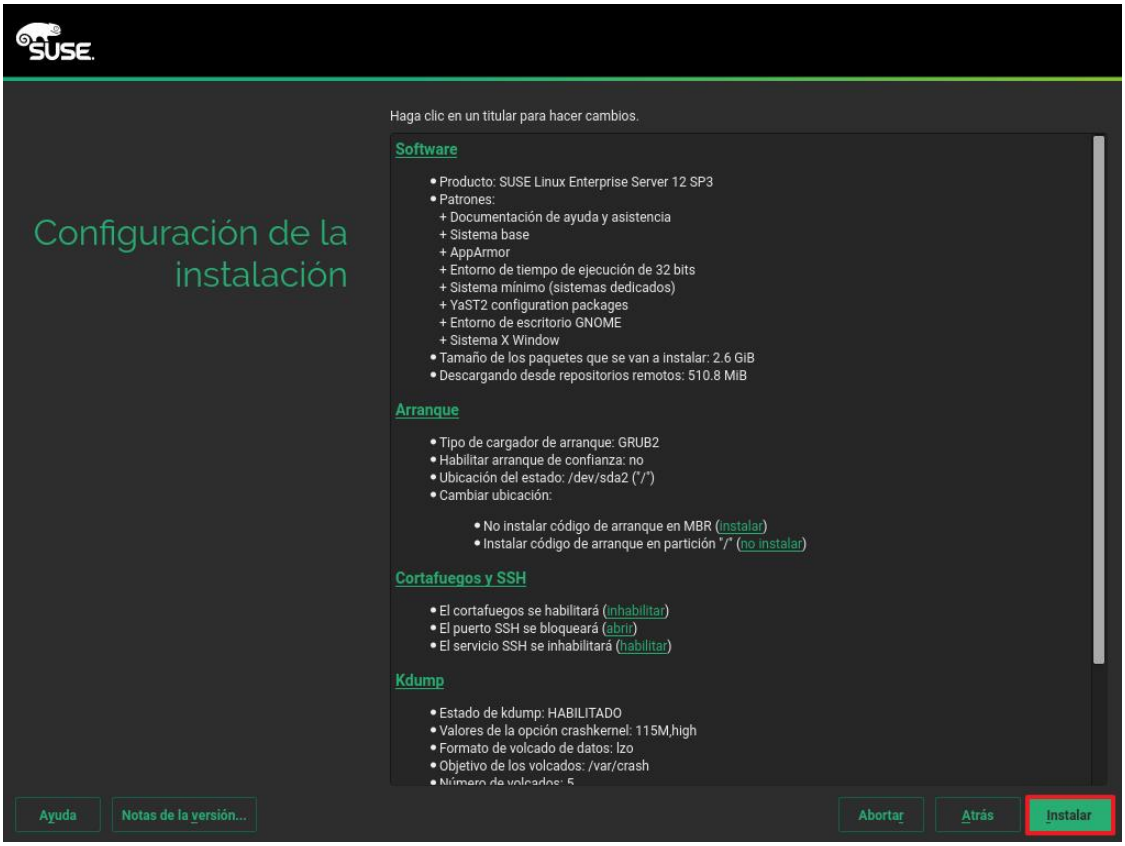
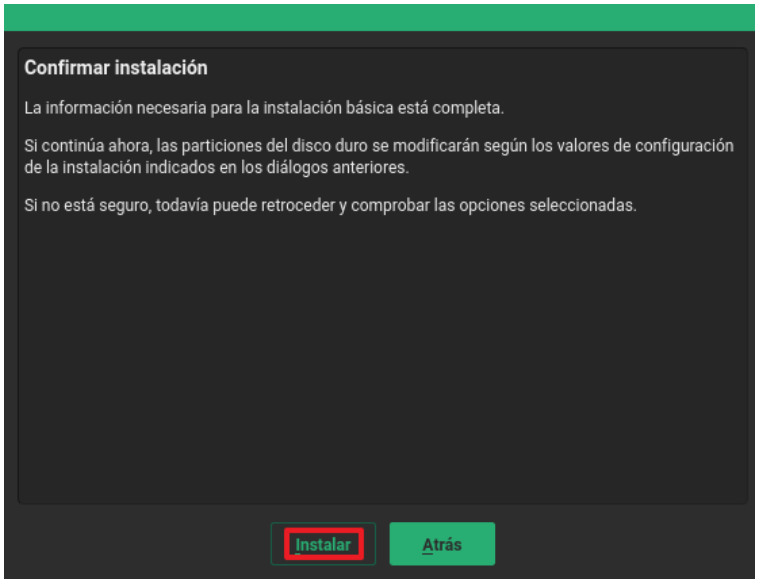
Paso	Descripción
5.	En el menú registro, se piden las credenciales de una subscripción válida y activa. Si posee una subscripción para el producto, puede recopilar los datos necesarios de la página web oficial de SUSE Linux en su “Customer Center”. 
6.	En el menú “Registro”, seleccione la opción “Registrar sistema mediante scc.suse.com”. E introduzca unas credenciales válidas. Una vez haya introducido unas credenciales válidas, pulse el botón “Siguiente” para continuar. 

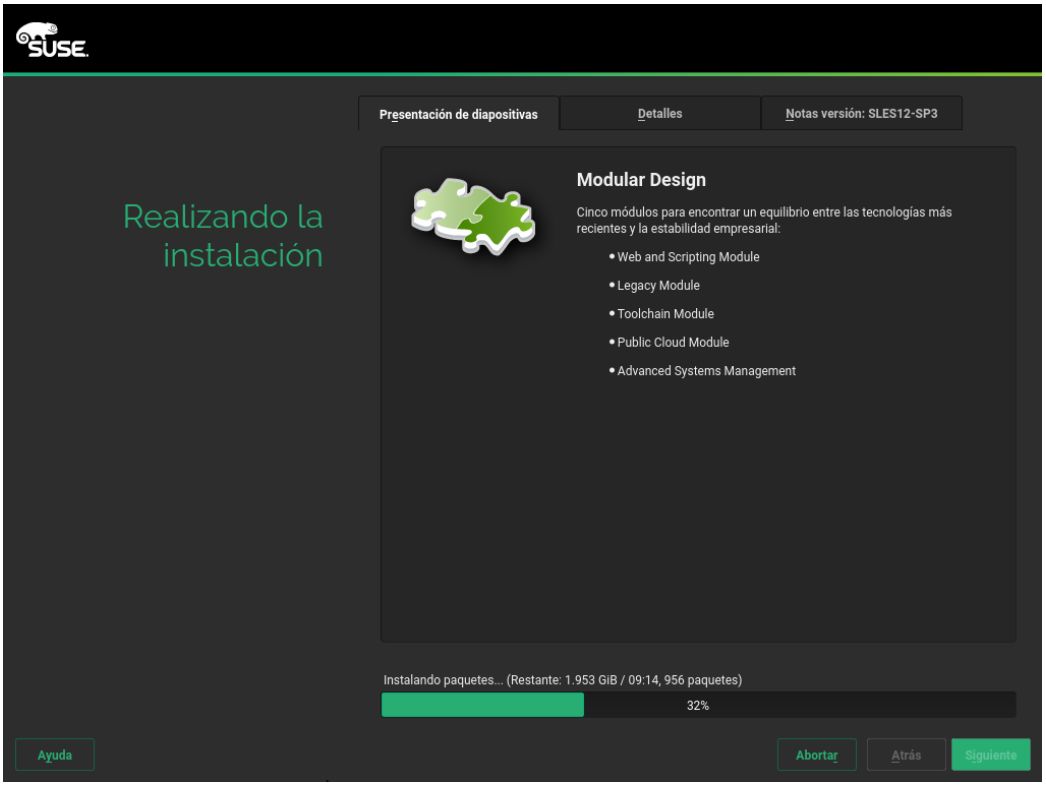
Paso	Descripción
7.	Se ofrecerá, en el servidor de registro una actualización de repositorios para la instalación. Seleccione la opción más acorde con la configuración de su organización. 
8.	Una vez se haya completado el registro, en el menú “Selección de extensión y módulo” seleccione las extensiones que sean de aplicación para su organización y pulse el botón “Siguiente”. 

Paso	Descripción
9.	En el menú “Producto adicional” seleccione los productos que sean de aplicación para su organización y pulse el botón “Siguiente”. 
10.	En el menú “Función del sistema” seleccione la opción “Sistema por defecto” y pulse el botón “Siguiente”. 

Paso	Descripción
11.	En el menú “Propuesta de particionamiento” mantenga la opción recomendada por defecto y sin modificar ninguna opción, pulse el botón “Siguiente”.  **Nota:** En el caso de necesitar una de las dos opciones no contempladas en este documento, no se asegura la correcta funcionalidad de los scripts, los cuales deberán de adaptar a su nueva configuración.
12.	En el menú “Reloj y zona horaria” seleccione Zona horaria, España y Región Europa y a continuación pulse el botón “Siguiente”. 

Paso	Descripción
13.	En el menú “Usuario local” configure los siguientes parámetros. – Nombre completo del usuario: Usuario correspondiente a su organización. – Nombre de usuario: Usuario correspondiente a su organización. – Desmarcar la opción: Utilizar esta contraseña para el administrador del sistema. – Desmarcar la opción: Inicio de sesión automático. – Configurar una contraseña distinta para cada usuario y con los requisitos de seguridad y complejidad acordes a su categoría. Una vez configurados los parámetros pulse el botón “Siguiente” para continuar. 
14.	En el menú “Contraseña para el administrador del sistema “root” configure una contraseña distinta a las contraseñas de usuario y con los requisitos de seguridad y complejidad acordes a su categoría. Una vez configurados los parámetros correctamente, pulse el botón “Siguiente” para continuar.  **Nota:** El menú contempla un campo llamado “Probar distribución de teclado” por si se quisieran probar distintos caracteres especiales y poder cerciorarse en que tecla de su teclado se encuentran.

Paso	Descripción
15.	En el menú “Configuración de la instalación” vaya a cada apartado y pulse en “(inhabilitar)” o “(habilitar)” dependiendo de las necesidades de su organización. A continuación pulse en el botón “Instalar”. 
16.	En este momento aparecerá una ventana de confirmación de cambios para instalación, pulse en el botón “Instalar” para continuar, o “Atrás” si necesita revisar algún parámetro. 

Paso	Descripción
17.	Se iniciará la instalación, si algún paquete fallara al actualizar, compruebe la conexión a internet y pulse reintentar. 
18.	Ahora el sistema mostrará la pantalla de bienvenida, con el usuario creado. Pulse sobre el usuario e introduzca las credenciales. 
19.	Una vez introducidos las credenciales, pulse el botón “Iniciar sesión”.
20.	Finalmente se mostrará el escritorio. 

ANEXO A.3. CATEGORÍA BÁSICA

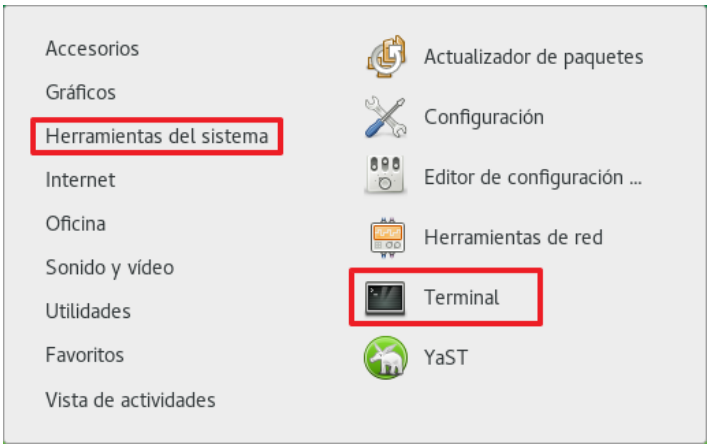
ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES SUSE ENTERPRISE 12 LINUX QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

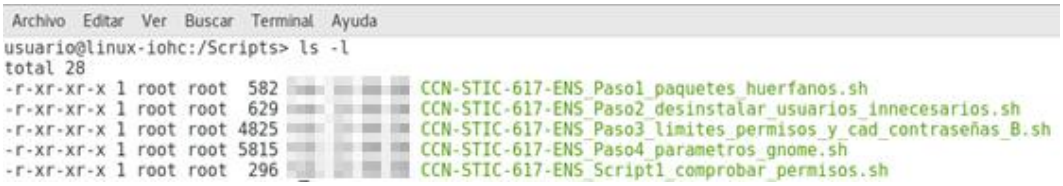
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores SUSE ENTERPRISE 12 LINUX con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad. Antes de realizar la 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, 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.

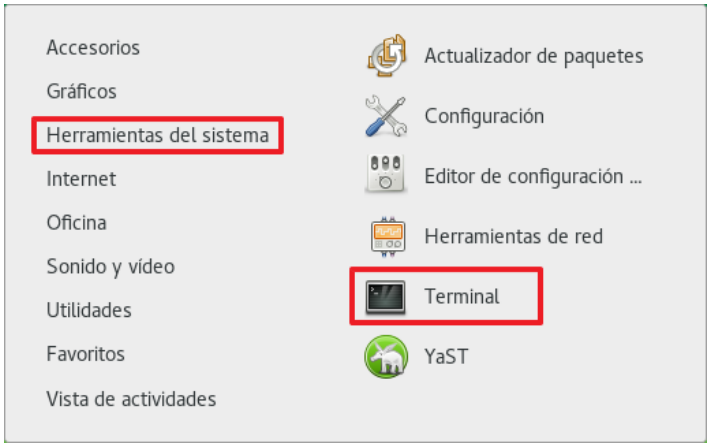
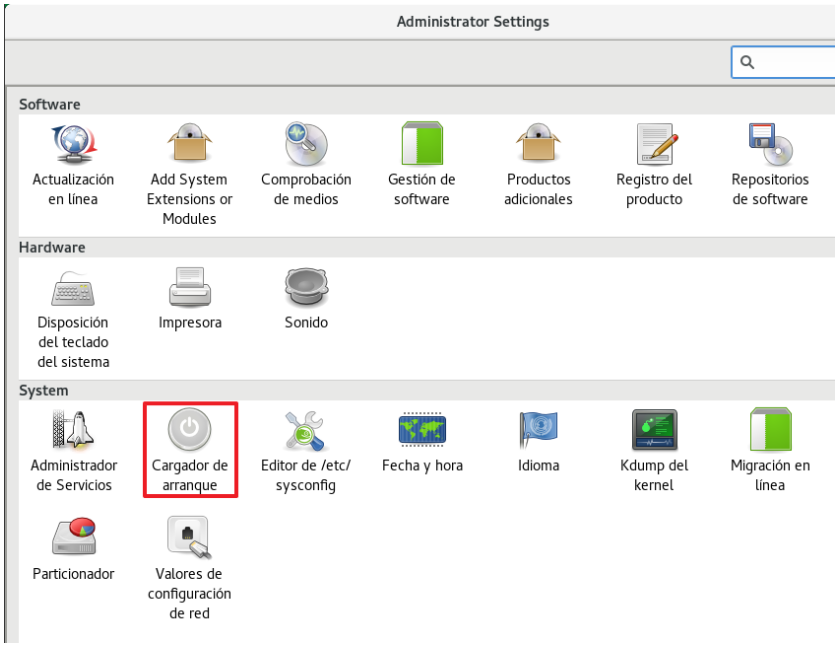
Los pasos que se describen a continuación se realizarán en todos aquellos servidores SUSE ENTERPRISE 12 LINUX, independientes a un dominio, que implementen servicios o información de categoría básica y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

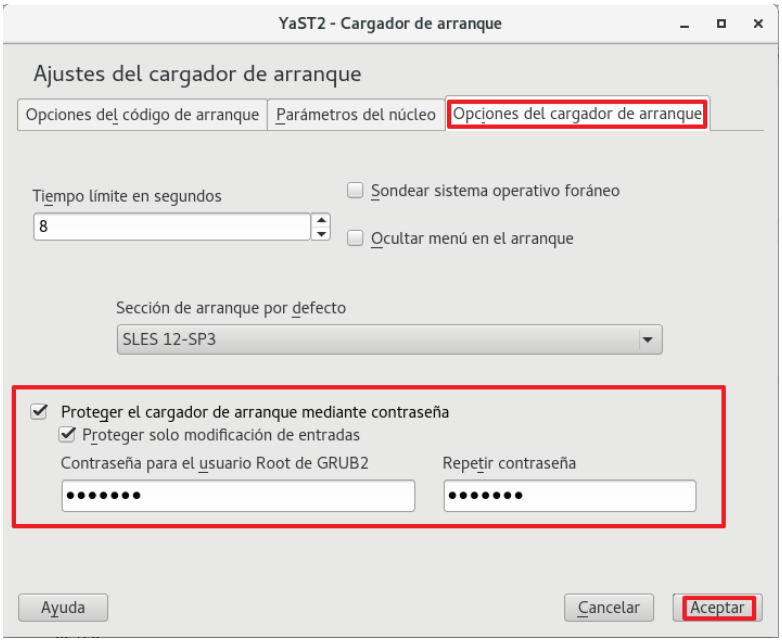
1. CONFIGURACIÓN SEGURA DEL ARRANQUE DEL SISTEMA

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 “CATEGORIA_BASICA” correspondiente al directorio. “Scripts/ENS_CATEGORIA_BASICA” asociado a esta guía en la ruta “**/Scripts**”.
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando **“cd /Scripts/”** y pulse la tecla “Enter”.

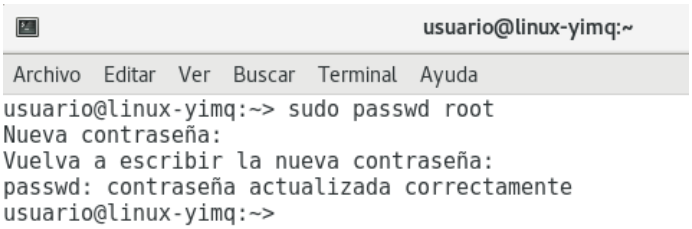
Paso	Descripción
6.	Posteriormente ejecute "**ls -l**" y compruebe que están todos los scripts. 

1.1. CONTRASEÑA DE GRUB

Paso	Descripción
7.	Se procede a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "YaST". 
8.	Introduzca la contraseña cuando se le solicite y aparecerá la siguiente pantalla. Pulse entonces el icono "Cargador de arranque". 

Paso	Descripción
9.	Una vez se encuentre en la ventana "YaST2 – Cargador de arranque", despliegue la pestaña "Opciones del cargador de arranque" y habilite "Proteger el cargador de arranque mediante contraseña" y "Proteger solo modificación de entradas". Posteriormente pulse "Aceptar". 

1.2. CONTRASEÑA SEGURA DE ROOT

Paso	Descripción
10.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
11.	Ejecute el siguiente comando. **$ sudo passwd root**
12.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se procederá a actualizar. Se pedirá la nueva contraseña y la confirmación de la misma. 
13.	Cuando el proceso haya terminado se mostrará el mensaje. "passwd: contraseña actualizada correctamente". Si no muestra ese mensaje, repita los pasos anteriores.

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, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**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 "4.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

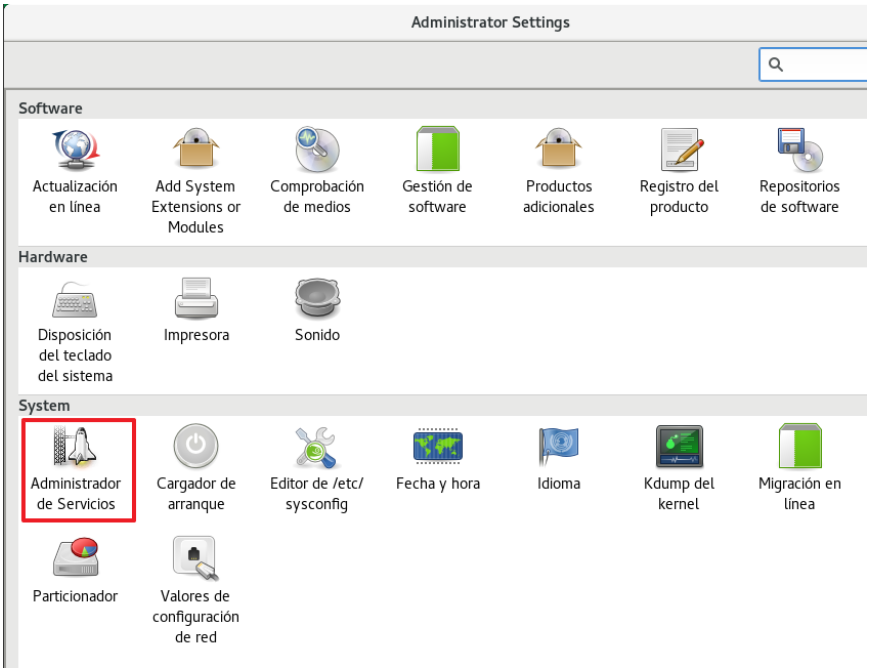
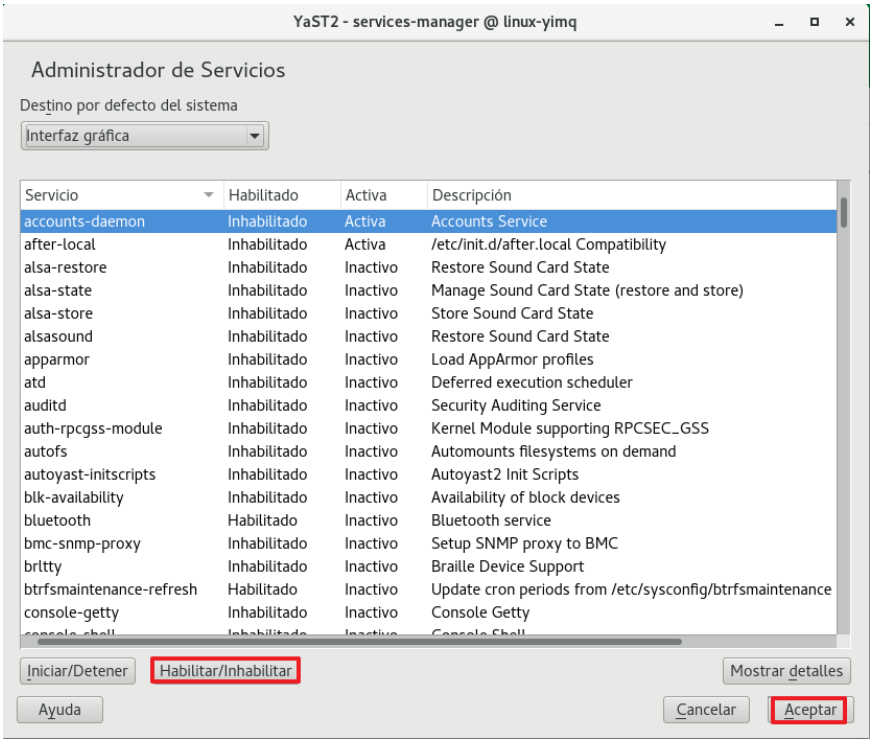
1.4. USUARIOS CON UID 0 QUE NO SEAN ROOT

Paso	Descripción
17.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**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 "4.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

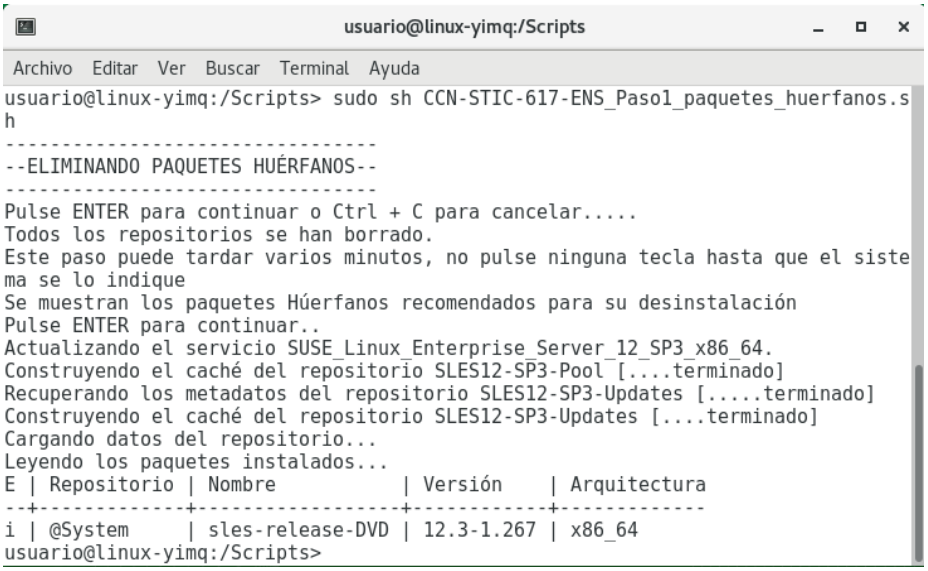
2. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

2.1. LIMITACIÓN DE SERVICIOS Y DEMONIOS

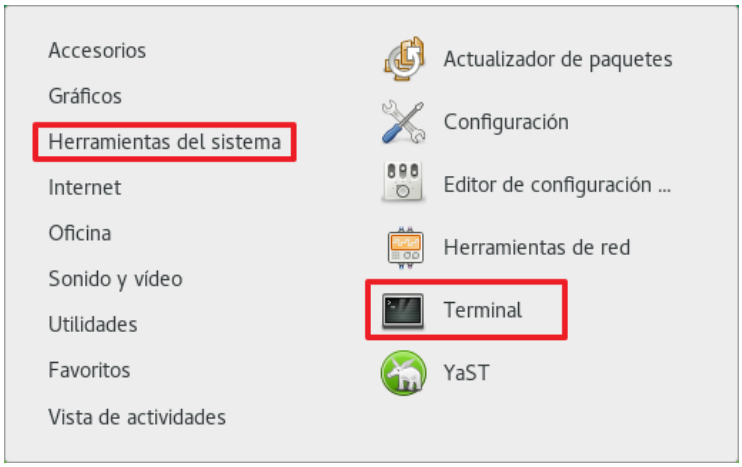
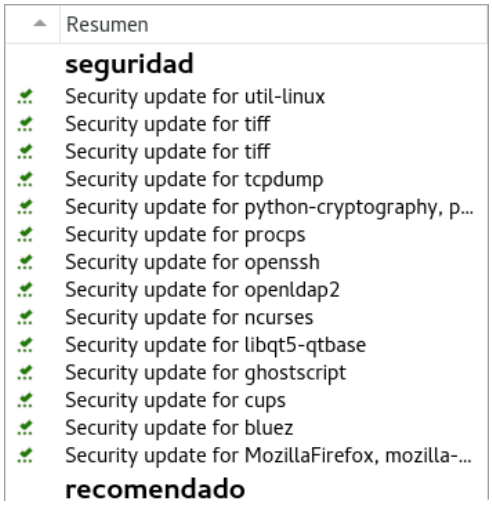
Paso	Descripción
20.	Se procede a deshabilitar servicios y demonios innecesarios. Para ello diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "YaST".

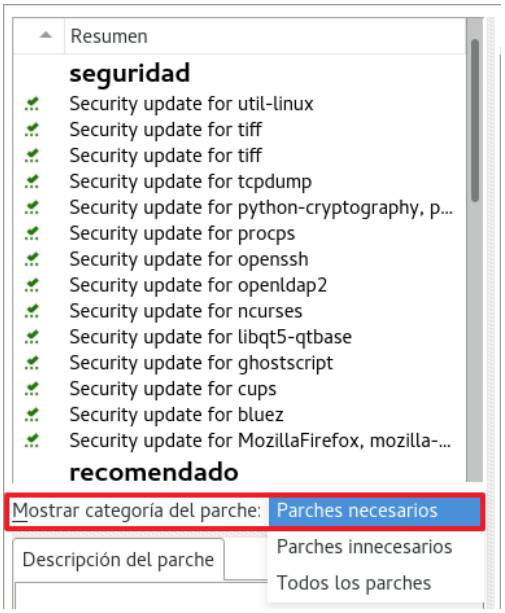
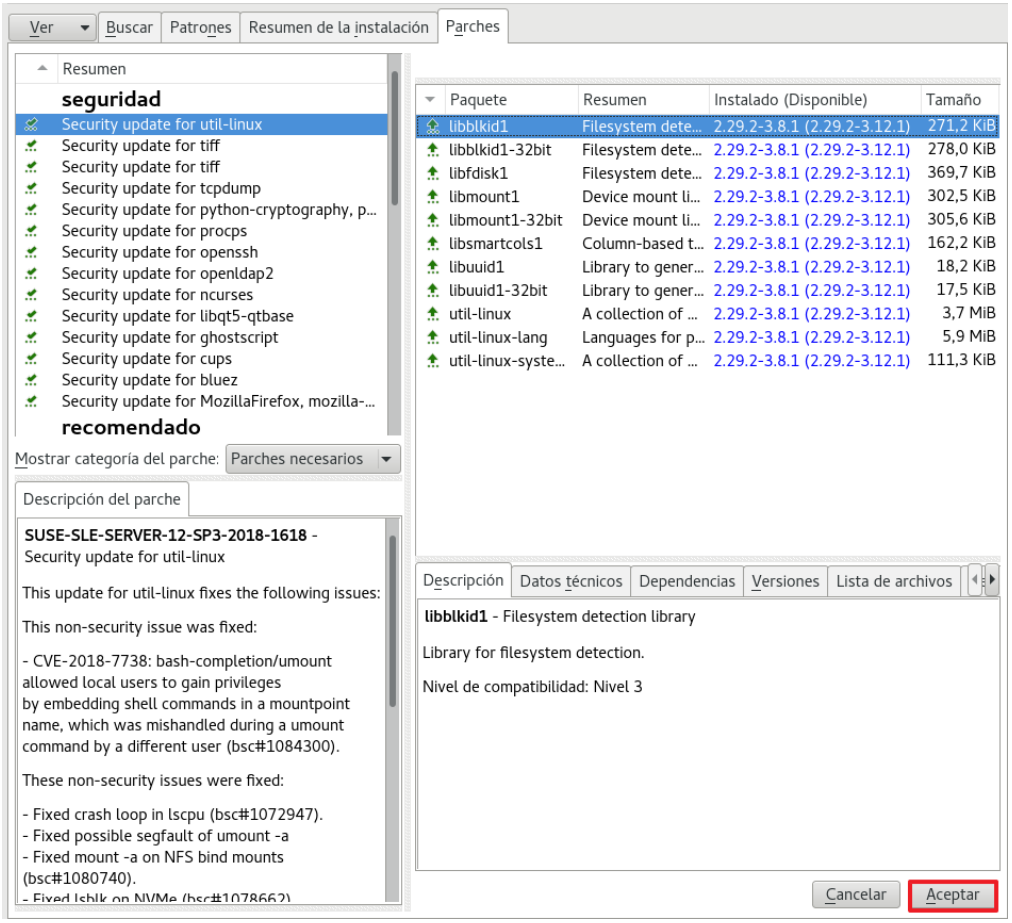
Paso	Descripción
21.	Introduzca la contraseña cuando se le solicite y aparecerá la siguiente pantalla. Pulse entonces el icono “Administrador de Servicios”. 
22.	Una vez se encuentre en la ventana “YaST2 – services-manager”, revise los servicios y habilite o inhabilite según las necesidades de su organización. Posteriormente pulse el botón “Aceptar”. 

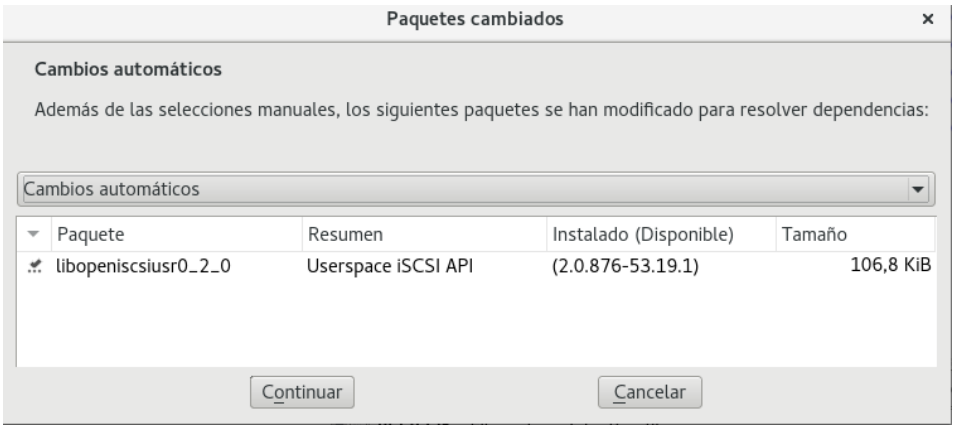
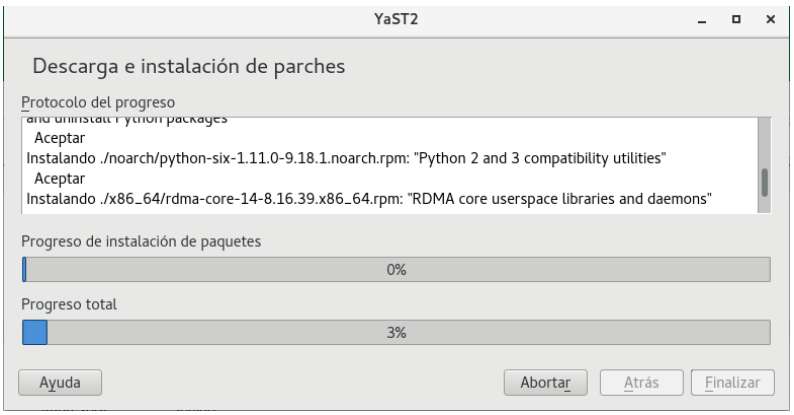
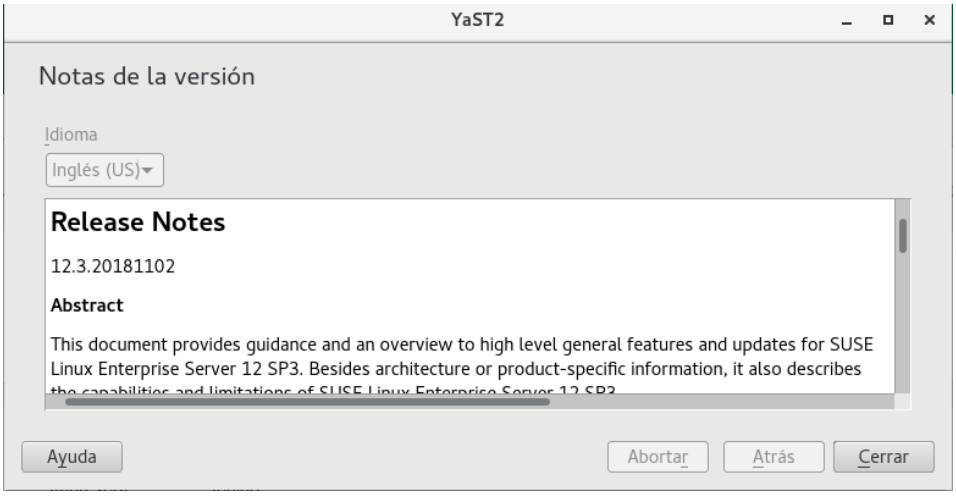
2.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

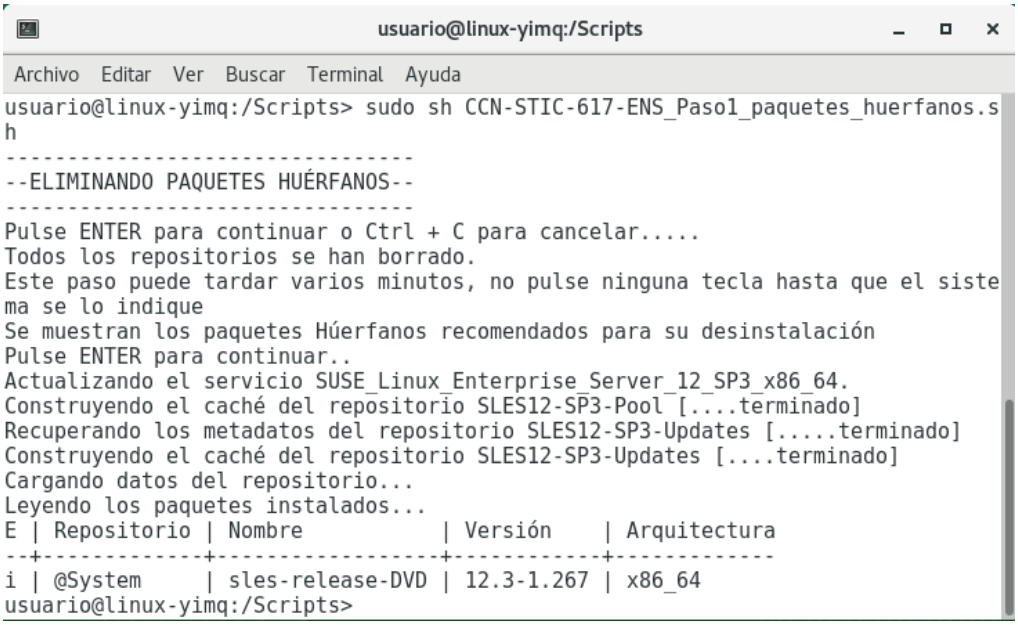
Paso	Descripción
23.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
24.	Se procederá a revisar los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**
25.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh** El script iniciará un proceso de comprobación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice, se mostrarán los paquetes huérfanos candidatos para su desinstalación, así mismo se copiarán en el archivo "orphaned.txt" que se generará en la misma ruta del script. La desinstalación se deberá hacer manualmente.  **Nota:** Si el script detectara algún programa o repositorio candidato para su desinstalación, una vez finalice la desinstalación, se recomienda volver al punto 23 de este apartado y volver a ejecutar el script, para eliminar posibles paquetes huérfanos. La desinstalación deberá hacerse manualmente.

3. APLICACIÓN DE ACTUALIZACIONES

Paso	Descripción
26.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “YaST”. Introduzca la contraseña necesaria para elevar privilegios. Y pulse “Continuar”. 
27.	En el apartado “Software” dirijase al icono “Actualización en línea” y haga clic en él. 
28.	En la columna de la izquierda aparecerá un cuadro resumen con las actualizaciones de seguridad y las recomendadas. 

Paso	Descripción
29.	Debe comprobar que en el apartado “Mostrar categoría del parche:” esta seleccionado “Parches necesarios”. 
30.	Si pulsa sobre alguna de las actualizaciones se verá un resumen de las mismas. Elija las actualizaciones de los parches que más convengan para su organización. Una vez realizada las comprobaciones pertinentes pulse el botón “Aceptar”. 

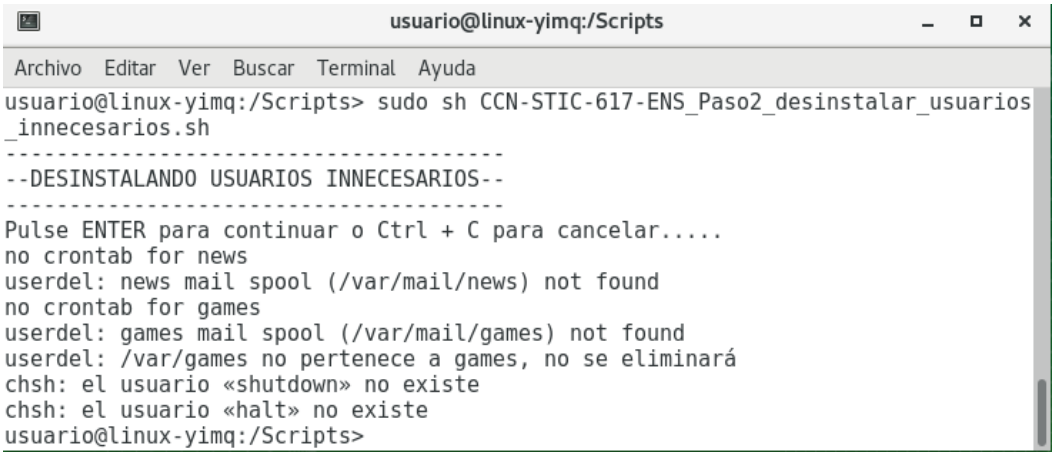
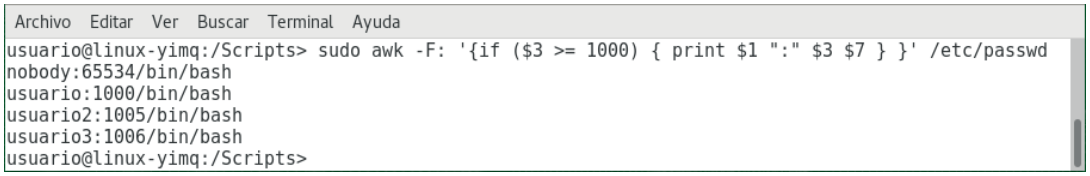
Paso	Descripción
31.	Si hubiera alguna modificación en actuales paquetes instalados, el programa de actualización lo comunicará. Revise los paquetes que modifica y escoja las opciones que más convengan a su organización. En cualquier caso, pulse el botón “Continuar” para seguir con la instalación. 
32.	El programa comenzará la instalación de las actualizaciones, no pulse ninguna tecla hasta la finalización de las mismas. 
33.	Al finalizar YaST2 mostrará las Notas de versión actualizadas. 

Paso	Descripción
34.	Una vez finalizada la actualización, vuelva a ejecutar el script "CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh" del punto "2.2 COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS". Para ello diríjase a la barra de tareas, pulse en "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "Terminal". Ejecute el comando **"cd /"** y pulse la tecla **"Enter".**
35.	Diríjase a la carpeta **"/Scripts/"** y ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh** El script iniciará un proceso de comprobación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice, se mostrarán los paquetes huérfanos candidatos para su desinstalación, así mismo se copiarán en el archivo "orphaned.txt" que se generará en la misma ruta del script. 

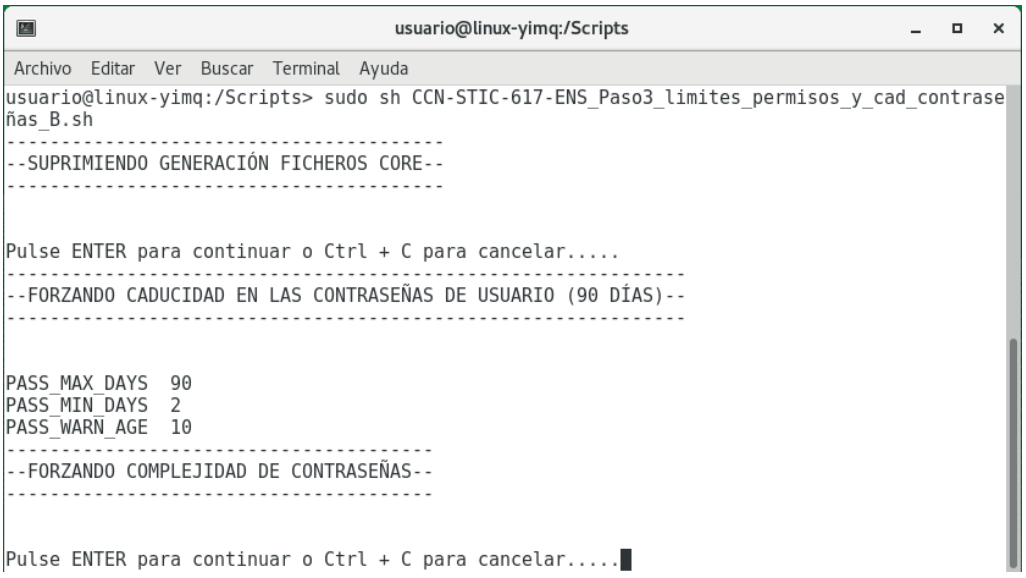
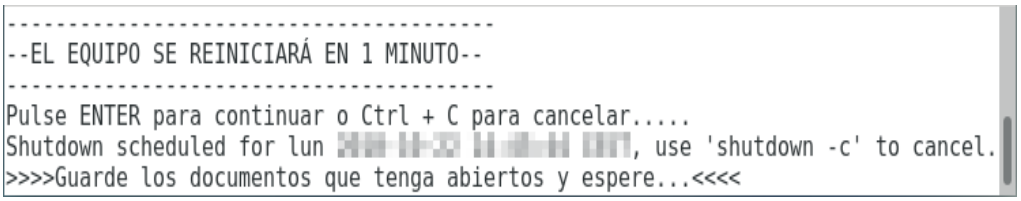
4. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

4.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

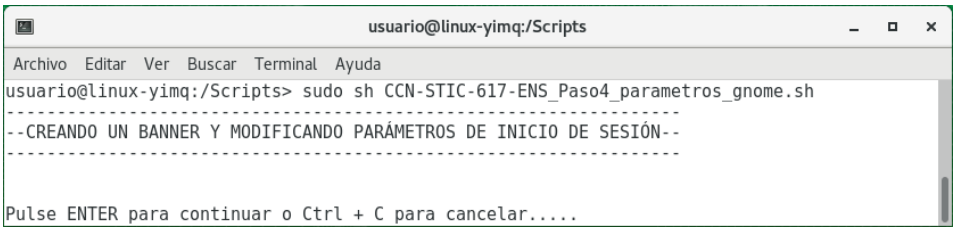
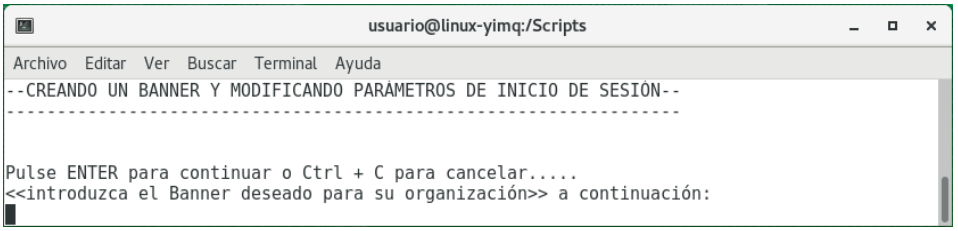
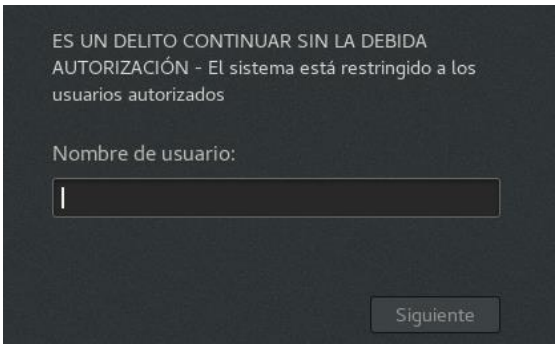
Paso	Descripción
36.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
37.	Se va a proceder a eliminar los usuarios 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-617-ENS_Paso2_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**
41.	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 es posible que aparezca el usuario nfsnobody 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.
42.	Cuando finalice todas las tareas reinicie el sistema.

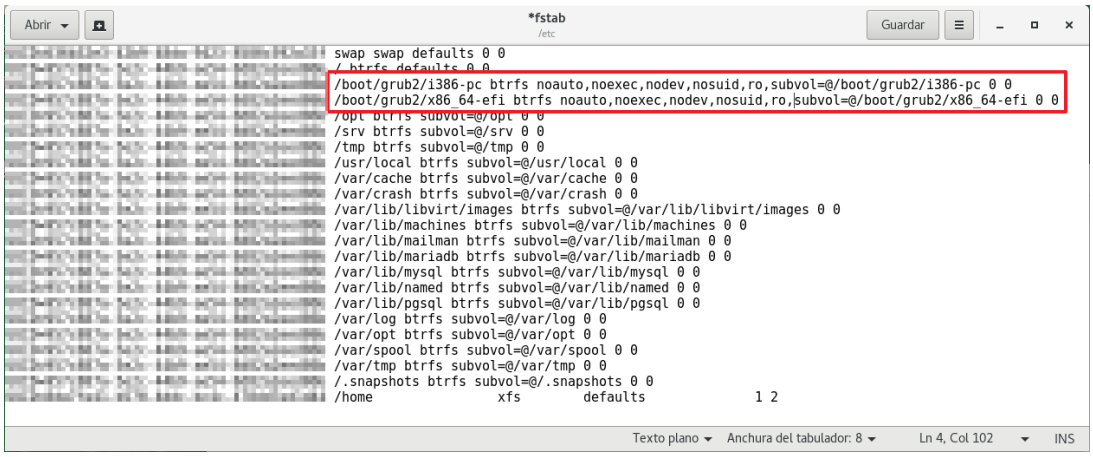
4.2. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

Paso	Descripción
43.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
44.	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**
45.	Ejecute el siguiente script. **$ sudo sh CCN-STIC-617-ENS_Paso3_limites_permisos_y_cad_contraseñas_B.sh** 
46.	Cuando finalice el script, saldrá un mensaje advirtiendo que el sistema se reiniciará en 1 minuto. Espere y cierre las aplicaciones que tenga abiertas. 
47.	Cuando reinicie el sistema e inicie sesión, aparecerá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos.
48.	Le pedirá la contraseña actual y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.

4.3. CONFIGURACIÓN SEGURA DE GNOME

Paso	Descripción
49.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
50.	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-617-ENS_Paso4_parametros_gnome.sh** 
51.	Introduzca el Banner deseado acorde con su organización. 
52.	El script iniciará un proceso que modificará la pantalla de inicio de SUSE Enterprise Linux 12 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:** SUSE Enterprise Linux 12 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. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

Paso	Descripción
1.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
2.	Ejecute el siguiente comando. **$ gnomesu gedit /etc/fstab &>/dev/null**
3.	Edite el fichero de configuración y modifique los permisos de la partición "**/boot**" para que el resultado sea similar al de la imagen (noauto, noexec, nodev, nosuid, ro). 
4.	Cuando termine, pulse el botón "**Guardar**" y cierre el editor de texto. Elimine el directorio "/Scripts" y todo su contenido.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE CLIENTE SUSE ENTERPRISE LINUX 12 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 SERVIDORES SUSE ENTERPRISE 12 LINUX QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS".

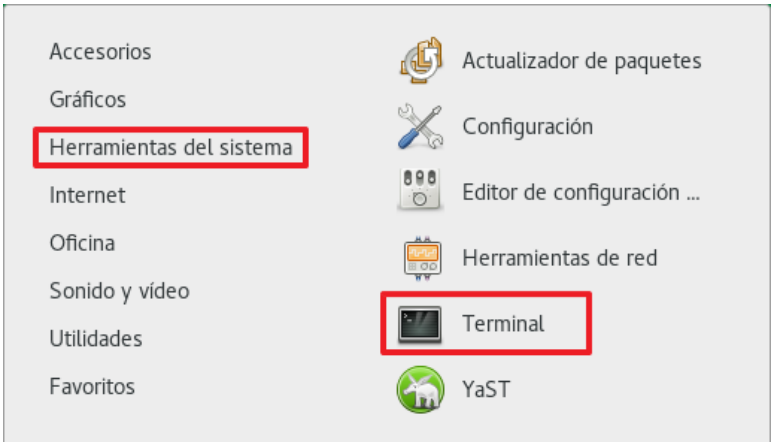
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores SUSE Enterprise Linux 12 independientes con implementación de seguridad de categoría básica del ENS.

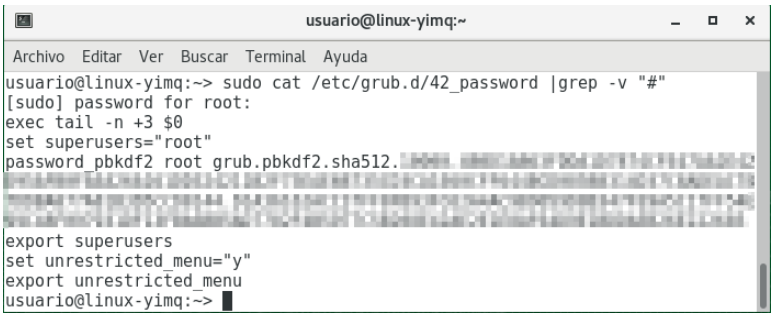
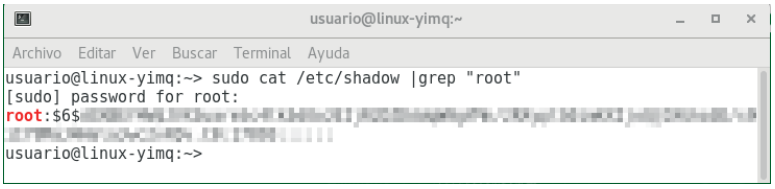
Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

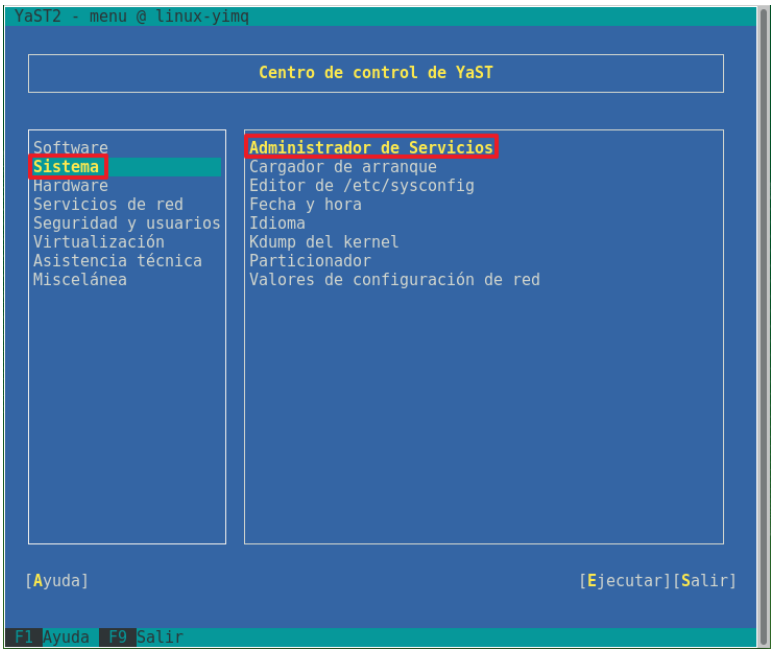
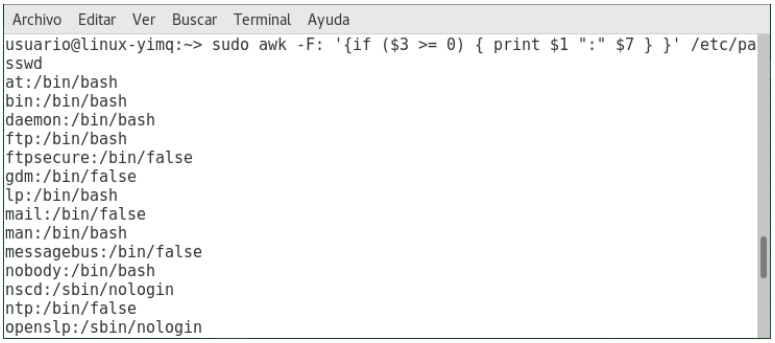
Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas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

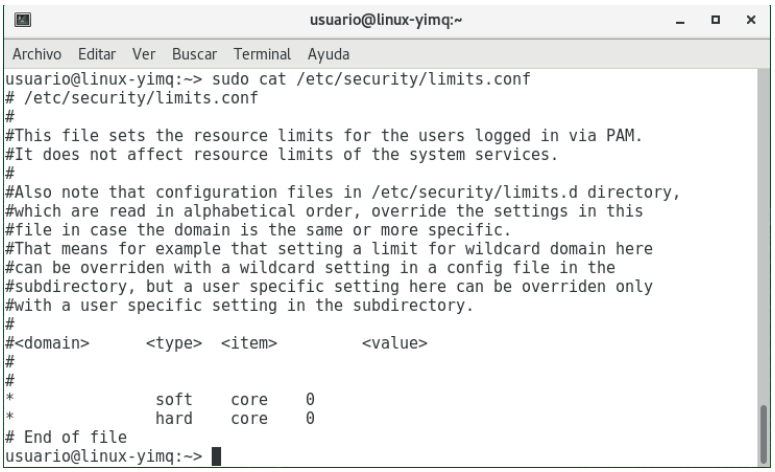
a) Terminal de Linux

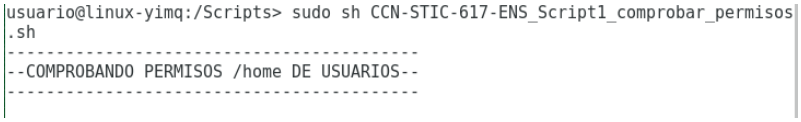
b) Herramienta YaST

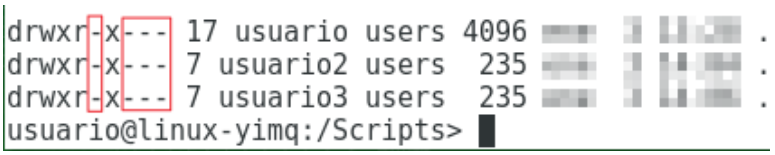
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En el cliente, inicie sesión con una cuenta con privilegios de root. Cree la carpeta "Scripts" en "/" y copie el contenido de la categoría de seguridad "BASICA" correspondiente al directorio "Scripts/ENS_CATEGORIA_BASICA" asociado a esta guía en la ruta "/Scripts".
2. Inicie la Terminal de Linux		Ejecute la "Terminal". Para ello Diríjase a la barra de tareas, pulse en Aplicaciones y en el apartado "Herramientas del sistema" seleccione "Terminal". 

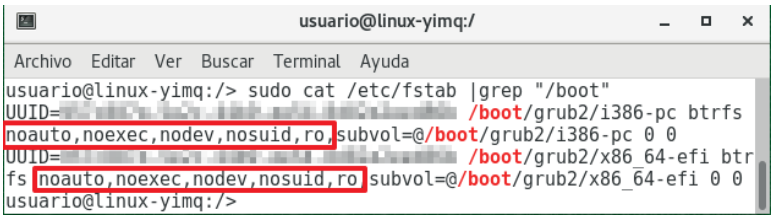
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que grub tiene contraseña configurada y root como único usuario de modificación.		En la "Terminal" ejecute el siguiente comando. **$ sudo cat /etc/grub.d/42_password |grep -v "#"**  **Nota:** Fíjese en las letras y números que están situadas después de "**password_pbkdf2 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.
5. Búsqueda de usuarios sin contraseña.		Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f2 | grep ":$" |cut -d":" -f1**
6. Búsqueda de usuarios con UID 0.		Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1 |grep -v "root"**

Comprobación	OK/NOK	Cómo hacerlo
7. Servicios innecesarios por medio de herramienta YaST.		Abra la Terminal y ejecute el siguiente comando. **$ sudo yast**  Revise que los servicios activos al iniciar el sistema son los correctos para su organización.
8. Comprobación de usuarios y shells predetermina-das.		Ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 0) { print $1 ":" $7 } }' /etc/passwd**  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
 
</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>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.
$ cat /etc/login.defs |grep "PASS_MAX_DAYS"
$ cat /etc/login.defs |grep "PASS_MIN_DAYS"
$ cat /etc/login.defs |grep "PASS_MIN_LEN"
$ cat /etc/login.defs |grep "PASS_WARN_AGE"
$ cat /etc/login.defs |grep "UMASK"
Compruebe si se han configurado bien los valores.</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></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>PASS_MIN_LEN</td><td>8</td><td></td></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>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>12. Verifique la directiva de complejidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ cat /etc/pam.d/common-password |grep "minlen="
$ cat /etc/pam.d/common-password |grep "dcredit="
$ cat /etc/pam.d/common-password |grep "ucredit="
$ cat /etc/pam.d/common-password |grep "lcredit="
$ cat /etc/pam.d/common-password |grep "ocredit="
<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>
<tr><td>ocredit</td><td>-1</td><td></td></tr>
</table></td></tr>
<tr><td>13. Comprobar permisos</td><td></td><td>Se va a proceder a revisar los permisos de la ruta “/home” de cada usuario del sistema.
Para ello diríjase a la carpeta “Scripts”.
$ cd /Scripts
Ejecute el siguiente comando.
$ sudo sh CCN-STIC-617-ENS_Script1_comprobar_permisos.sh
 

El script mostrará los permisos de las carpetas “/home” y se debe comprobar que las columnas marcadas se encuentren vacías.
 
</td></tr>
<tr><td>14. 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.
$ sudo 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>
$ sudo 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 rowspan="11"></td><td></td><td>$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "idle-delay=uint32"
$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "lock-enabled"
$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "lock-delay=uint32"</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>idle-delay=uint32</td><td>0</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></td></tr>
<tr><td></td><td>$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "automount="
$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "automount-open="
$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "autorun-never="</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>automount</td><td>false</td><td></td></tr>
<tr><td>automount-open</td><td>false</td><td></td></tr>
<tr><td>autorun-never</td><td>true</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "hide-identity"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "old-files-age"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "remember-recent-files"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep " remove-old-temp-files”</td></tr>
<tr><td colspan="2"><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>15. 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

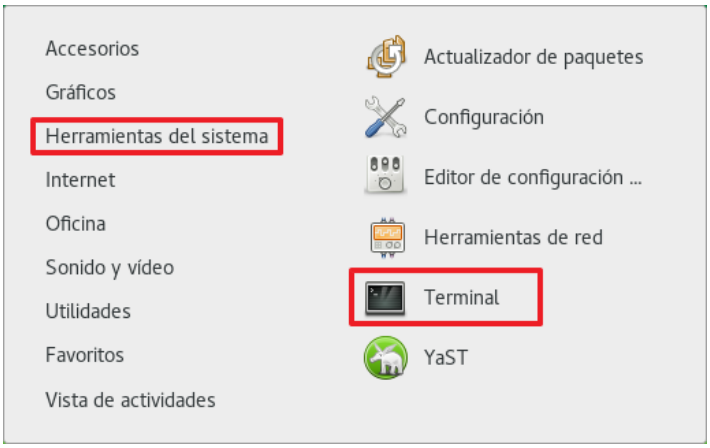
ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES SUSE ENTERPRISE LINUX 12 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores SUSE Enterprise Linux 12 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.

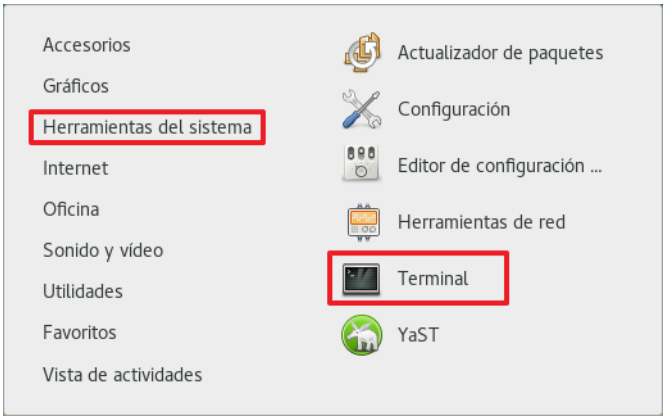
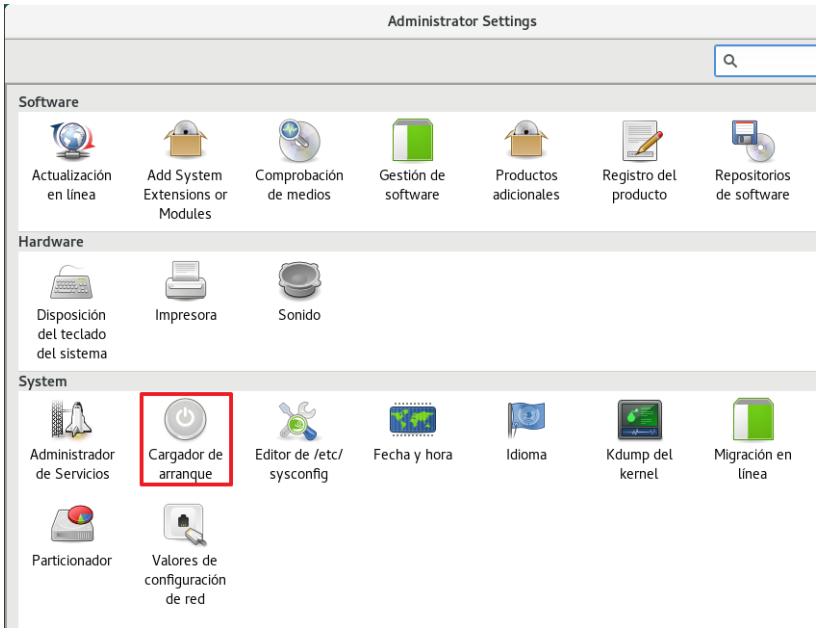
Los pasos que se describen a continuación se realizarán en todos aquellos servidores SUSE Enterprise Linux 12, independientes a un dominio, que implementen servicios o información de categoría media y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

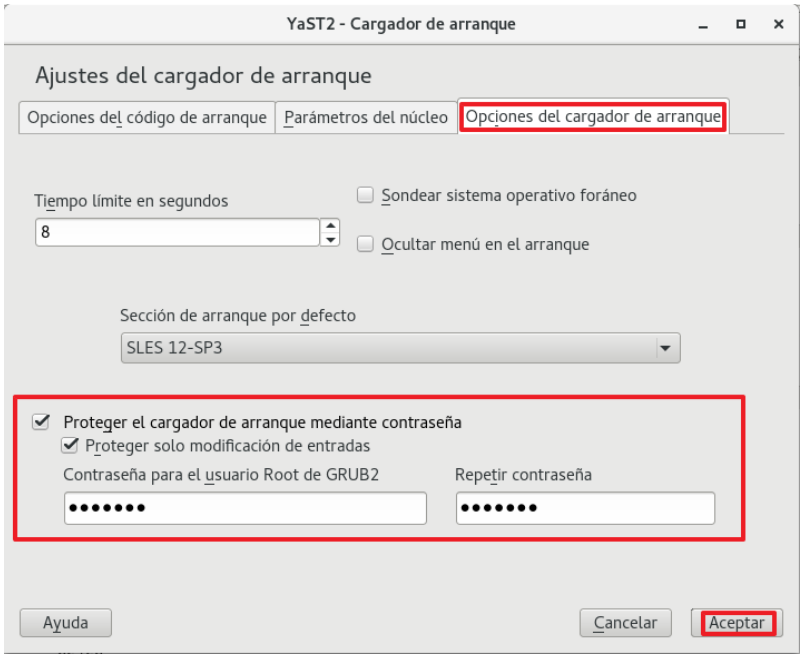
1. CONFIGURACIÓN SEGURA DEL ARRANQUE DEL SISTEMA

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 “CATEGORIA_MEDIA” correspondiente al directorio “Scripts/ENS_CATEGORIA_MEDIA” asociado a esta guía en la ruta “**/Scripts**”.
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando **“cd /Scripts”** y pulse la tecla “Enter”.

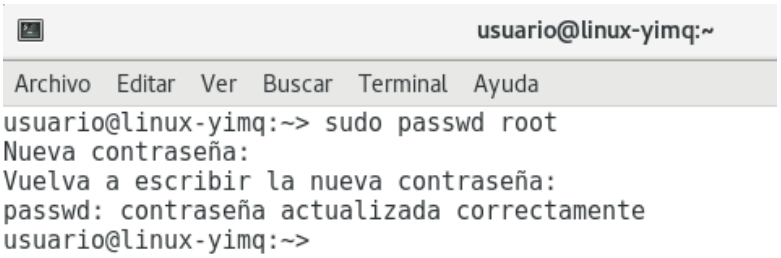
Paso	Descripción
6.	Posteriormente ejecute "**ls -l**" y compruebe que están todos los scripts. Archivo Editar Ver Buscar Terminal Ayuda usuario@linux-iohc:/Scripts> ls -l total 40 -r-xr-x--- 1 root root 561 [redacted] CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh -r-xr-x--- 1 root root 6519 [redacted] CCN-STIC-617-ENS_Paso2_reglas_audit.sh -r-xr-x--- 1 root root 629 [redacted] CCN-STIC-617-ENS_Paso3_desinstalar_usuarios_innecesarios.sh -r-xr-x--- 1 root root 6544 [redacted] CCN-STIC-617-ENS_Paso4_parametros_gnome_M.sh -r-xr-x--- 1 root root 1631 [redacted] CCN-STIC-617-ENS_Paso5_intentos_fallidos_M.sh -r-xr-x--- 1 root root 4744 [redacted] CCN-STIC-617-ENS_Paso6_limites_permisos_y_cad_contraseñas_M.sh -r-xr-x--- 1 root root 296 [redacted] CCN-STIC-617-ENS_Script1_comprobar_permisos.sh

1.1. CONTRASEÑA DE GRUB

Paso	Descripción
7.	Se procede a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "YaST". 
8.	Introduzca la contraseña cuando se le solicite y aparecerá la siguiente pantalla. Pulse entonces el icono "Cargador de arranque". 

Paso	Descripción
9.	Una vez se encuentre en la ventana “YaST2 – Cargador de arranque”, despliegue la pestaña Opciones del cargador de arranque y habilite “Proteger el cargador de arranque mediante contraseña” y “Proteger solo modificación de entradas”. Posteriormente pulse “Aceptar”. 

1.2. CONTRASEÑA SEGURA DE ROOT

Paso	Descripción
10.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “**Terminal**”. Ejecute el comando **“cd /”** y pulse la tecla “Enter”.
11.	Ejecute el siguiente comando. **$ sudo passwd root**
12.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se procederá a actualizar. Se pedirá la nueva contraseña y la confirmación de la misma. 
13.	Cuando el proceso haya terminado se mostrará el siguiente mensaje. “passwd: contraseña actualizada correctamente.” Si no muestra ese mensaje, repita los pasos anteriores.

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, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**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".

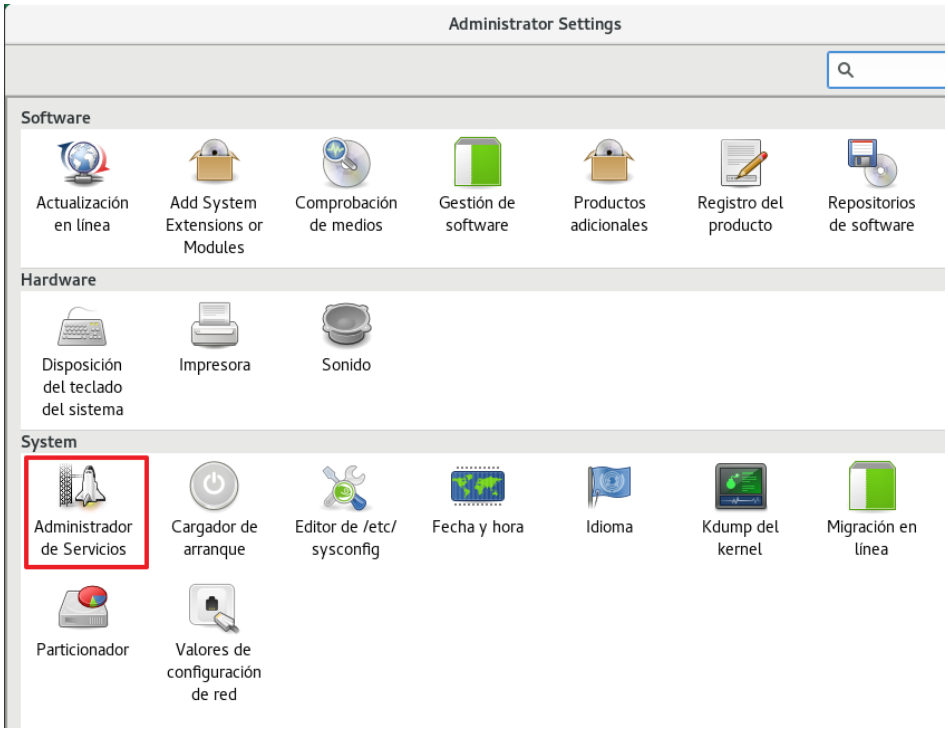
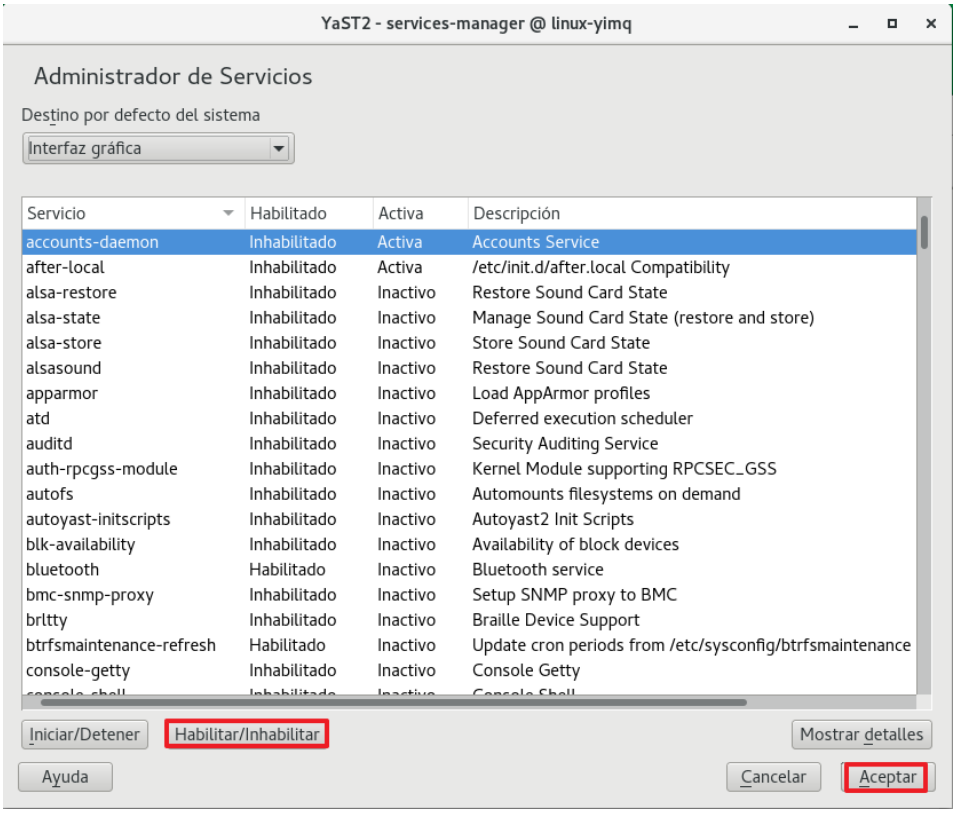
1.4. USUARIOS CON UID 0 QUE NO SEAN ROOT

Paso	Descripción
17.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**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 "4.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

2. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

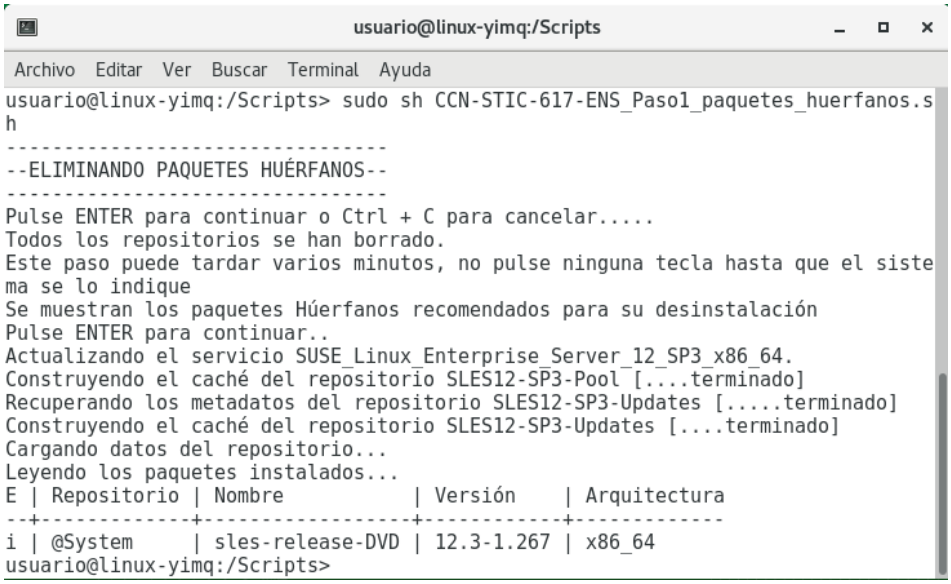
2.1. LIMITACIÓN DE SERVICIOS Y DEMONIOS

Paso	Descripción
20.	Se procede a deshabilitar servicios y demonios innecesarios. Para ello diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "YaST".

Paso	Descripción
21.	Introduzca la contraseña cuando se le solicite y aparecerá la siguiente pantalla. Pulse entonces el icono “Administrador de Servicios”. 
22.	Una vez se encuentre en la ventana “YaST2 – services-manager”, revise los servicios y habilite o inhabilite según las necesidades de su organización. Posteriormente pulse el botón “Aceptar”. 

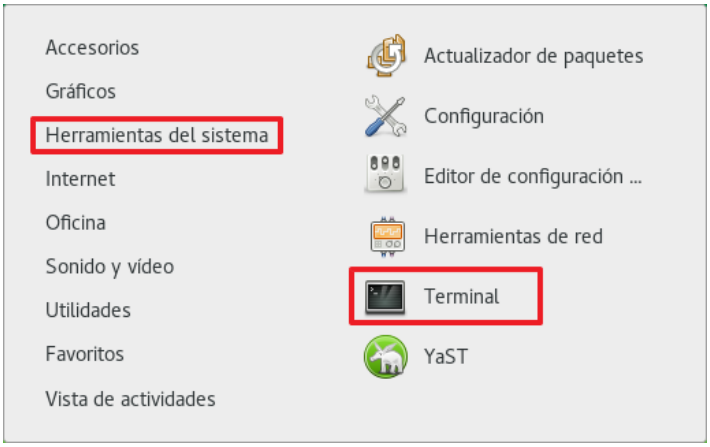
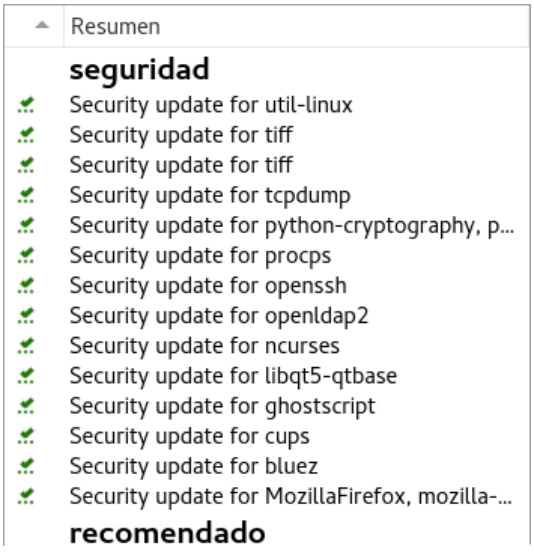
2.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

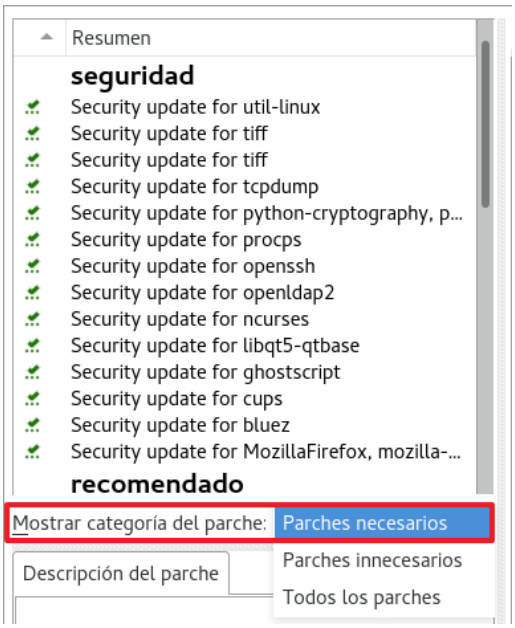
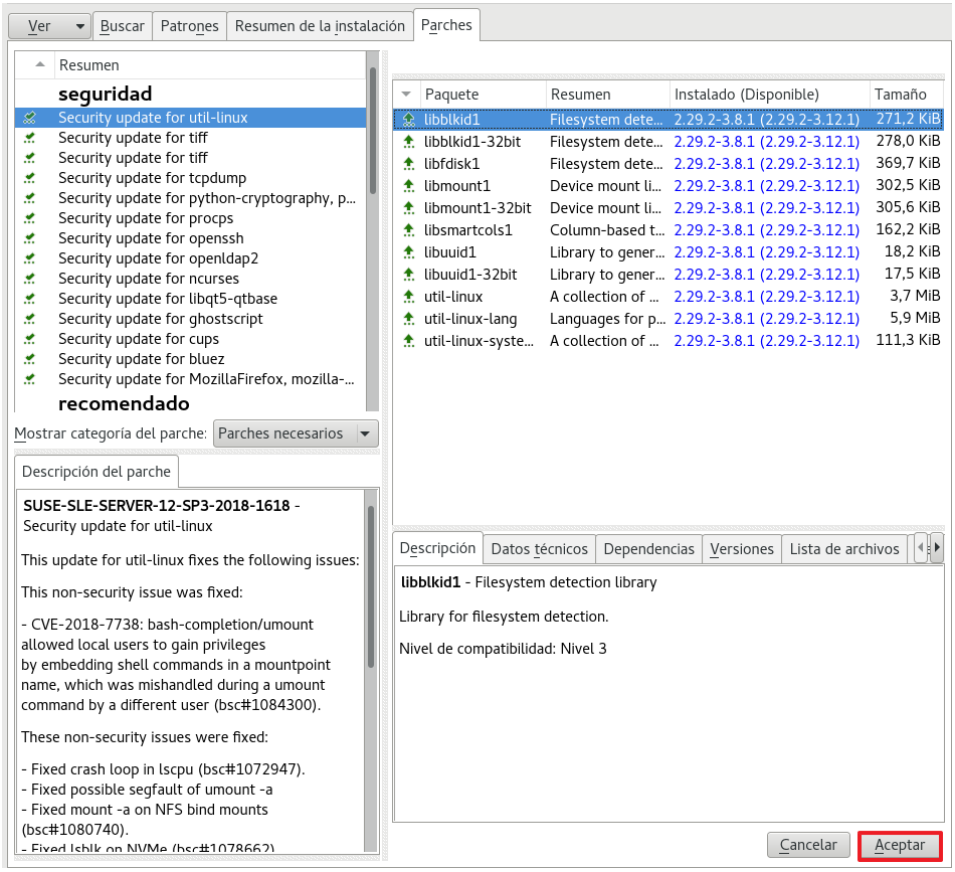
Paso	Descripción
23.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
24.	Se procederá a revisar los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**
25.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh** El script iniciará un proceso de comprobación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice, se mostrarán los paquetes huérfanos candidatos para su desinstalación, así mismo se copiarán en el archivo "orphaned.txt" que se generará en la misma ruta del script.

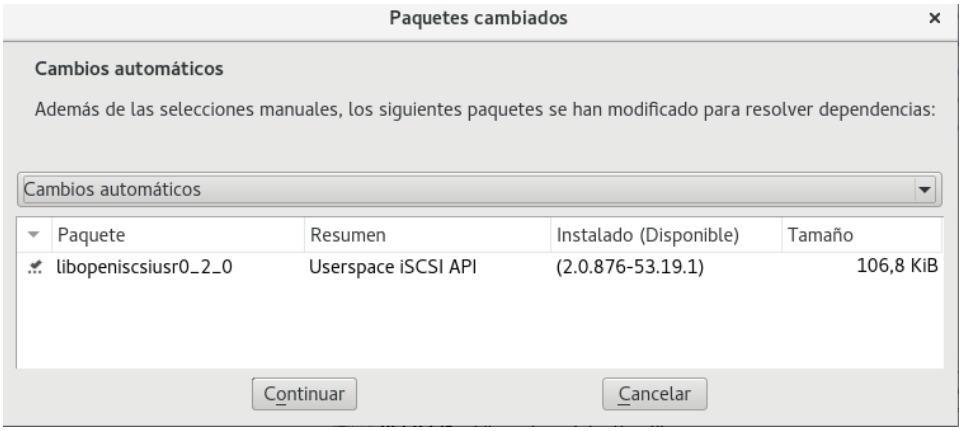
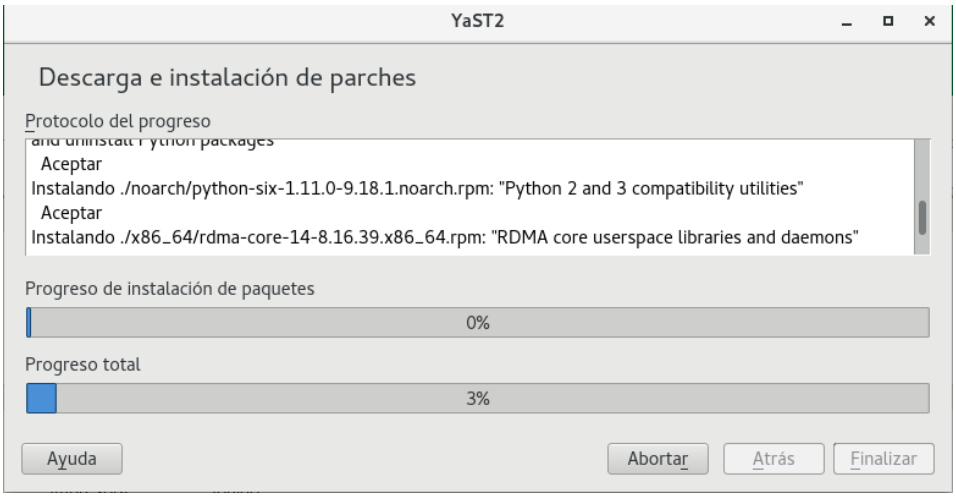
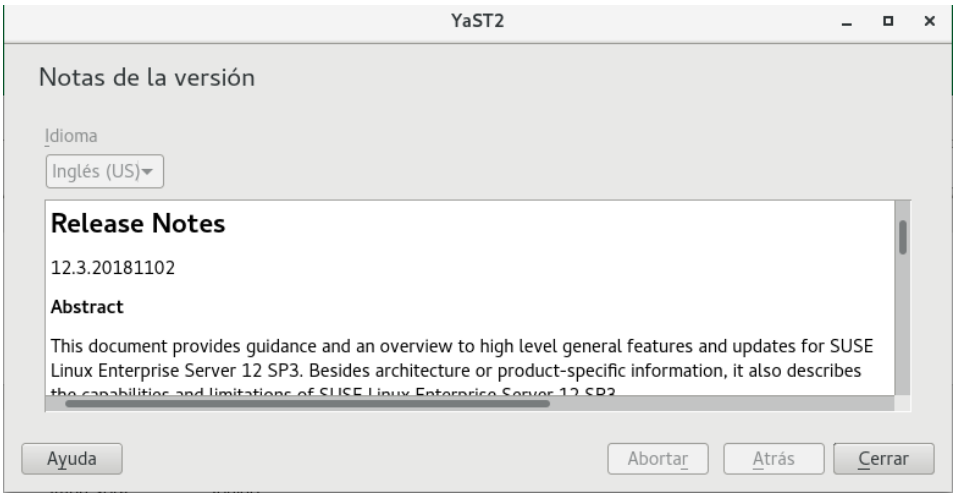


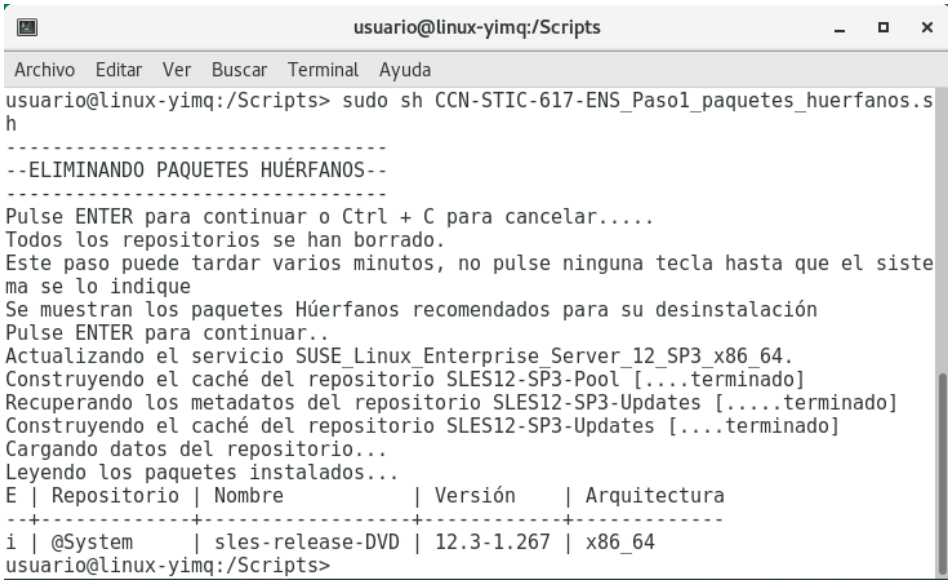
Nota: Si el script detectara algún programa o repositorio candidato para su desinstalación, una vez finalice la desinstalación, se recomienda volver al punto 23 de este apartado y volver a ejecutar el script, para eliminar posibles paquetes huérfanos. La desinstalación deberá hacerse manualmente.

3. APLICACIÓN DE ACTUALIZACIONES

Paso	Descripción
26.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “YaST”. Introduzca la contraseña necesaria para elevar privilegios. Y pulse “Continuar”. 
27.	En el apartado “Software” dirijase al icono “Actualización en línea” y haga clic en él. 
28.	En la columna de la izquierda aparecerá un cuadro resumen con las actualizaciones de seguridad y las recomendadas. 

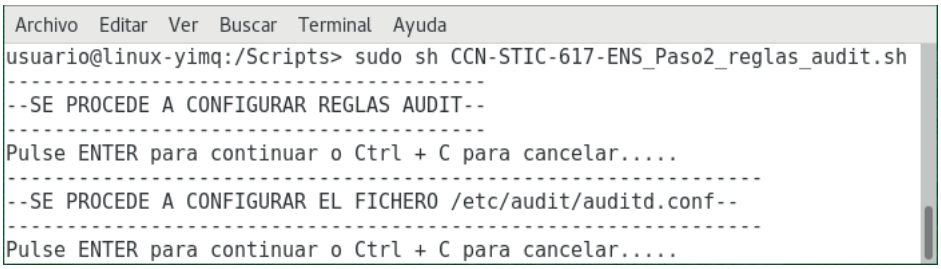
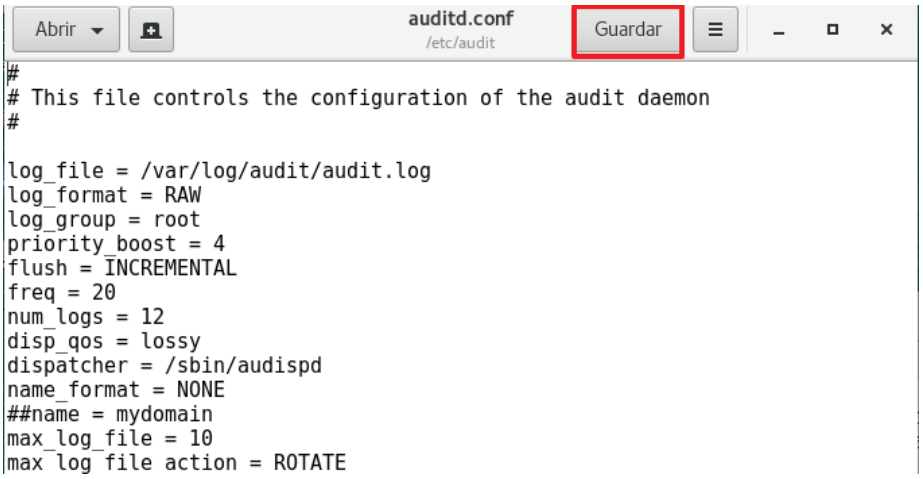
Paso	Descripción
29.	Debe comprobar que en el apartado “Mostrar categoría del parche:” esta seleccionado “Parches necesarios”. 
30.	Si pulsa sobre alguna de las actualizaciones se verá un resumen de las mismas. Elija las actualizaciones de los parches que más convengan para su organización. Una vez realizada las comprobaciones pertinentes pulse el botón “Aceptar”. 

Paso	Descripción
31.	Si hubiera alguna modificación en actuales paquetes instalados, el programa de actualización lo comunicará. Revise los paquetes que modifica y escoja las opciones que más convengan a su organización. En cualquier caso, pulse el botón “Continuar” para seguir con la instalación. 
32.	El programa comenzará la instalación de las actualizaciones, no pulse ninguna tecla hasta la finalización de las mismas. 
33.	Al finalizar YaST2 mostrará las Notas de versión actualizadas. 

Paso	Descripción
34.	Una vez finalizada la actualización, vuelva a ejecutar el script "CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh" del punto "2.2 COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS". Para ello diríjase a la barra de tareas, pulse en "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "Terminal". Ejecute el comando **"cd /"** y pulse la tecla **"Enter".**
35.	Diríjase a la carpeta **"/Scripts/"** y ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh** El script iniciará un proceso de comprobación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice, se mostrarán los paquetes huérfanos candidatos para su desinstalación, así mismo se copiarán en el archivo "orphaned.txt" que se generará en la misma ruta del script. 

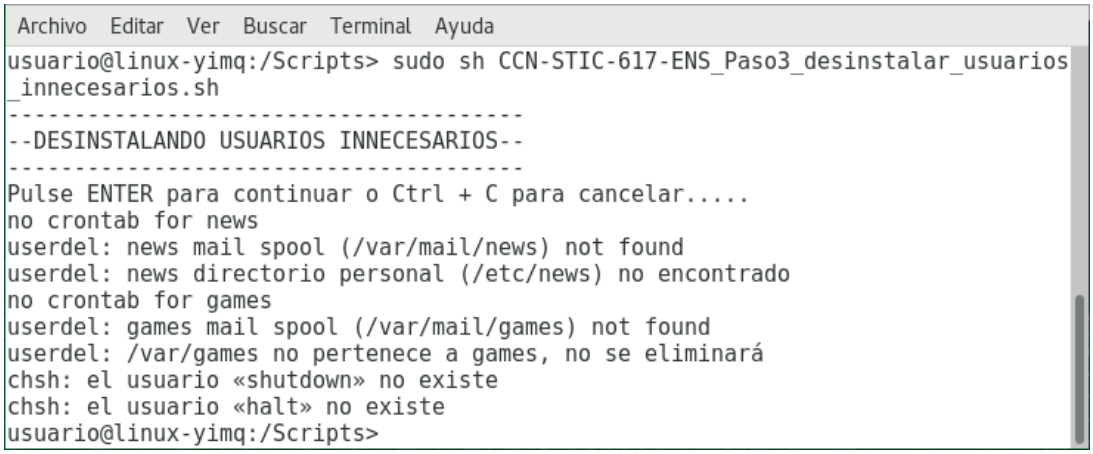
4. CONFIGURACIÓN DE REGISTROS DE ACTIVIDAD

Paso	Descripción
36.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
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**

Paso	Descripción
38.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso2_reglas_audit.sh** El script finalizará mostrando las reglas creadas. Si el sistema indicara lo contrario vuelva a ejecutar 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".**
39.	Ajuste esta configuración con los parámetros necesarios para su organización. Para ello ejecute el siguiente comando. **$ gnomesu gedit /etc/audit/auditd.conf &>/dev/null**
40.	Modifique los parámetros marcados según las necesidades de su organización. Luego pulse el botón "Guardar" y cierre el editor de textos. 

5. CONFIGURACIÓN DE USUARIOS Y POLÍTICA DE CREDENCIALES

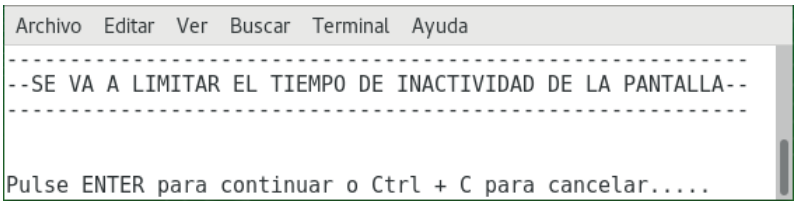
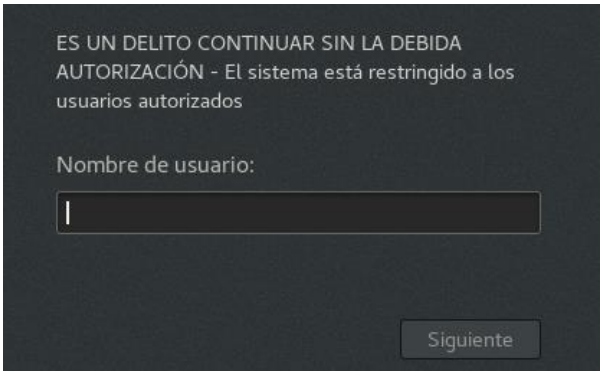
5.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

Paso	Descripción
41.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
42.	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-617-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. 
43.	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".**
44.	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
45.	Se mostrarán todos los usuarios y sus respectivas shells. Compruebe que todas las shells de usuario coinciden con "**/bin/bash**". Archivo Editar Ver Buscar Terminal Ayuda usuario@linux-yimq:/Scripts> sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd nobody:65534/bin/bash usuario:1000/bin/bash usuario2:1005/bin/bash usuario3:1006/bin/bash usuario@linux-yimq:/Scripts> **Nota:** Como se puede observar es posible que aparezca el usuario nfsnobody 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.
46.	Cuando finalice todas las tareas reinicie el sistema.

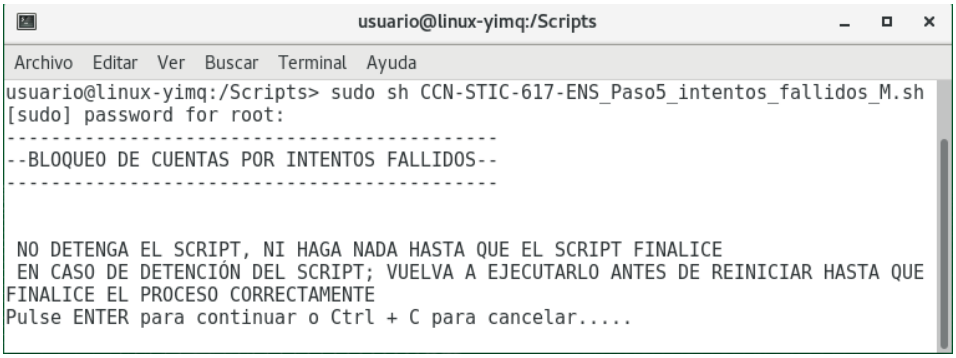
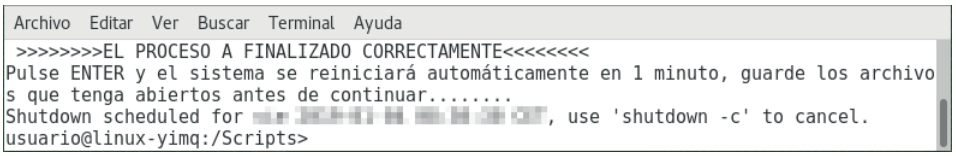
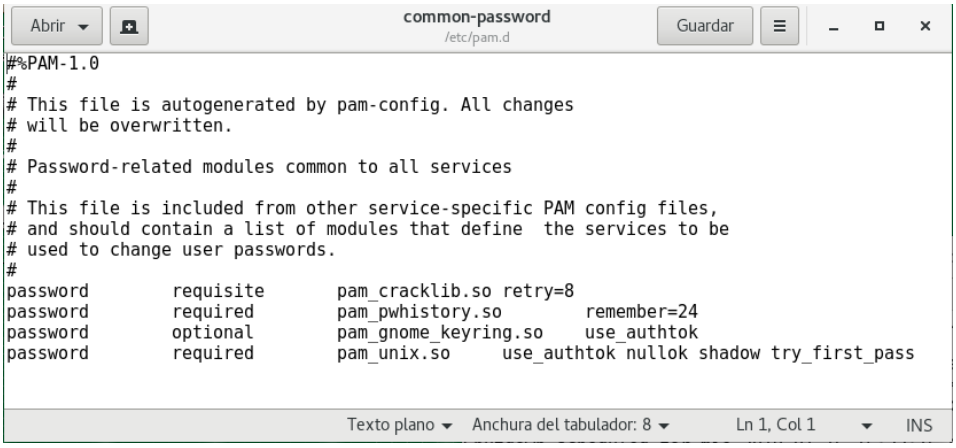
5.2. CONFIGURACIÓN SEGURA DE GNOME

Paso	Descripción
47.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
48.	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-617-ENS_Paso4_parametros_gnome_M.sh** Archivo Editar Ver Buscar Terminal Ayuda usuario@linux-yimq:/Scripts> sudo sh CCN-STIC-617-ENS_Paso4_parametros_gnome_M.sh ---------- --CREANDO UN BANNER Y MODIFICANDO PARÁMETROS DE INICIO DE SESIÓN-- ---------- Pulse ENTER para continuar o Ctrl + C para cancelar.....

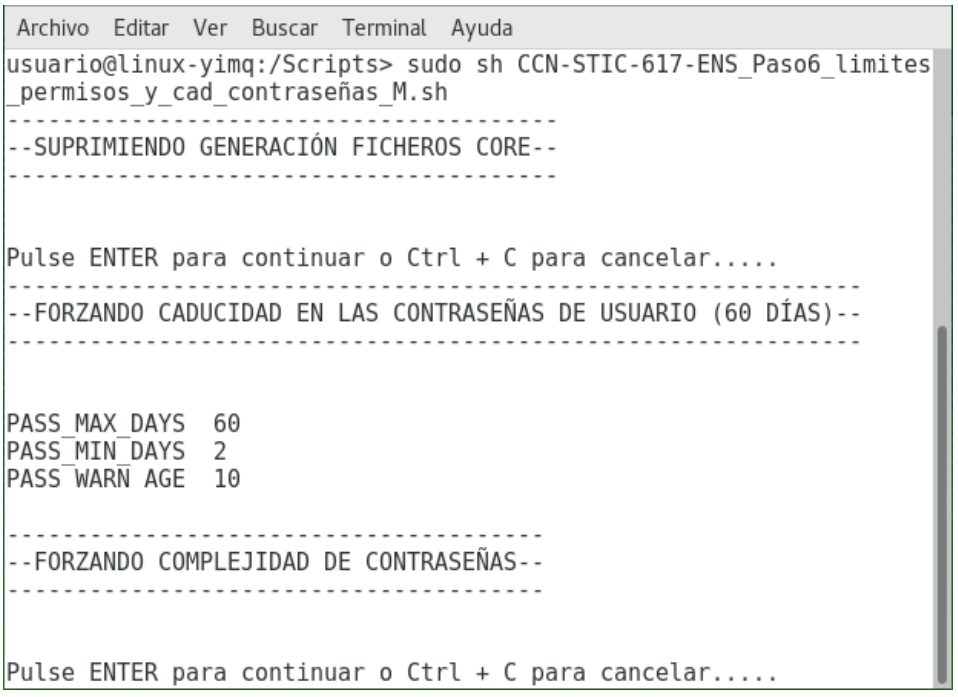
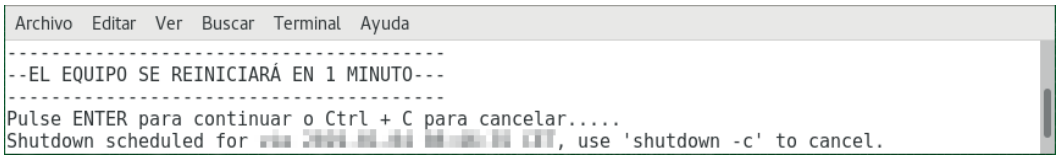
Paso	Descripción
49.	El script iniciará un proceso que modificará la pantalla de inicio de SUSE Enterprise Linux para que aparezca un mensaje disuasorio (banner) al inicio y solicite usuario y contraseña. Así mismo se configurará un tiempo mínimo de bloqueo según requisitos de seguridad.   **Nota:** SUSE Enterprise Linux 12 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.

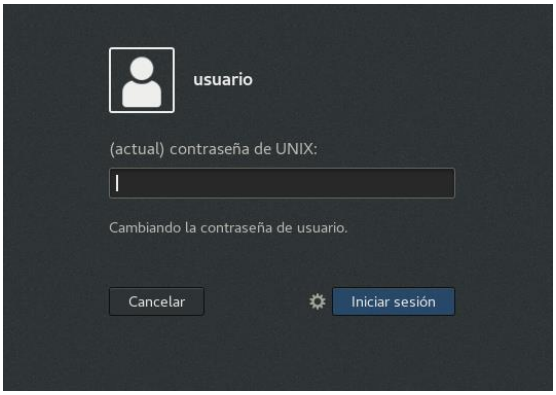
5.3. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS

Paso	Descripción
50.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
51.	Se procederá a configurar el bloqueo de cuentas por intentos fallidos, por medio de los módulos pam_tally2.so y cracklib.so. Para ello diríjase a la carpeta "Scripts". $ **cd /Scripts**
52.	Ejecute el siguiente script. $ **sudo sh CCN-STIC-617-ENS_Paso5_intentos_fallidos_M.sh**

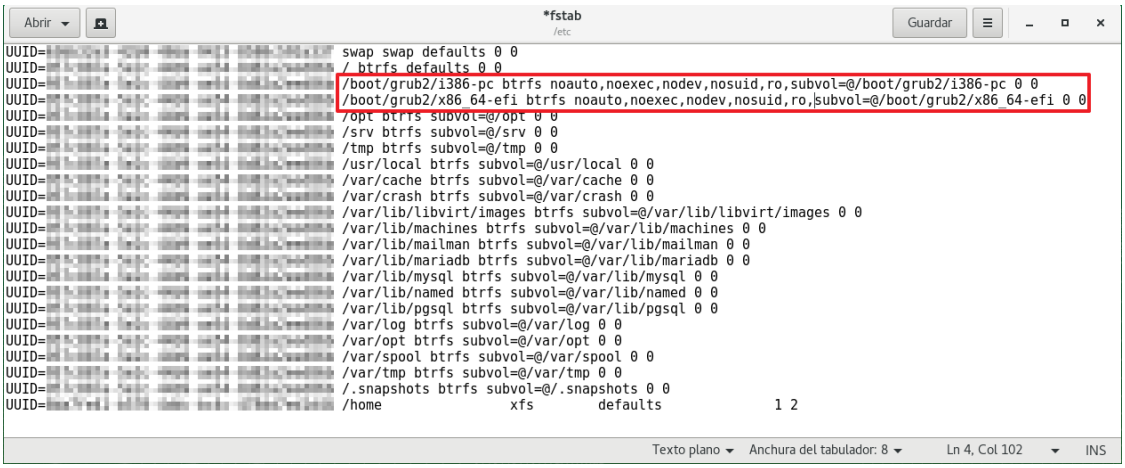
Paso	Descripción
53.	El script alertará de la pérdida de configuración en el fichero de configuración /etc/pam.d/common-auth, ya que el script añadirá una configuración que cumpla con los mínimos requisitos de seguridad.   **Nota:** Si el script se detuviera o no terminara correctamente, deberá de iniciarlo una vez más antes de reiniciar, por el contrario, es posible que el sistema no pueda iniciarse correctamente.
54.	Si quisiera editar los documentos con las necesidades de seguridad requeridos por su organización, ejecute los siguientes comandos dependiendo del fichero que desee modificar. **$ gnomesu gedit /etc/pam.d/common-password &>/dev/null** **$ gnomesu gedit /etc/pam.d/login &>/dev/null** **$ gnomesu gedit /etc/pam.d/su &>/dev/null** **$ gnomesu gedit /etc/pam.d/gdm &>/dev/null**  **Nota:** No modifique estos ficheros de configuración si no conoce el funcionamiento de los módulos **"pam.d"**, podría provocar que el sistema no iniciara correctamente.
55.	Una vez finalice pulse el botón "Guardar" y cierre el editor de texto. Reinicie el sistema para que los cambios queden aplicados.

5.4. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

Paso	Descripción
56.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
57.	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-617-ENS_Paso6_limites_permisos_y_cad_contraseñas_M.sh** 
58.	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
59.	Cuando reinicie el sistema e inicie sesión, saldrá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos. 
60.	Le pedirá la contraseña actual y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.
61.	A continuación, se muestra un ejemplo del fichero "/etc/security/limits.conf", con líneas comentadas (**"#"**) en el que se limitan ciertas partes para un usuario específico. Para modificar dicho fichero ejecute el siguiente comando. **$ gnomesu gedit /etc/security/limits.conf &>/dev/null** Abrir — *limits.conf /etc/security — Guardar #Where: #<domain> can be: # - a user name # - a group name, with @group syntax # - the wildcard *, for default entry # - the wildcard %, can be also used with %group syntax, # for maxlogin limit # #<type> can have the two values: # - "soft" for enforcing the soft limits # - "hard" for enforcing hard limits # #<item> can be one of the following: # - core - limits the core file size (KB) # - data - max data size (KB) # - fsize - maximum filesize (KB) # - memlock - max locked-in-memory address space (KB) # - nofile - max number of open file descriptors # - rss - max resident set size (KB) # - stack - max stack size (KB) # - cpu - max CPU time (MIN) # - nproc - max number of processes # - as - address space limit (KB) # - maxlogins - max number of logins for this user # - maxsyslogins - max number of logins on the system # - priority - the priority to run user process with # - locks - max number of file locks the user can hold # - sigpending - max number of pending signals # - msgqueue - max memory used by POSIX message queues (bytes) # - nice - max nice priority allowed to raise to values: [-20, 19] # - rtprio - max realtime priority # #<domain> <type> <item> <value> # # * hard core 0 #usuario hard rss 10000 # cantidad de memoria residente expresada en KB #usuario hard maxlogins 1 # numero máximo de conexiones para el usuario (usuario) #usuario hard nproc 15 # cantidad de procesos simultanos para el usuario (usuario) # End of file
62.	Modifique el fichero de configuración de la manera que más se adapte a las necesidades de su organización, pulse el botón "**Guardar**" y cierre el editor de texto.

6. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

Paso	Descripción
63.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
64.	Ejecute el siguiente comando. **$ gnomesu gedit /etc/fstab &>/dev/null**
65.	Edite el fichero de configuración y modifique los permisos de la partición "**/boot**" para que el resultado sea similar al de la imagen (noauto, noexec, nodev, nosuid, ro). 
66.	Cuando termine, pulse el botón "**Guardar**" y cierre el editor de texto. Elimine el directorio "/Scripts" y todo su contenido.

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE CLIENTE SUSE ENTERPRISE LINUX 12 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 SERVIDORES SUSE ENTERPRISE LINUX 12 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

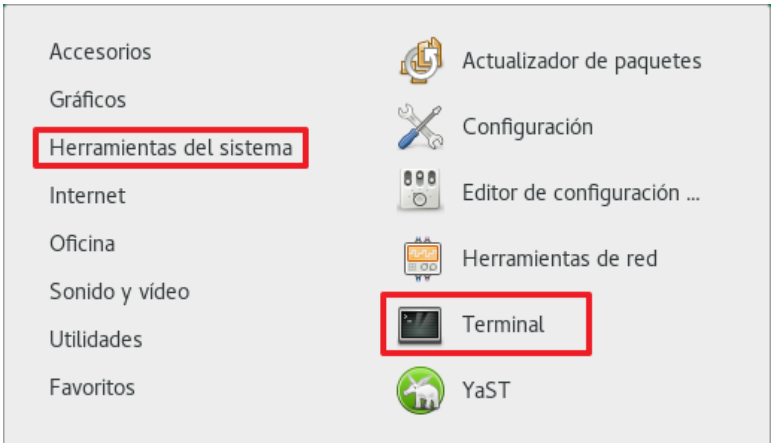
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores SUSE Enterprise 12 Linux independientes con implementación de seguridad de categoría media del ENS.

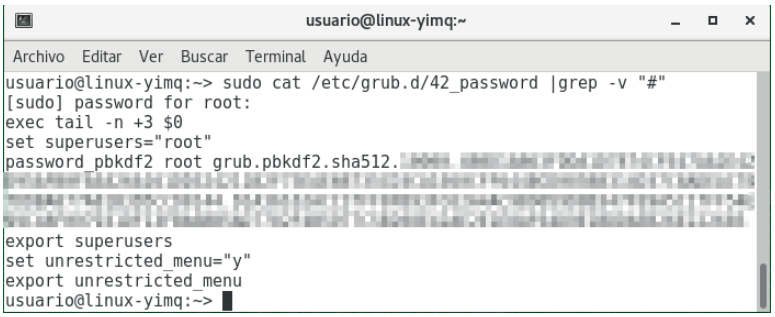
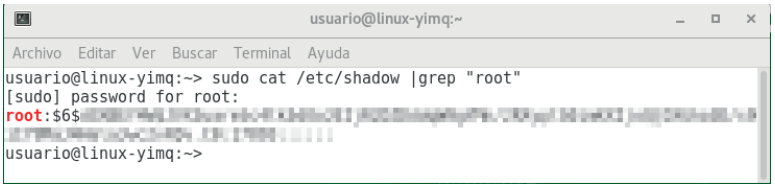
Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

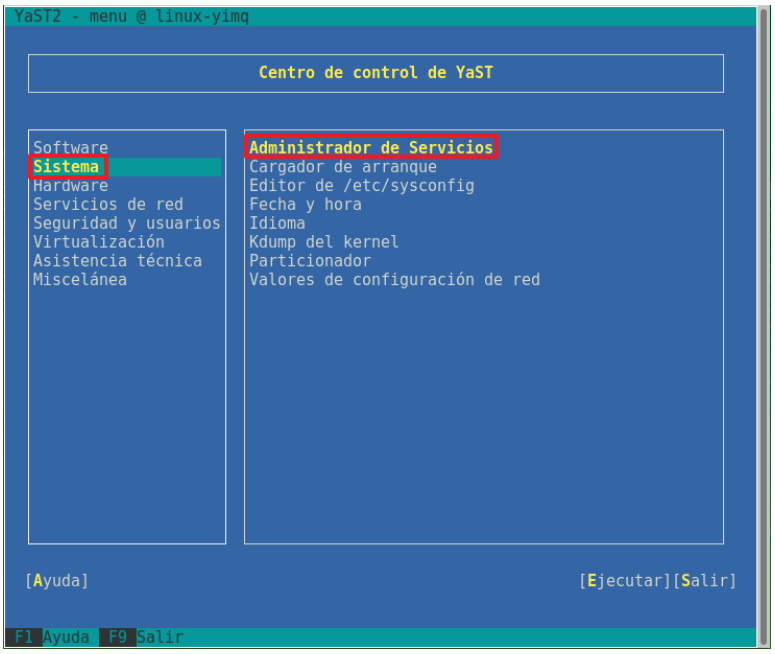
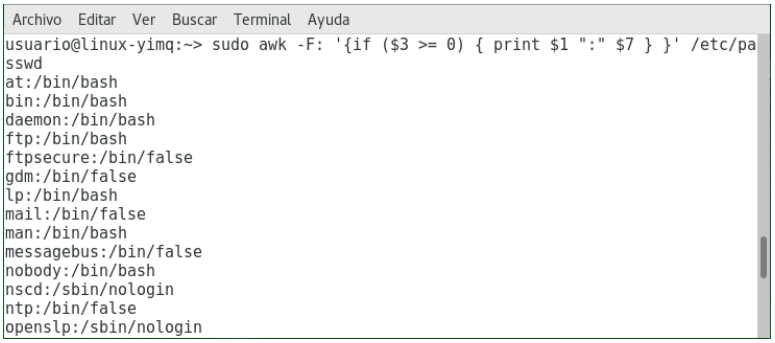
Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas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

a) Terminal de Linux

b) Herramienta YaST

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 de la categoría 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, pulse en Aplicaciones y en el apartado "Herramientas del sistema" seleccione "Terminal". 

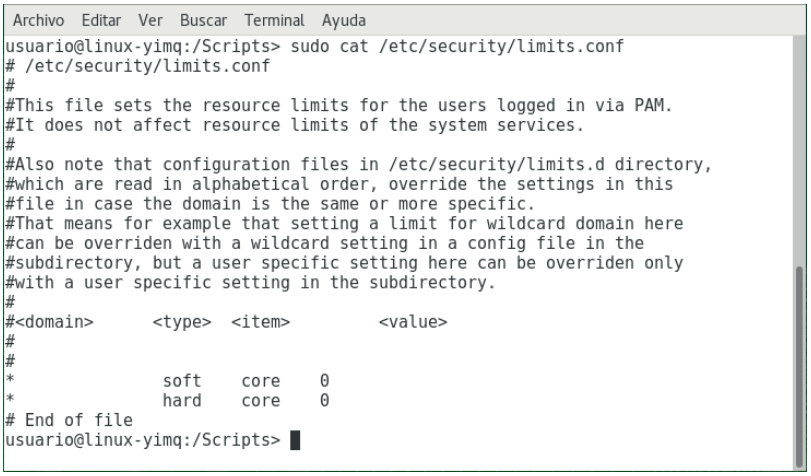
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que grub tiene contraseña configurada y root como único usuario de modificación.		En la "Terminal" ejecute el siguiente comando. **$ sudo cat /etc/grub.d/42_password |grep -v "#"**  **Nota:** Fíjese en las letras y números que están situadas después de "**password_pbkdf2 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.
5. Búsqueda de usuarios sin contraseña.		Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1**
6. Búsqueda de usuarios con UID 0.		Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1 |grep -v "root"**

Comprobación	OK/NOK	Cómo hacerlo
7. Servicios innecesarios por medio de herramienta ntsysv		Abra la Terminal y ejecute el siguiente comando. **$ sudo yast**  Revise que los servicios activos al iniciar el sistema son los correctos para su organización.
8. Comprobación de usuarios y shells predetermina-das.		Ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 0) { print $1 ":" $7 } }' /etc/passwd**  Compruebe si los usuarios que se muestran son los más adecuados para su organización y que están correctas las shells predeterminadas.

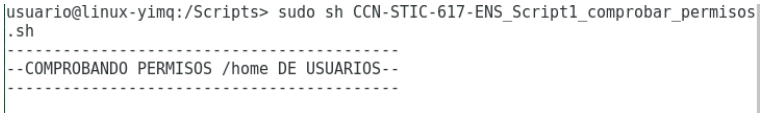
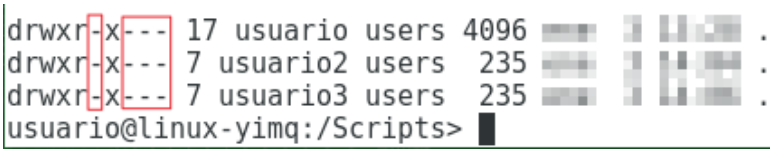
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="5">9. Comprobación de registros de actividad</td><td></td><td>Primero se va a comprobar el fichero de configuración, con los parámetros definidos por esta guía.
Ejecute los siguientes comandos.
$ sudo cat /etc/audit/auditd.conf |grep "max_log_file ="
$ sudo cat /etc/audit/auditd.conf |grep "num_logs ="
$ sudo cat /etc/audit/auditd.conf |grep "max_log_file_action ="</td></tr>
<tr><td colspan="3"><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>
</table></td></tr>
<tr><td></td><td>Se procede a visualizar la totalidad del fichero de configuración del demonio auditd para que pueda revisar los parámetros específicos de su organización.
$ sudo cat /etc/audit/auditd.conf
Archivo Editar Ver Buscar Terminal Ayuda
linux-yimq:/home/usuario # sudo cat /etc/audit/auditd.conf
#
This file controls the configuration of the audit daemon
#

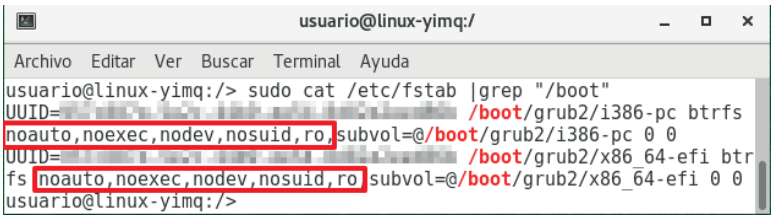
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 12
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 10
max_log_file_action = ROTATE
space_left = 75</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></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/login
– /etc/pam.d/su
– /etc/pam.d/gdm
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/login |grep "auth" |grep "pam_tally2" |grep "deny="
$ sudo cat /etc/pam.d/login |grep "auth" |grep "pam_tally2" |grep "unlock_time="
$ sudo cat /etc/pam.d/su |grep "auth" |grep "pam_tally2" |grep "deny="
$ sudo cat /etc/pam.d/su |grep "auth" |grep "pam_tally2" |grep "unlock_time="
$ cat /etc/pam.d/gdm |grep "auth" |grep "pam_tally2" |grep "deny="
$ cat /etc/pam.d/gdm |grep "auth" |grep "pam_tally2" |grep "unlock_time="</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>auth required</td><td>pam_tally2.so</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td><td>– /etc/pam.d/common-passwd
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/common-password |grep "requisite" |grep "cracklib" |grep "retry="</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>retry</td><td>8</td><td></td></tr>
</table></td></tr>
</table>

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

Nota: Si ha hecho modificaciones personalizadas para su organización con respecto a limitación de recursos por usuarios, las puede revisar en este apartado.</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>
<tr><td>13. Verifique la directiva de caducidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ cat /etc/login.defs |grep "PASS_MAX_DAYS"
$ cat /etc/login.defs |grep "PASS_MIN_DAYS"
$ cat /etc/login.defs |grep "PASS_MIN_LEN"
$ cat /etc/login.defs |grep "PASS_WARN_AGE"
$ cat /etc/login.defs |grep "UMASK"
Compruebe si se han configurado bien los valores.</td></tr>
<tr><td></td><td colspan="2"><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>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>14. Verifique la directiva de complejidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/common-password |grep "minlen="
$ sudo cat /etc/pam.d/common-password |grep "dcredit="
$ sudo cat /etc/pam.d/common-password |grep "ucredit="
$ sudo cat /etc/pam.d/common-password |grep "lcredit="
$ sudo cat /etc/pam.d/common-password |grep "ocredit="</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>
<tr><td>ocredit</td><td>-1</td><td></td></tr>
</table></td></tr>
<tr><td>15. 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”.
$ sudo cd /Scripts
Ejecute el siguiente comando.
$ sudo sh CCN-STIC-617-ENS_Script1_comprobar_permisos.sh
 
El script mostrará los permisos de las carpetas “/home” y se debe comprobar que las columnas marcadas se encuentren vacías.
  </td></tr>
<tr><td>16. 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.
$ sudo cat /etc/dconf/db/gdm.d/01-banner-message</td></tr>
<tr><td colspan="3"><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></td></tr>
<tr><td></td><td></td><td>$ sudo cat /etc/dconf/db/gdm.d/00-login-screen |grep "disable-user-list"</td></tr>
<tr><td colspan="3"><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 rowspan="11"></td><td></td><td>$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "idle-delay=uint32"
$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "lock-enabled"
$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "lock-delay=uint32"</td></tr>
<tr><td colspan="2"><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>1</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "automount="
$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "automount-open="
$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "autorun-never="</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>automount</td><td>false</td><td></td></tr>
<tr><td>automount-open</td><td>false</td><td></td></tr>
<tr><td>autorun-never</td><td>true</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "hide-identity"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "old-files-age"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "remember-recent-files"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep " remove-old-temp-files"</td></tr>
<tr><td colspan="2"><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>17. 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 SERVIDORES SUSE ENTERPRISE LINUX 12 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores SUSE Enterprise Linux 12 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.

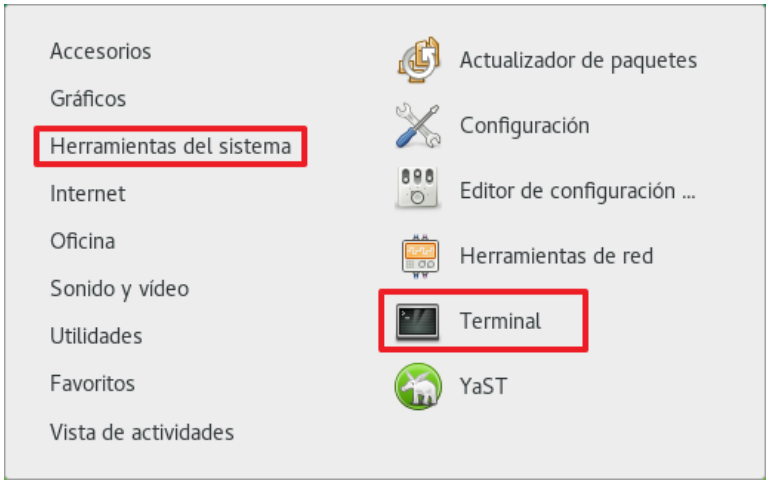
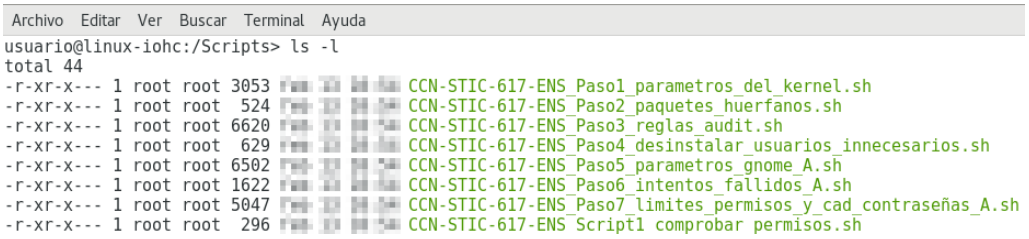
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender a las peculiaridades del sistema operativo utilizado en el caso de una red de este tipo.

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.

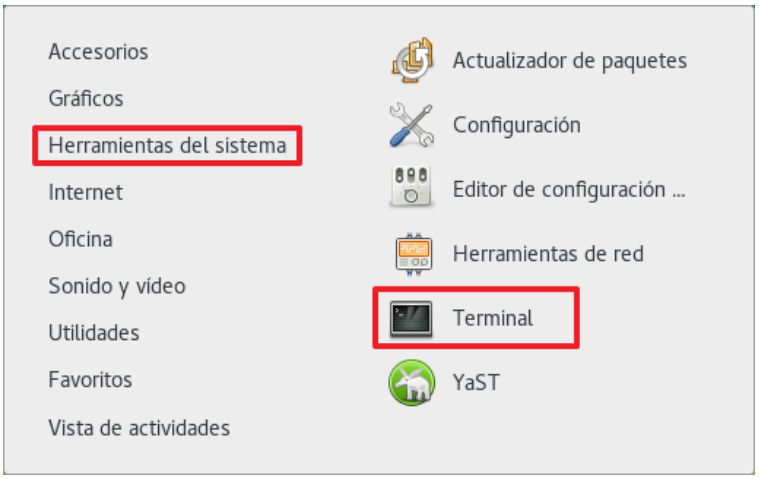
Los pasos que se describen a continuación se realizarán en todos aquellos servidores SUSE Enterprise Linux 12, independientes a un dominio, que implementen servicios o información de categoría alta – DL y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

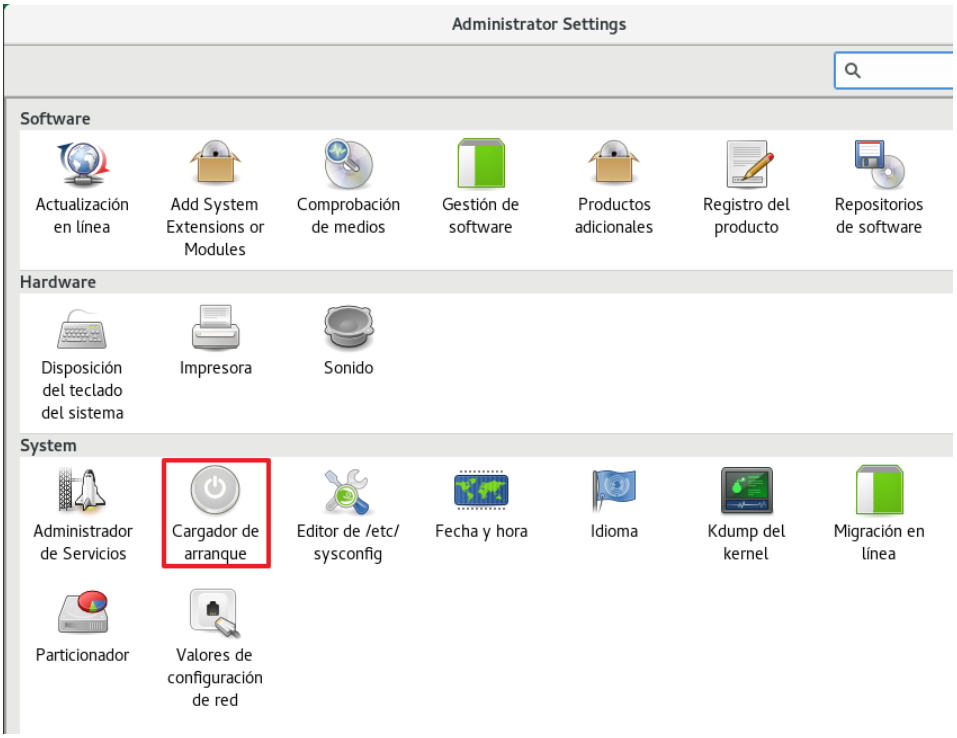
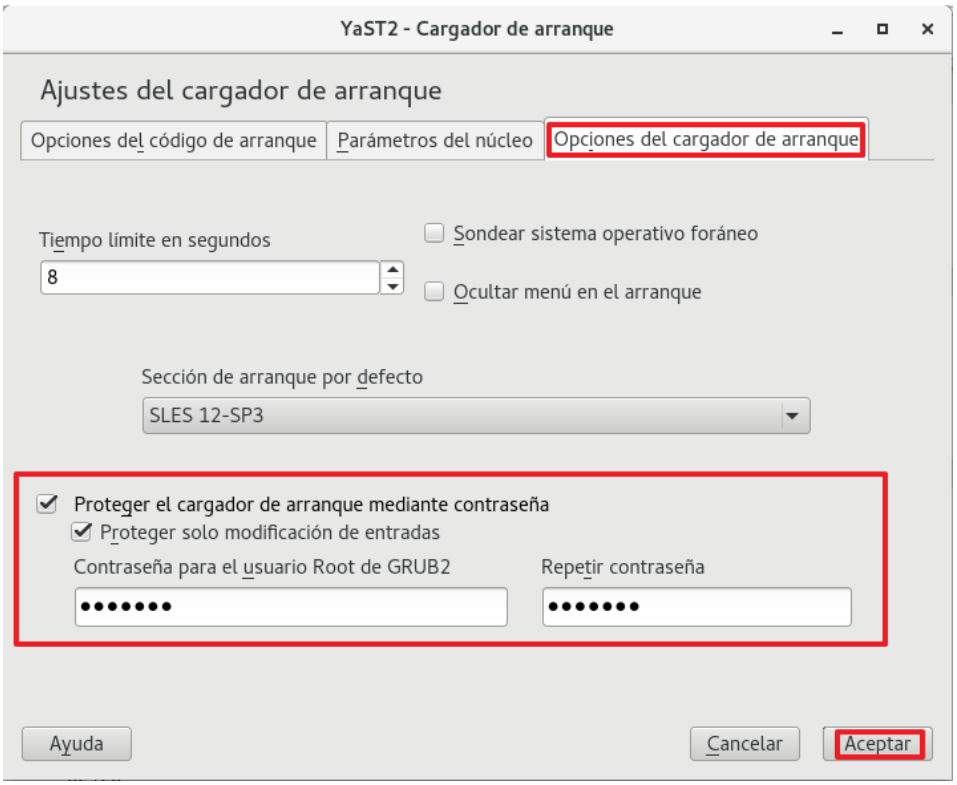
1. CONFIGURACIÓN SEGURA DEL ARRANQUE DEL SISTEMA

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 “CATEGORIA_ALTA_DL” correspondiente al directorio “Scripts/ENS_CATEGORIA_ALTA_DL” asociado a esta guía en la ruta “**/Scripts**”.

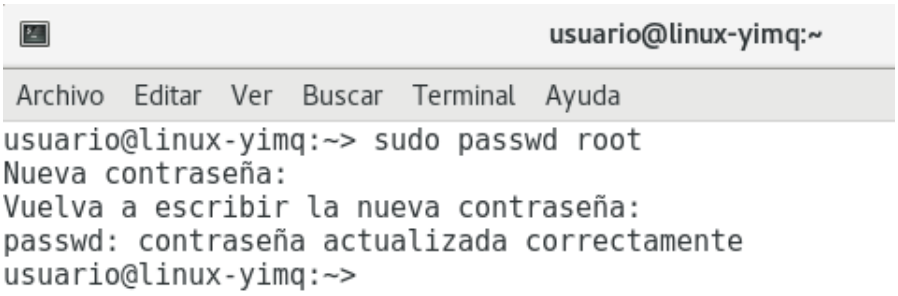
Paso	Descripción
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando **“cd /Scripts”** y pulse la tecla “Enter”.
6.	Posteriormente ejecute “**ls -l**” y compruebe que están todos los scripts. 

1.1. CONTRASEÑA DE GRUB

Paso	Descripción
7.	Se procede a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “YaST”. 

Paso	Descripción
8.	Introduzca la contraseña cuando se le solicite y aparecerá la siguiente pantalla. Pulse el icono “Cargador de arranque”. 
9.	Una vez se encuentre en la ventana “YaST2 – Cargador de arranque”, despliegue la pestaña Opciones del cargador de arranque y habilite “Proteger el cargador de arranque mediante contraseña” y “Proteger solo modificación de entradas”. Posteriormente pulse “Aceptar”. 

1.2. CONTRASEÑA SEGURA DE ROOT

Paso	Descripción
10.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
11.	Ejecute el siguiente comando. $ **sudo passwd root**
12.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se procederá a actualizar. Se pedirá la nueva contraseña y la confirmación de la misma. 
13.	Cuando el proceso haya terminado se mostrará el siguiente mensaje. "passwd: contraseña actualizada correctamente". Si no muestra ese mensaje, vuelva repetir los pasos anteriores.

1.3. BÚSQUEDA DE CUENTAS SIN CONTRASEÑA

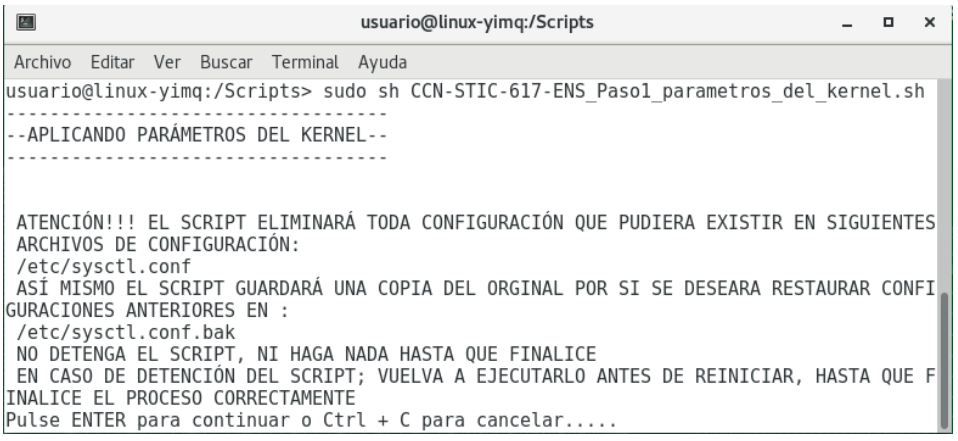
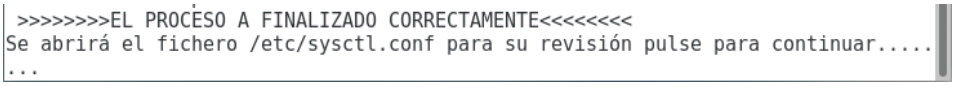
Paso	Descripción
14.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
15.	Ejecute el siguiente comando. $ **sudo 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 "6.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

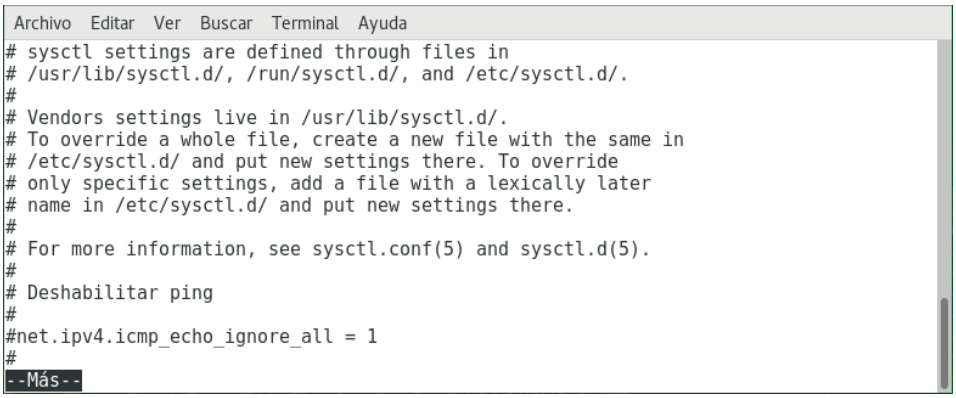
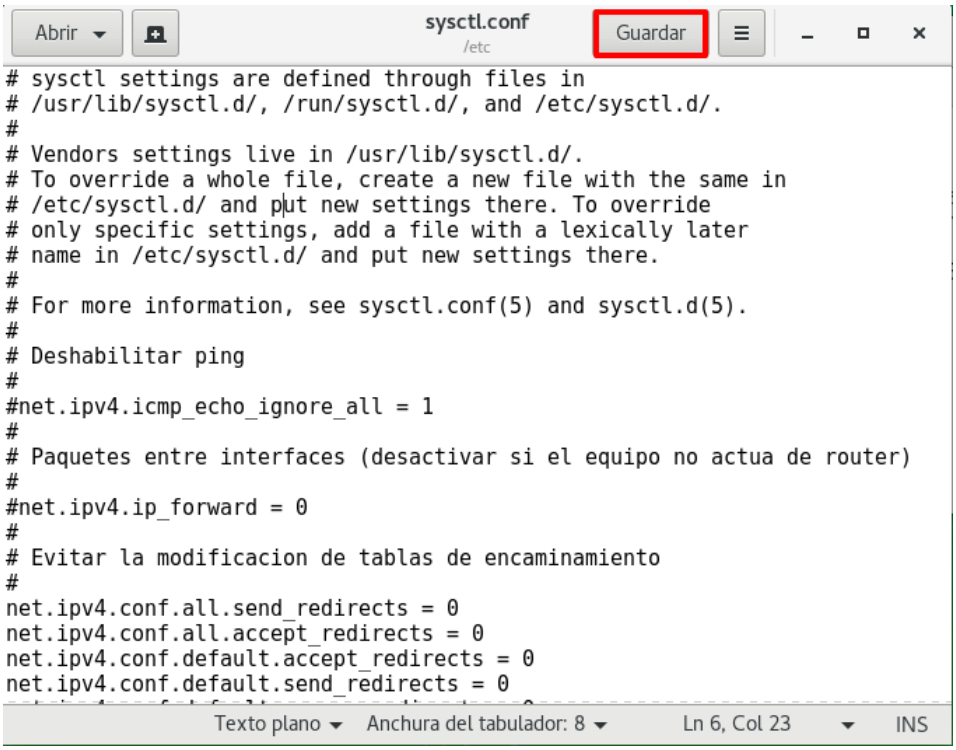
1.4. USUARIOS CON UID 0 QUE NO SEAN ROOT

Paso	Descripción
17.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".

Paso	Descripción
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 "6.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS".

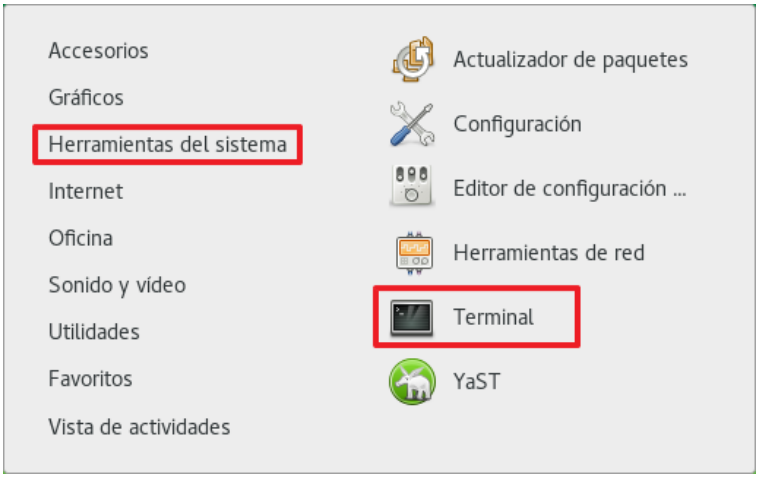
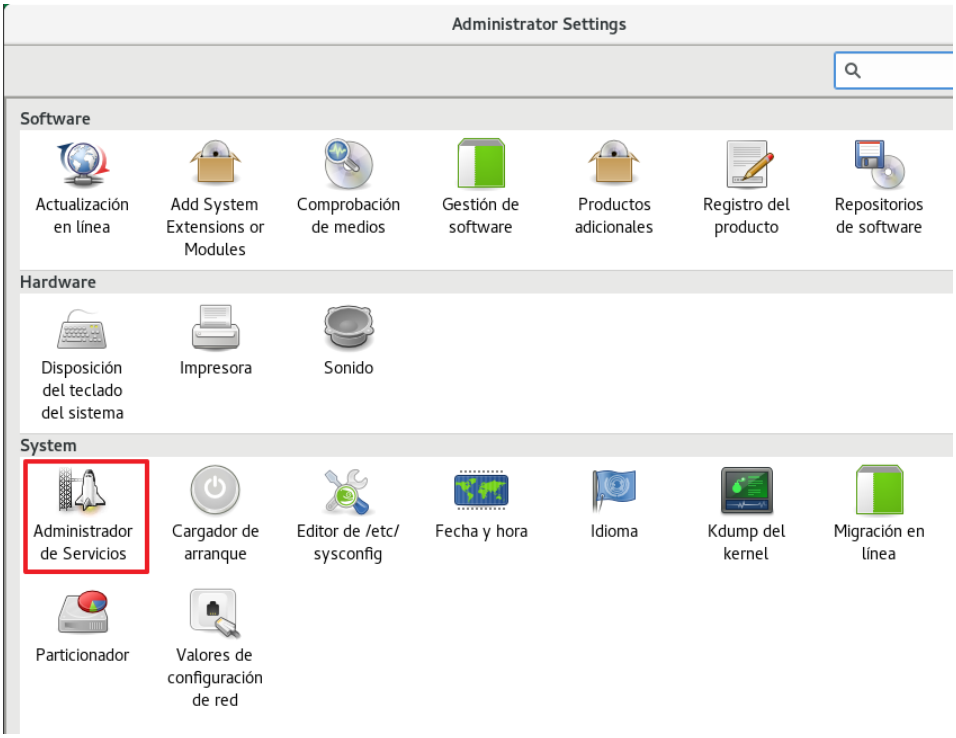
2. FORTIFICACIÓN DE KERNEL

Paso	Descripción
20.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**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". **$ sudo cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso1_parametros_del_kernel.sh**
23.	El script alertará de la pérdida de configuración en el fichero /etc/sysctl.conf, ya que el script añadirá una configuración que cumpla con los mínimos de seguridad. 
24.	Cuando la configuración predeterminada finalice, pulse "Enter" y se mostrará el fichero de configuración. 

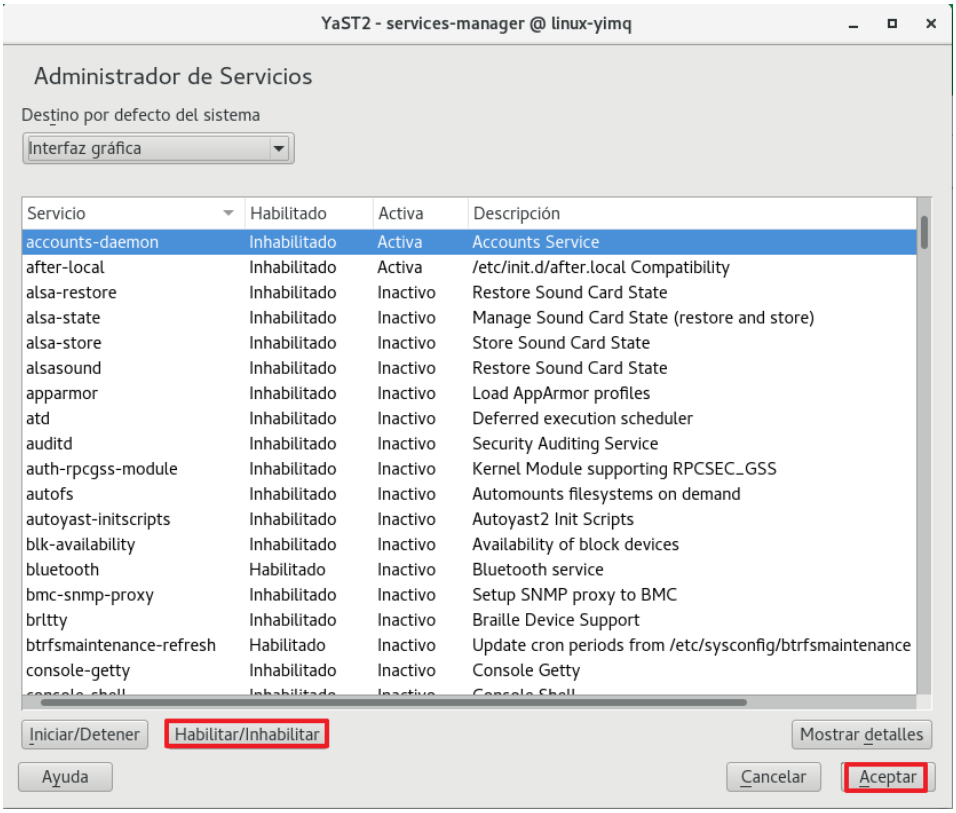
Paso	Descripción
25.	Se puede observar que hay ciertos parámetros que no están actuando. Una vez revisadas las necesidades particulares de su organización, pulse “q” para salir, el script informará de que el equipo se va a reiniciar. Guarde los documentos que tenga abiertos y pulse “Enter” para reiniciar. 
26.	Si fuera necesario, modificar algún parámetro, edite el fichero “/etc/sysctl.conf”, después de reiniciar, con el siguiente comando. **$ gnomesu gedit /etc/sysctl.conf &>/dev/null** Habilite, deshabilite o añada según las necesidades de su organización. 
27.	Cuando finalice, guarde y cierre el editor de texto pulsando el botón “Guardar” y cerrando la ventana.

3. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

3.1. LIMITACIÓN DE SERVICIOS Y DEMONIOS

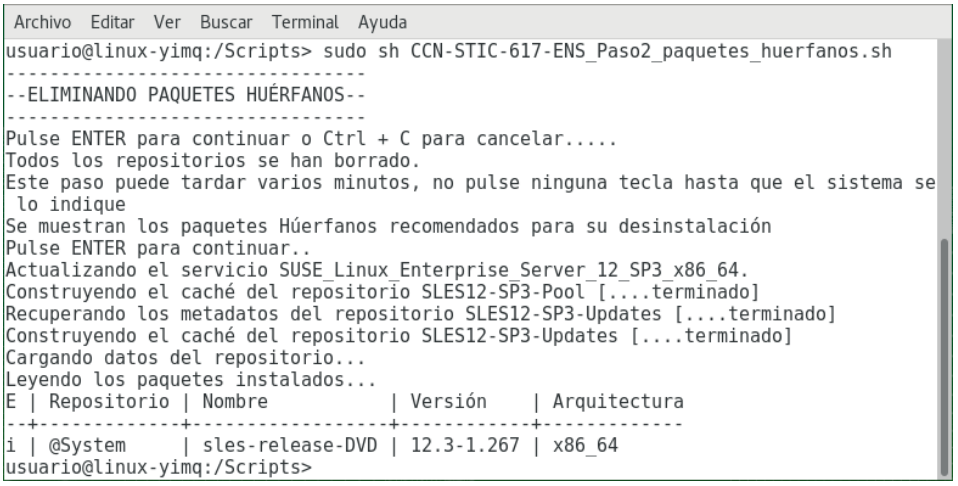
Paso	Descripción
28.	Se procede a deshabilitar servicios y demonios innecesarios. Para ello diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “YaST”. 
29.	Introduzca la contraseña cuando se le solicite y aparecerá la siguiente pantalla. Pulse entonces el icono “Administrador de Servicios”. 

Paso	Descripción
30.	Una vez se encuentre en la ventana "YaST2 – services-manager", revise los servicios y habilite o inhabilite según las necesidades de su organización. Posteriormente pulse el botón "Aceptar".

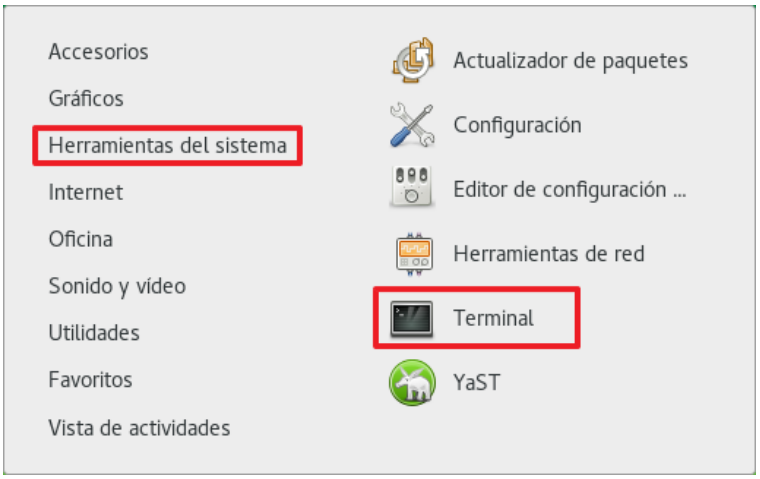


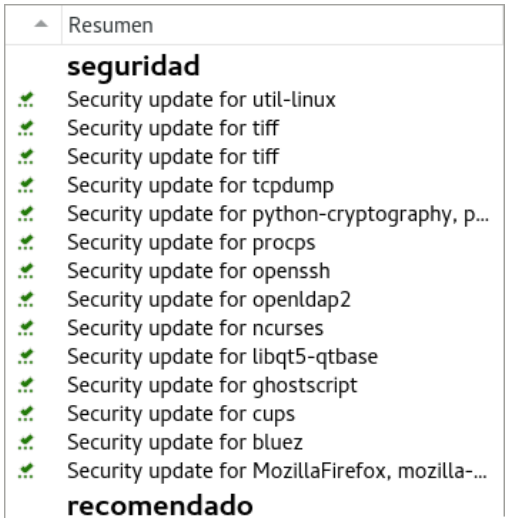
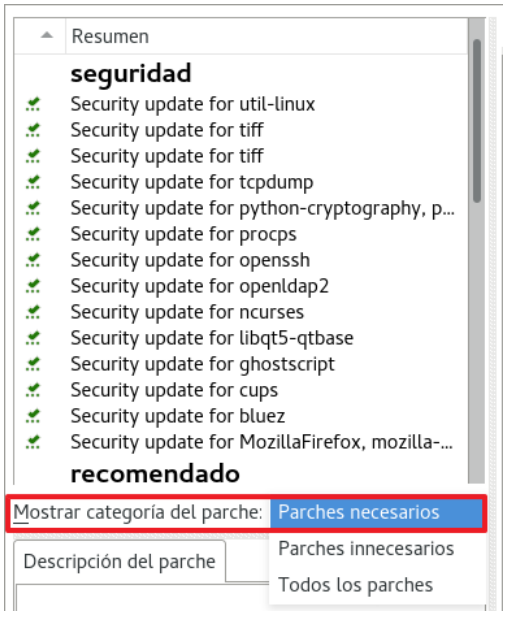
3.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

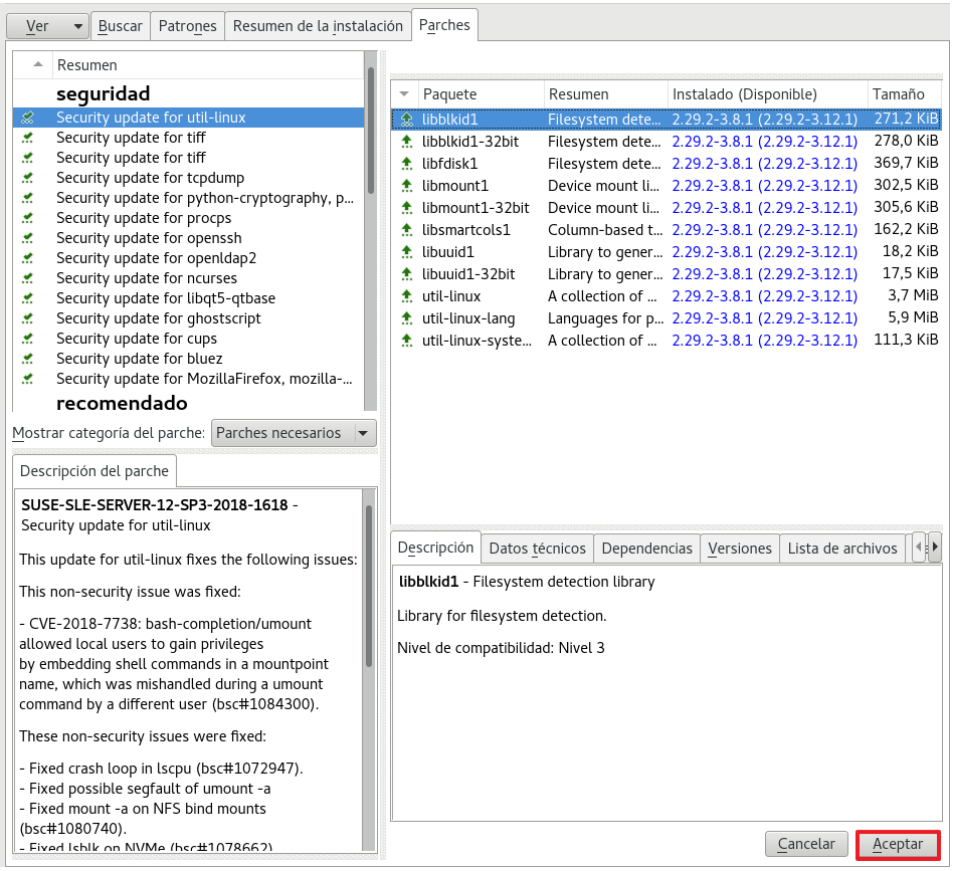
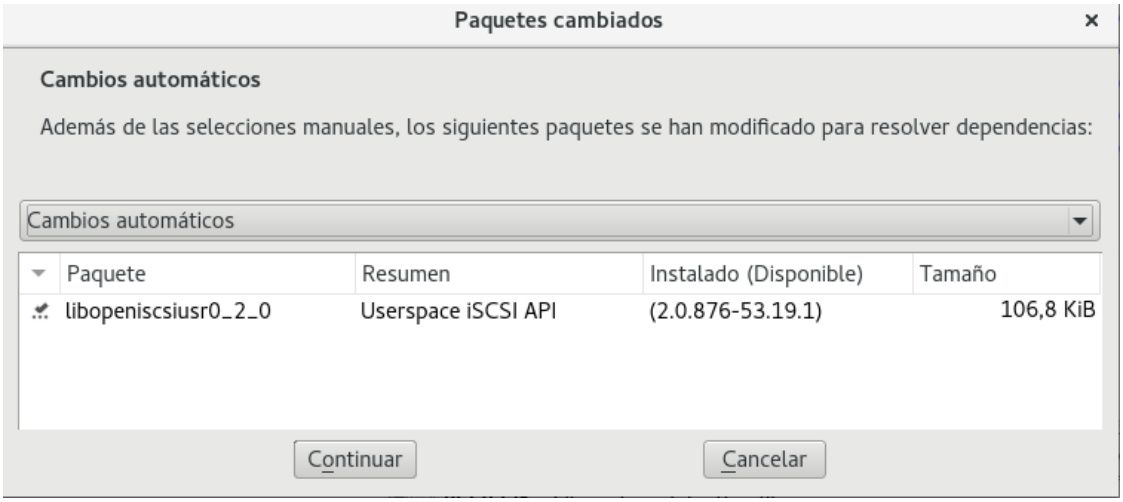
Paso	Descripción
31.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
32.	Se procederá a revisar los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta "Scripts". `$ cd /Scripts`

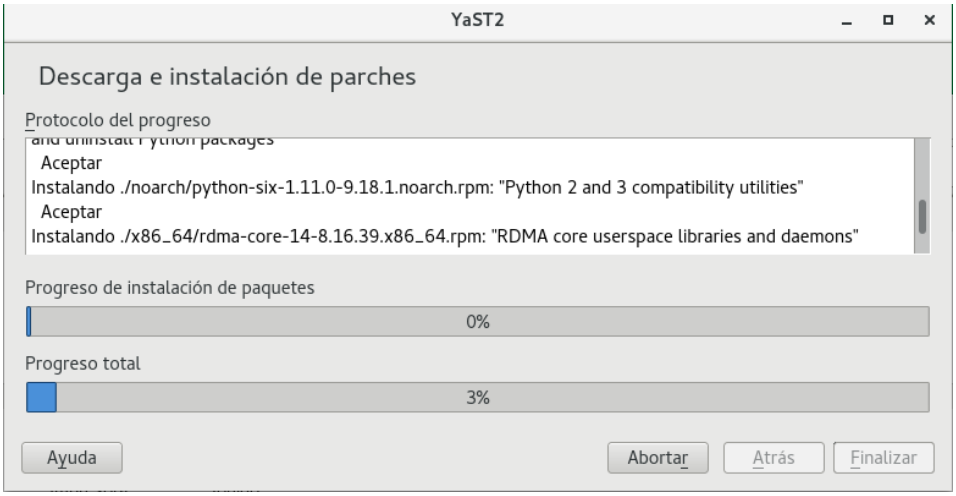
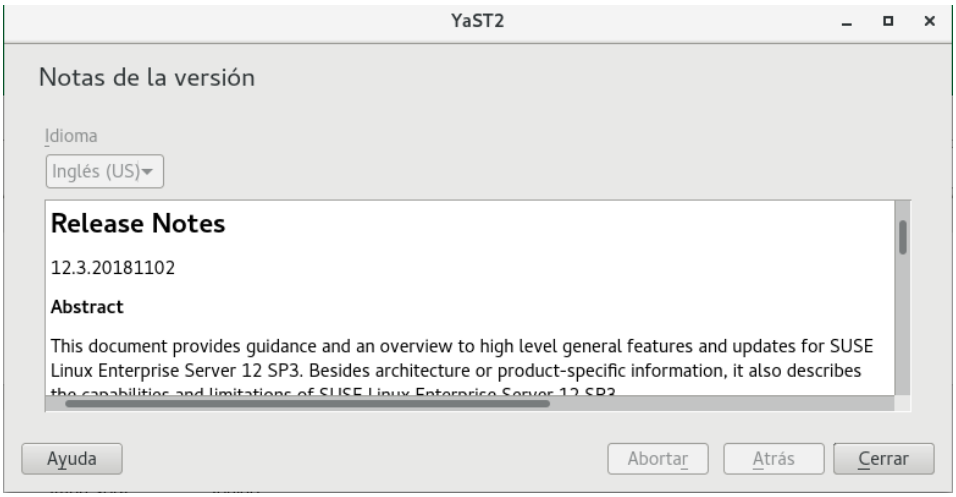
Paso	Descripción
33.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso2_paquetes_huerfanos.sh** El script iniciará un proceso de comprobación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que se lo indique o finalice, se mostrarán los paquetes huérfanos candidatos para su desinstalación, así mismo se copiarán en el archivo "orphaned.txt" que se generará en la misma ruta del script.  **Nota:** Si el script detectara algún programa o repositorio candidato para su desinstalación, una vez finalice la desinstalación, se recomienda volver al inicio de este apartado y volver a ejecutar el script, para eliminar posibles paquetes huérfanos. La desinstalación deberá hacerse manualmente.

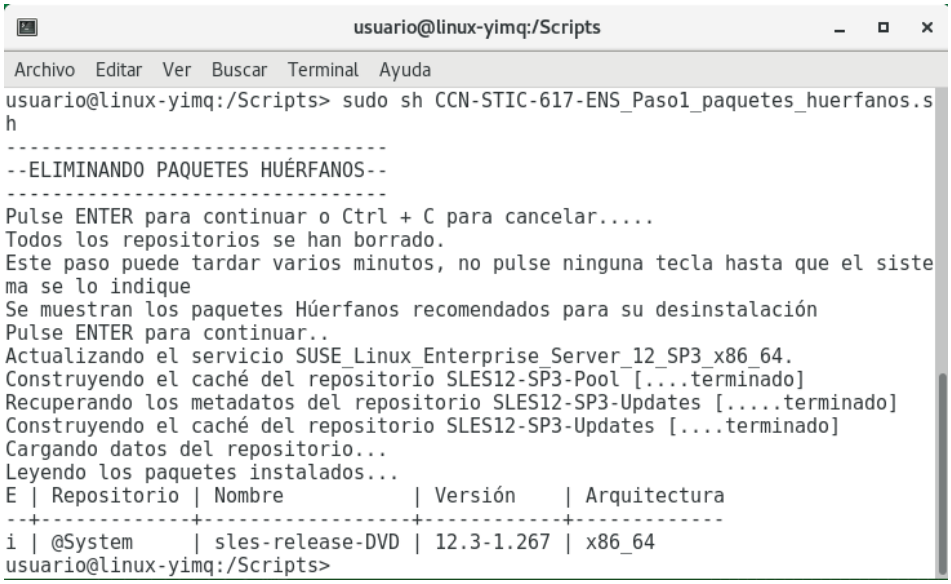
4. APLICACIÓN DE ACTUALIZACIONES

Paso	Descripción
34.	Diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "YaST". Introduzca la contraseña necesaria para elevar privilegios. Y pulse "Continuar". 

Paso	Descripción
35.	En el apartado “Software” dirijase al icono “Actualización en línea” y haga clic en él. 
36.	En la columna de la izquierda aparecerá un cuadro resumen con las actualizaciones de seguridad y las recomendadas. 
37.	Debe comprobar que en el apartado “Mostrar categoría del parche:” esta seleccionado “Parches necesarios”. 

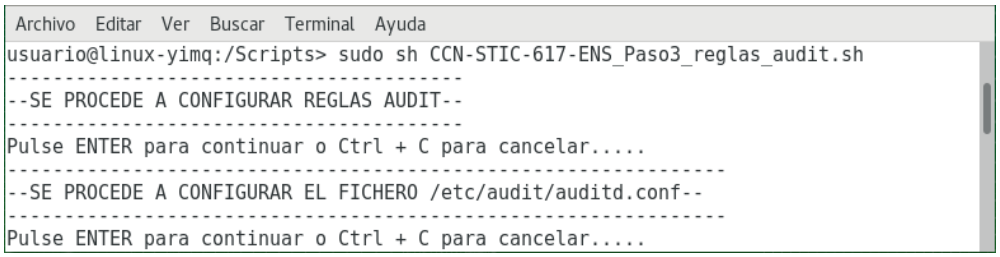
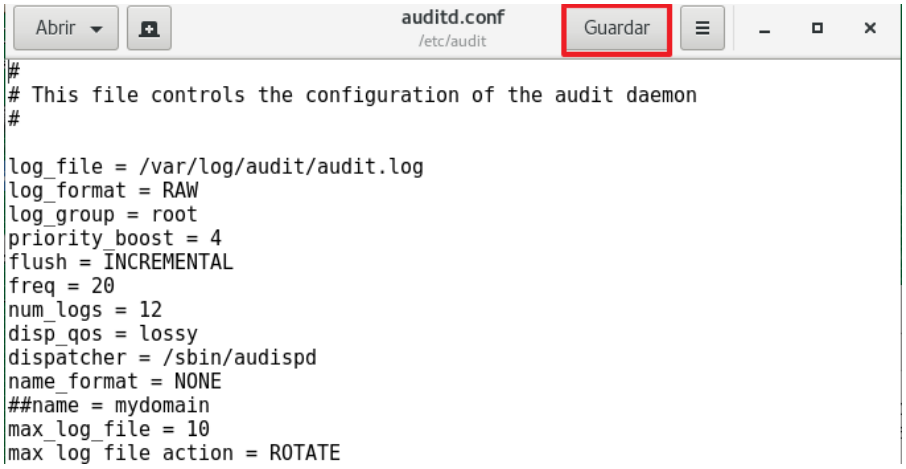
Paso	Descripción
38.	Si pulsa sobre alguna de las actualizaciones se verá un resumen de las mismas. Elija las actualizaciones de los parches que más convengan para su organización. Una vez realizada las comprobaciones pertinentes pulse el botón “Aceptar”. 
39.	Si hubiera alguna modificación en actuales paquetes instalados, el programa de actualización lo comunicará. Revise los paquetes que modifica y escoja las opciones que más convengan a su organización. En cualquier caso, pulse el botón “Continuar” para seguir con la instalación. 

Paso	Descripción
40.	El programa comenzará la instalación de las actualizaciones, no pulse ninguna tecla hasta la finalización de las mismas. 
41.	Al finalizar YaST2 mostrará las Notas de versión actualizadas. 
42.	Una vez finalizada la actualización, vuelva a ejecutar el script "CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh" del punto "3.2 COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS". Para ello diríjase a la barra de tareas, pulse en "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "Terminal". Ejecute el comando **"cd /"** y pulse la tecla **"Enter".**

Paso	Descripción
43.	Diríjase a la carpeta **"/Scripts/"** y ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso1_paquetes_huerfanos.sh** El script iniciará un proceso de comprobación de dichos paquetes, no pulse ninguna tecla ni cierra la ventana hasta que finalice, se mostrarán los paquetes huérfanos candidatos para su desinstalación, así mismo se copiarán en el archivo "orphaned.txt" que se generará en la misma ruta del script. 

5. CONFIGURACIÓN DE REGISTROS DE ACTIVIDAD

Paso	Descripción
44.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
45.	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**

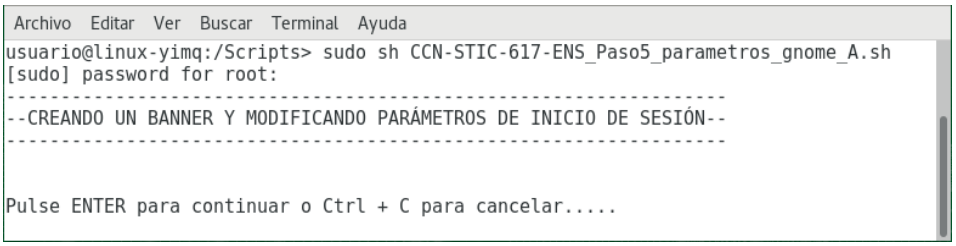
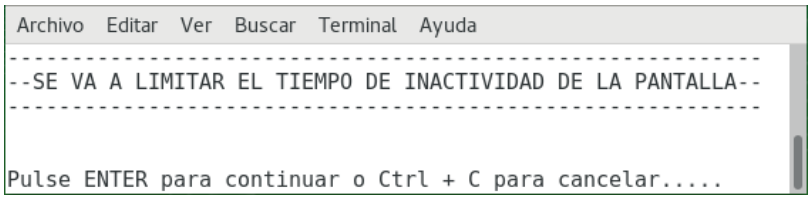
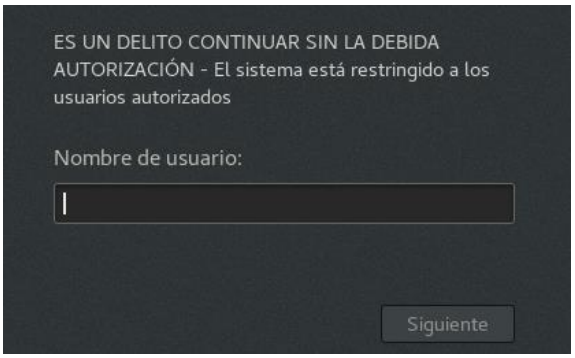
Paso	Descripción
46.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso3_reglas_audit.sh** El script finalizará mostrando las reglas creadas. Si el sistema indicara lo contrario vuelva a ejecutar de nuevo el script.  **Nota:** El script añade los parámetros necesarios al fichero de configuración **"/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".**
47.	Ajuste esta configuración con los parámetros necesarios para su organización. Para ello ejecute el siguiente comando. **$ gnomesu gedit /etc/audit/auditd.conf &>/dev/null**
48.	Modifique los parámetros marcados según las necesidades de su organización. Luego pulse el botón "Guardar" y cierre el editor de textos. 

6. CONFIGURACIÓN DE USUARIOS Y POLÍTICA DE CREDENCIALES

6.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

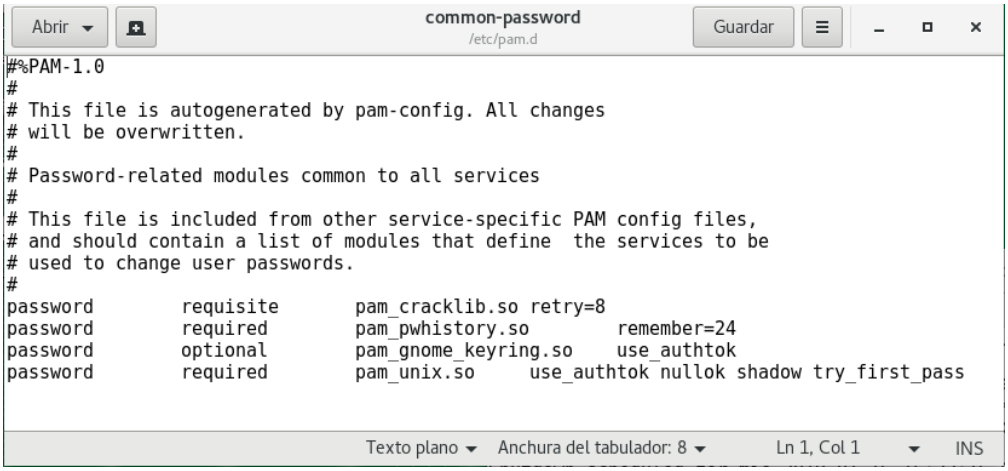
Paso	Descripción
49.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
50.	Se va a proceder a eliminar los usuarios creados por defecto en la instalación y que son innecesarios. Para ello diríjase a la carpeta "Scripts". **$ sudo cd /Scripts**
51.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-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. Archivo Editar Ver Buscar Terminal Ayuda usuario@linux-yimq:/Scripts> sudo sh CCN-STIC-617-ENS_Paso4_desinstalar_usuarios_innecesarios.sh ---------- --DESINSTALANDO USUARIOS INNECESARIOS-- ---------- Pulse ENTER para continuar o Ctrl + C para cancelar.....
52.	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".**
53.	Ahora compruebe las "shells" predeterminadas de los usuarios con UID por encima del **1000** (usuarios normales del sistema). Para ello ejecute el siguiente comando. **$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd**
	Se mostrarán todos los usuarios y sus respectivas shells. Compruebe que todas las shells de usuario coinciden con "**/bin/bash**". usuario@C7CL01:/Scripts Archivo Editar Ver Buscar Terminal Ayuda [usuario@C7CL01 Scripts]$ sudo awk -F: '{if ($3 >= 1000) { print $1 ":" $3 $7 } }' /etc/passwd nfsnobody:65534/sbin/nologin usuario:1000/bin/bash [usuario@C7CL01 Scripts]$ **Nota:** Como se puede observar puede aparecer el usuario nfsnobody 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.
54.	Cuando finalice todas las tareas reinicie el sistema.

6.2. CONFIGURACIÓN SEGURA DE GNOME

Paso	Descripción
55.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**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**
57.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-617-ENS_Paso5_parametros_gnome_A.sh** 
58.	El script iniciará un proceso que modificará la pantalla de inicio de SUSE Enterprise 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:** SUSE Enterprise Linux 12 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.

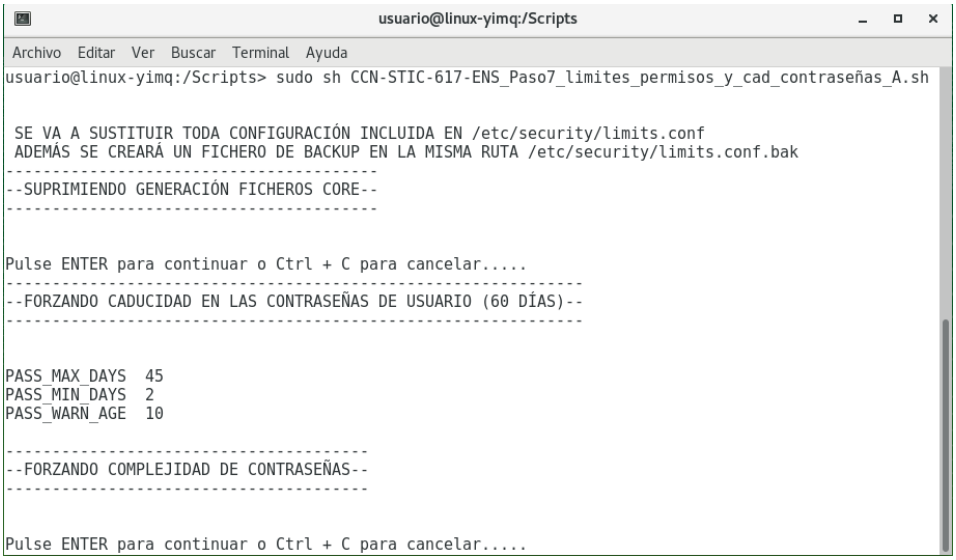
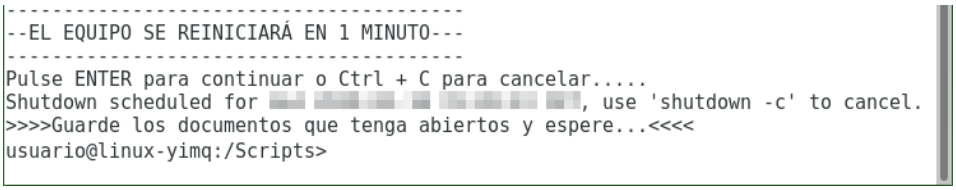
6.3. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS

Paso	Descripción
59.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
60.	Se procederá a configurar el bloqueo de cuentas por intentos fallidos, por medio de los módulos pam_tally2.so y cracklib.so. Para ello diríjase a la carpeta "Scripts". **$ sudo cd /Scripts**
61.	Ejecute el siguiente script. **$ sudo sh CCN-STIC-617-ENS_Paso6_intentos_fallidos_A.sh**
62.	El script alertará de la creación de la carpeta "pam.d_backup[fecha/hora]" en la ruta "/etc/" . Hay que tener en cuenta que el script generará una copia de seguridad cada vez que se ejecute. Archivo Editar Ver Buscar Terminal Ayuda usuario@linux-yimq:/Scripts> sudo sh CCN-STIC-617-ENS_Paso6_intentos_fallidos_A.sh [sudo] password for root: ---------- --BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS-- ---------- ANTES DE COMENZAR SE CREARÁ UN BACKUP DE LA CARPETA PAM.D EN EL DIRECTORIO /etc/pam.d_backup[fecha/hora] NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE EL SCRIPT FINALICE EN CASO DE DETENCIÓN DEL SCRIPT; VUELVA A EJECUTARLO ANTES DE REINICIAR HASTA QUE FINALICE EL PROCESO CO RRECTAMENTE Pulse ENTER para continuar o Ctrl + C para cancelar..... Archivo Editar Ver Buscar Terminal Ayuda >>>>>>>>EL PROCESO A FINALIZADO CORRECTAMENTE<<<<<<<< Pulse ENTER y el sistema se reiniciará automáticamente en 1 minuto, guarde los archivo s que tenga abiertos antes de continuar..... Shutdown scheduled for [redacted], use 'shutdown -c' to cancel. usuario@linux-yimq:/Scripts> **Nota:** Si el script se detuviera o no terminara correctamente, deberá de iniciarlo una vez más antes de reiniciar, por el contrario, es posible que el sistema no pueda iniciarse correctamente.

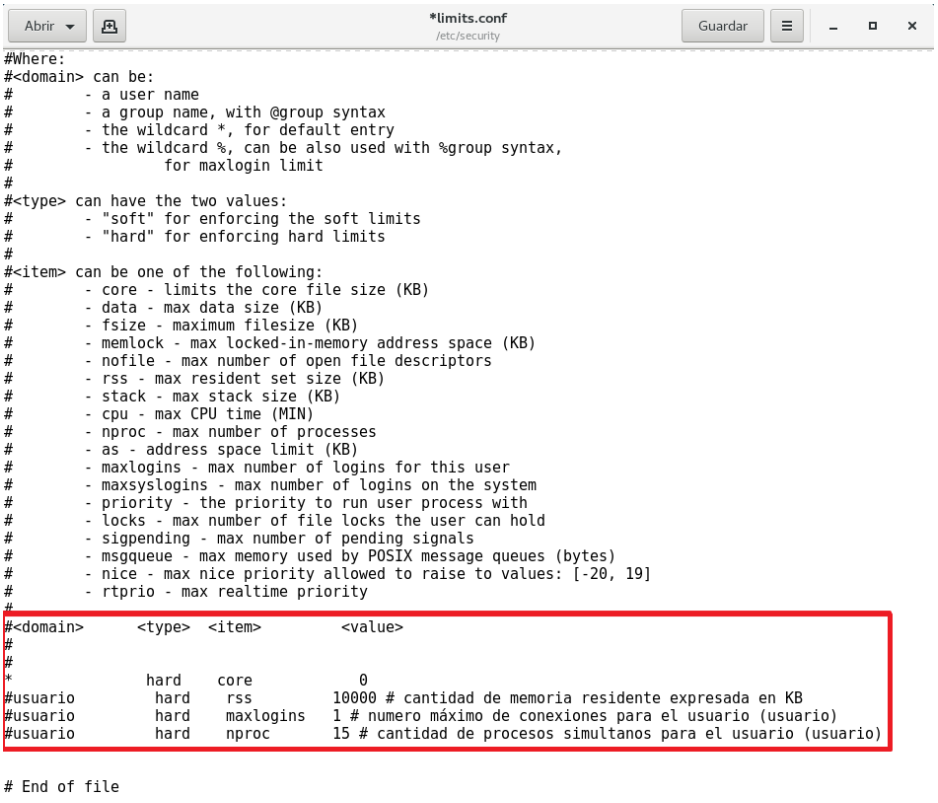
Paso	Descripción
63.	Si quisiera editar los documentos con las necesidades de seguridad requeridos por su organización, ejecute los siguientes comandos dependiendo del fichero que desee modificar. **$ gnomesu gedit /etc/pam.d/common-password &>/dev/null** **$ gnomesu gedit /etc/pam.d/login &>/dev/null** **$ gnomesu gedit /etc/pam.d/su &>/dev/null** **$ gnomesu gedit /etc/pam.d/gdm &>/dev/null**  **Nota:** No modifique estos ficheros de configuración si no conoce el funcionamiento de los módulos **"pam.d"**, podría provocar que el sistema no iniciara correctamente.
64.	Una vez finalice pulse el botón "Guardar" y cierre el editor de texto. Reinicie el sistema para que los cambios queden aplicados.

6.4. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

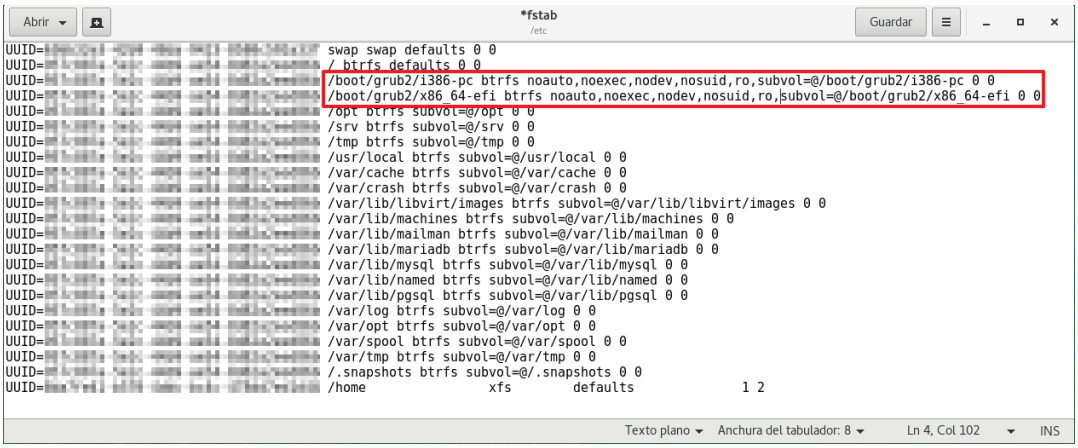
Paso	Descripción
65.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Favoritos" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
66.	Antes de comenzar este paso, asegúrese de haber cerrado y guardado las aplicaciones y los documentos importantes. Se va a proceder 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". **$ sudo cd /Scripts**

Paso	Descripción
67.	Ejecute el siguiente script. **$ sudo sh CCN-STIC-617-ENS_Paso7_limites_permisos_y_cad_contraseñas_A.sh** 
68.	Cuando finalice el script, saldrá un mensaje advirtiendo que el sistema se reiniciará en 1 minuto. Espere y cierre las aplicaciones que tenga abiertas. 
69.	Cuando reinicie el sistema e inicie sesión, saldrá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos. 
70.	Le pedirá la contraseña actual y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.

Paso	Descripción
71.	A continuación, se muestra un ejemplo del fichero "/etc/security/limits.conf", con líneas comentadas (**"#"**) en el que se limitan ciertas partes para un usuario específico. Para modificar dicho fichero ejecute el siguiente comando. **$ gnomesu gedit /etc/security/limits.conf &>/dev/null**
72.	Modifique el fichero de configuración de la manera que más se adapte a las necesidades de su organización, pulse el botón "**Guardar**" y cierre el editor de texto.



7. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

Paso	Descripción
73.	Si ha cerrado la "**Terminal**" en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
74.	Ejecute el siguiente comando. **$ gnomesu gedit /etc/fstab &>/dev/null**
75.	Edite el fichero de configuración y modifique los permisos de la partición "**/boot**" para que el resultado sea similar al de la imagen (noauto, noexec, nodev, nosuid, ro). 
76.	Cuando termine, pulse el botón "**Guardar**" y cierre el editor de texto. Elimine el directorio "/Scripts" y todo su contenido.

ANEXO A.5.2. LISTA DE COMPROBACIÓN DE CLIENTE SUSE ENTERPRISE LINUX 12 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 SERVIDORES SUSE ENTERPRISE LINUX 12 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA".

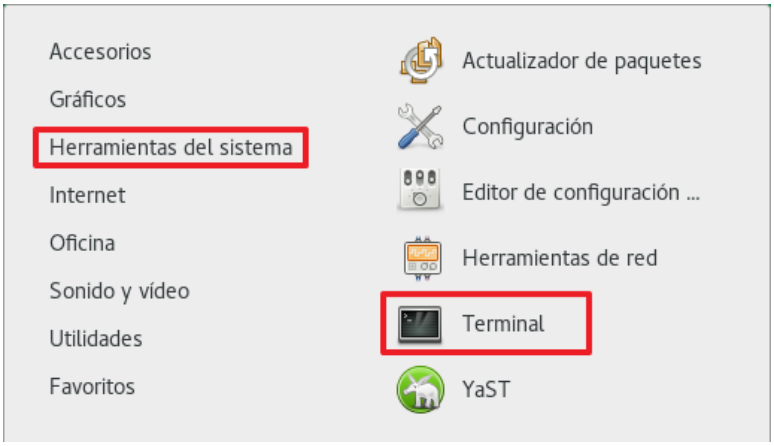
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores SUSE Enterprise 12 Linux independientes con implementación de seguridad de categoría alta del ENS.

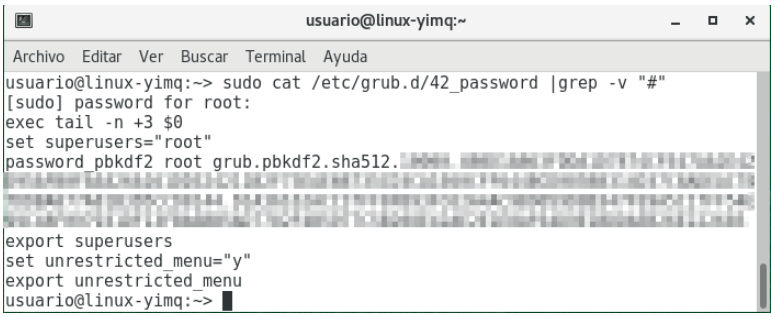
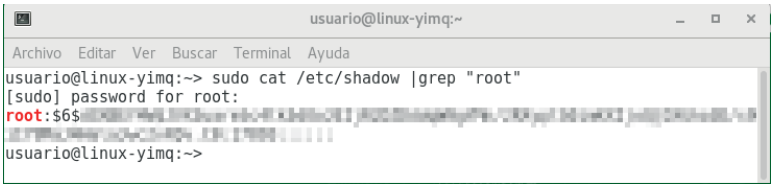
Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

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:

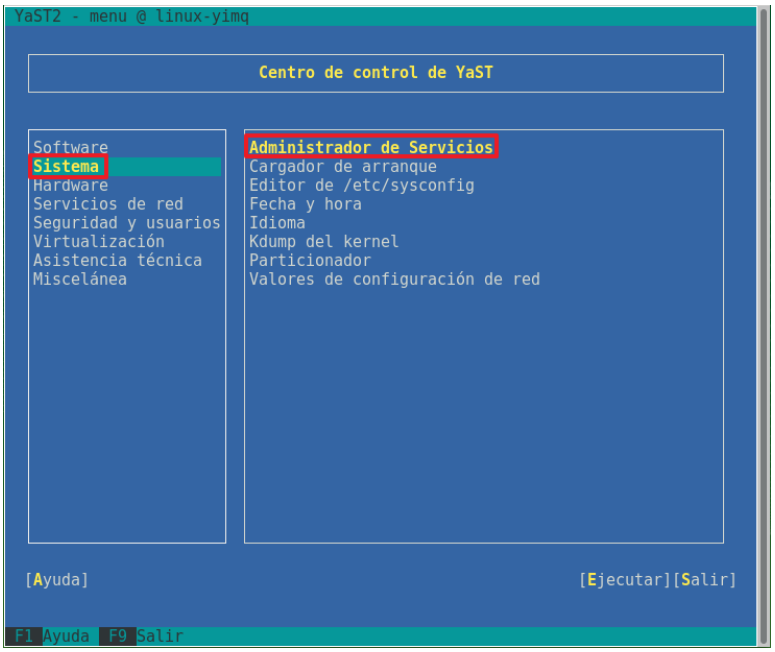
a) Terminal de Linux

b) Herramienta YaST

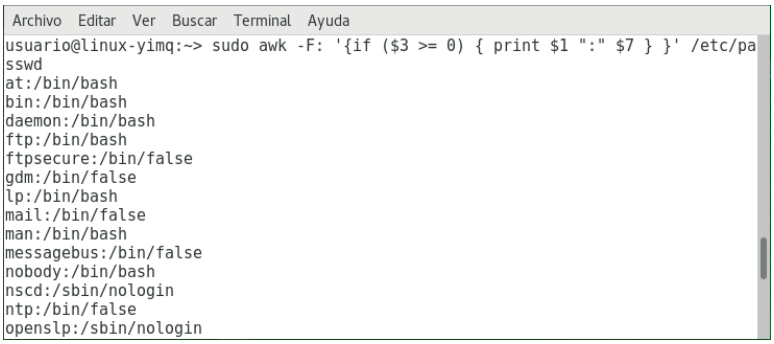
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de root. Cree la carpeta "**Scripts**" en "**/**" y copie el contenido de la categoría de seguridad "CATEGORIA_ALTA_DL" correspondiente al directorio "Scripts/ENS_CATEGORIA_ALTA_DL" 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, pulse en Aplicaciones y en el apartado "Herramientas del sistema" seleccione "Terminal". 

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. **$ cat /etc/grub.d/42_password |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.
5. Búsqueda de usuarios sin contraseña.		Ejecute el siguiente comando. **$ sudo cat /etc/shadow |cut -d":" -f-2 | grep ":$" |cut -d":" -f1**
6. Búsqueda de usuarios con UID 0.		Ejecute el siguiente comando. **$ sudo cat /etc/passwd |cut -d":" -f1,3 | grep -w 0|cut -d":" -f1 |grep -v "root"**
7. Verifique los parámetros del kernel.		Evitar modificación de tablas de encaminamiento. **$ 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 ="**

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Configuraciones</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>
<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>
<tr><th>Configuraciones</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>
<tr><th>Configuraciones</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>
<tr><th>Configuraciones</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>net.ipv4.icmp_echo_ignore_broadcasts</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 rowspan="8"></td><td></td><td>Ignorar mensajes de error mal formados.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.icmp_ignore_bogus_error_responses ="</td></tr>
<tr><td colspan="2"><table>
<tr><th>Configuraciones</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>
</table></td></tr>
<tr><td></td><td>Protegerse ante ataques TCP-SYN.
$ sudo cat /etc/sysctl.conf |grep "net.ipv4.tcp_syncookies ="</td></tr>
<tr><td colspan="2"><table>
<tr><th>Configuraciones</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>
<tr><td></td><td>Bloqueo de core dumps de programas con SUID.
$ sudo cat /etc/sysctl.conf |grep "fs.suid_dumpable ="</td></tr>
<tr><td colspan="2"><table>
<tr><th>Configuraciones</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 por medio de herramienta ntsysv</td><td></td><td>Abra la Terminal y ejecute el siguiente comando.
$ sudo yast
 

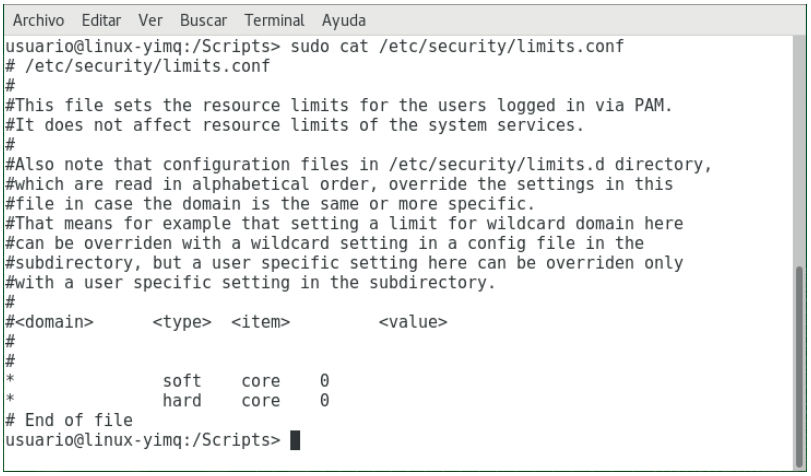
Revise que los servicios activos al iniciar el sistema son los correctos para su organización.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Comprobación de usuarios y shells predetermina-das.</td><td></td><td>Ejecute el siguiente comando.
$ sudo awk -F: '{if ($3 >= 0) { print $1 ":" $7 } }' /etc/passwd
 

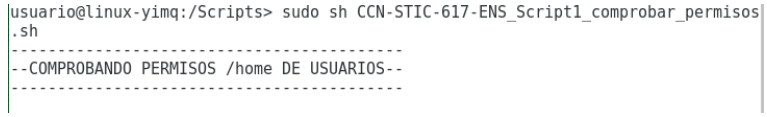
Compruebe si los usuarios que se muestran son los más adecuados para su organización y que están correctas las shells predeterminadas.</td></tr>
<tr><td>10. Comprobación de registros de actividad</td><td></td><td>Primero se va a comprobar el fichero de configuración, con los parámetros definidos por 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 ="
<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>
</table>
Se procede a visualizar la totalidad del fichero de configuración del demonio auditd para que pueda revisar los parámetros específicos de su organización.
$ sudo cat /etc/audit/auditd.conf
<pre>
#
This file controls the configuration of the audit daemon
#

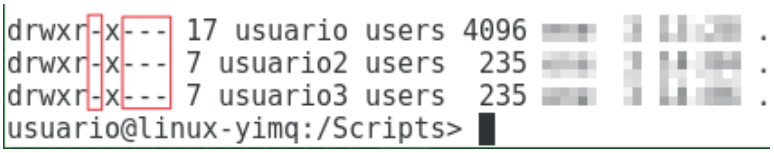
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 12
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 10
max_log_file_action = ROTATE
space_left = 75
</pre>
</td></tr>
</table>

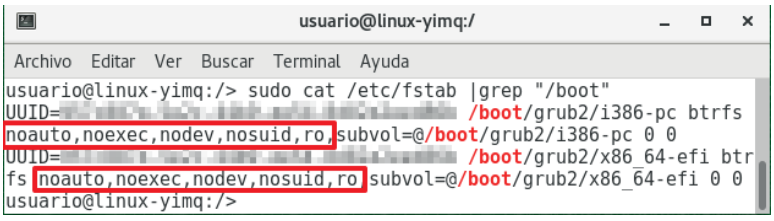
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>11. Parámetros de bloqueo de cuenta.</td><td></td><td>Se va a comprobar los ficheros de configuración, con los parámetros definidos por esta guía.
– /etc/pam.d/login
– /etc/pam.d/su
– /etc/pam.d/gdm
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/login |grep "auth" |grep "pam_tally2" |grep "deny="
$ sudo cat /etc/pam.d/login |grep "auth" |grep "pam_tally2" |grep "unlock_time="
$ sudo cat /etc/pam.d/su |grep "auth" |grep "pam_tally2" |grep "deny="
$ sudo cat /etc/pam.d/su |grep "auth" |grep "pam_tally2" |grep "unlock_time="
$ cat /etc/pam.d/gdm |grep "auth" |grep "pam_tally2" |grep "deny="
$ cat /etc/pam.d/gdm |grep "auth" |grep "pam_tally2" |grep "unlock_time="</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>auth required</td><td>pam_tally2.so</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td><td>– /etc/pam.d/common-passwd
Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/common-password |grep "requisite" |grep "cracklib" |grep "retry="</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>retry</td><td>8</td><td></td></tr>
</table></td></tr>
</table>

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

Nota: Si ha hecho modificaciones personalizadas para su organización con respecto a limitación de recursos por usuarios, las puede revisar en este apartado.</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>
<tr><td>14. Verifique la directiva de caducidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ cat /etc/login.defs |grep "PASS_MAX_DAYS"
$ cat /etc/login.defs |grep "PASS_MIN_DAYS"
$ cat /etc/login.defs |grep "PASS_MIN_LEN"
$ cat /etc/login.defs |grep "PASS_WARN_AGE"
$ cat /etc/login.defs |grep "UMASK"
Compruebe si se han configurado bien los valores.</td></tr>
<tr><td></td><td colspan="2"><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>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>15. Verifique la directiva de complejidad de contraseñas.</td><td></td><td>Ejecute los siguientes comandos.
$ sudo cat /etc/pam.d/common-password |grep "minlen="
$ sudo cat /etc/pam.d/common-password |grep "dcredit="
$ sudo cat /etc/pam.d/common-password |grep "ucredit="
$ sudo cat /etc/pam.d/common-password |grep "lcredit="
$ sudo cat /etc/pam.d/common-password |grep "ocredit="</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>
<tr><td>ocredit</td><td>-1</td><td></td></tr>
</table></td></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”.
$ sudo cd /Scripts
Ejecute el siguiente comando.
$ sudo sh CCN-STIC-617-ENS_Script1_comprobar_permisos.sh
 

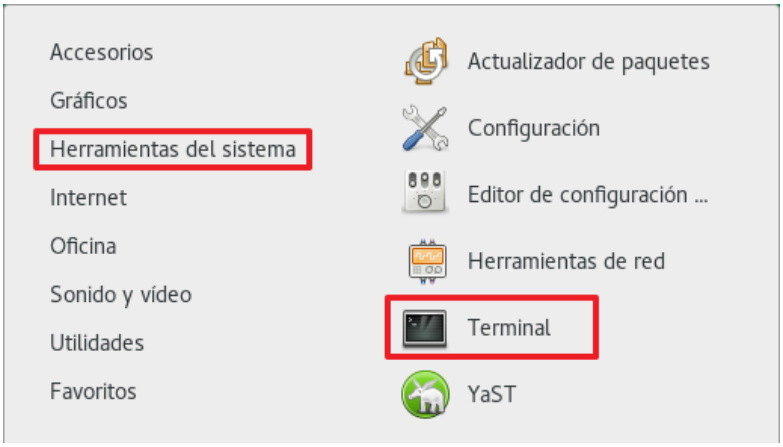
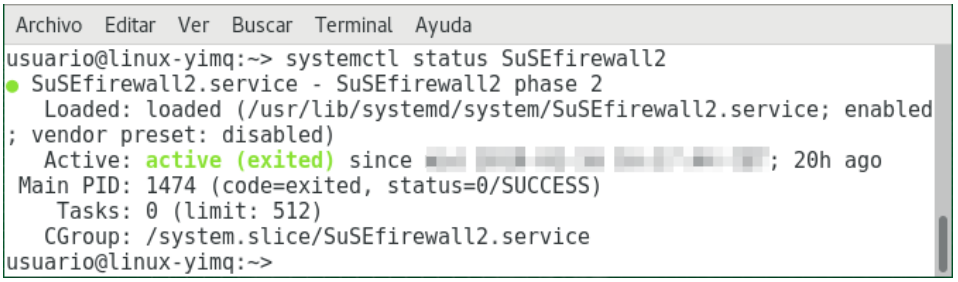
El script mostrará los permisos de las carpetas “/home” y se debe comprobar que las columnas marcadas se encuentren vacías.
 
</td></tr>
<tr><td>17. Configuración de Gnome</td><td></td><td>Se va a proceder a revisar los parámetros de configuración de Gnome. Para ello ejecute los siguientes comandos.
$ sudo cat /etc/dconf/db/gdm.d/01-banner-message</td></tr>
<tr><td colspan="3"><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></td></tr>
<tr><td></td><td></td><td>$ sudo cat /etc/dconf/db/gdm.d/00-login-screen |grep "disable-user-list"</td></tr>
<tr><td colspan="3"><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>

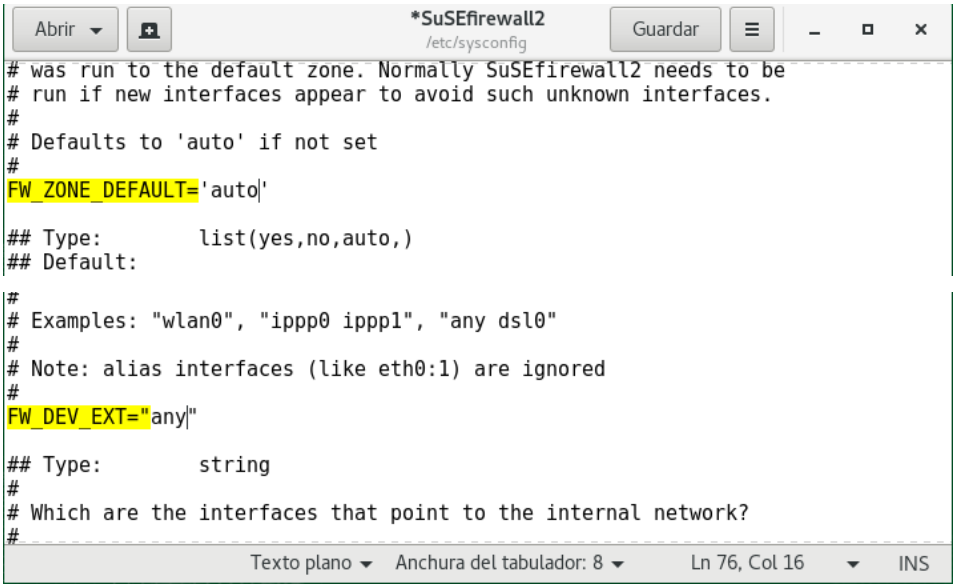
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="11"></td><td></td><td>$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "idle-delay=uint32"
$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "lock-enabled"
$ sudo cat /etc/dconf/db/local.d/00-screensaver |grep "lock-delay=uint32"</td></tr>
<tr><td colspan="2"><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>1</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "automount="
$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "automount-open="
$ sudo cat /etc/dconf/db/local.d/07-media-handling |grep "autorun-never="</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>automount</td><td>false</td><td></td></tr>
<tr><td>automount-open</td><td>false</td><td></td></tr>
<tr><td>autorun-never</td><td>true</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "hide-identity"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "old-files-age"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep "remember-recent-files"
$ sudo cat /etc/dconf/db/local.d/03-privacy |grep " remove-old-temp-files"</td></tr>
<tr><td colspan="2"><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>

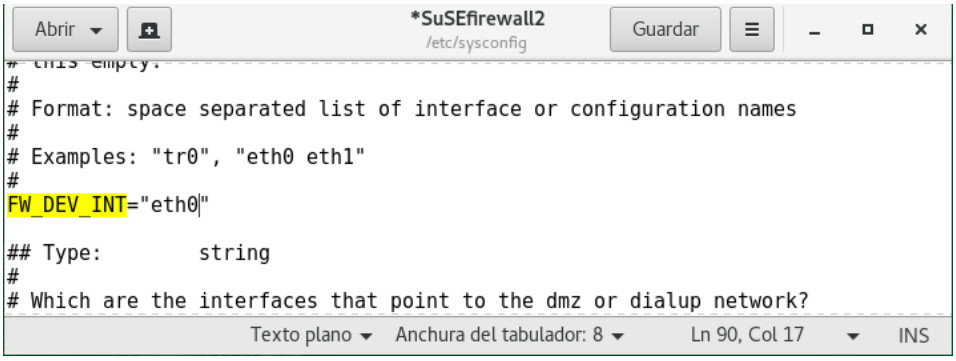
ANEXO A.6. TAREAS ADICIONALES DE SEGURIDAD

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

1. SUSEFIREWALL2

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, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
4.	Para evitar intrusiones y accesos no autorizados a los servicios expuestos a través de la red se debe utilizar un cortafuegos o “firewall”. SUSE incluye su propio servicio de firewall conocido como SuSEfirewall2. Para ello es importante que antes de crear las reglas y elegir la zona que más se adecue a su organización, se cree una copia de seguridad del archivo de configuración y se compruebe que está activo el servicio de SuSEfirewall2. Se procede a realizar la copia de seguridad ejecutando el siguiente comando. **$ sudo cp -v /etc/sysconfig/SuSEfirewall2 /etc/sysconfig/SuSEfirewall2.bak**
5.	Revise el estado del servicio. **$ systemctl status SuSEfirewall2** 

Paso	Descripción
6.	Primero se van a asignar las interfaces de red del equipo a las zonas “INTERNA” y “EXTERNA”. **$ gnomesu gedit /etc/sysconfig/SuSEfirewall2 &>/dev/null** No cierre el editor hasta que finalice de configurar todos los parámetros. **Nota:** Las comunicaciones entre las zonas INTERNA Y EXTERNA se encontrarán por defecto deshabilitadas, siendo la zona EXTERNA más restrictiva que la zona INTERNA. Por defecto, se aconseja configurar todas las interfaces en la zona EXTERNA, designando de forma concreta aquéllas que van a utilizarse para dar servicio al resto de equipos de la red de trabajo en la zona INTERNA.
7.	En el fichero de configuración de SuSEfirewall2 que se ha abierto, añada la expresión “any” a la variable FW_DEV_EXT y la expresión “auto” a la variable FW_ZONE_DEFAULT para asignar por defecto todas las interfaces a la zona EXTERNA. **FW_ZONE_DEFAULT="auto"** **FW_DEV_EXT="any"** 

Paso	Descripción
8.	Añada las interfaces que quiera utilizar en la zona INTERNA a la variable FW_DEV_INT, por ejemplo “eth0”. **FW_DEV_INT="eth0"**  **Nota:** Las conexiones de red (interfaces) podrán variar dependiendo de las especificaciones técnicas de hardware de cada equipo. En Linux, el comando para visualizar las interfaces es “sudo /sbin/ifconfig” (sin comillas). Deberá adaptar la configuración según los parámetros adecuados a su organización.
9.	A continuación, se definen los servicios y puertos asociados a los que se va a permitir el acceso desde cada una de las redes. El formato de la variable a configurar es FW_SERVICES_ZONA_**PROTOCOLO**. Por ejemplo, para configurar el acceso por SSH (TCP) a redes conectadas a la zona INTERNA, la variable será la siguiente. **FW_SERVICES_INT_TCP** Los valores posibles son los siguientes. **FW_SERVICES_EXT_TCP # Servicios TCP en la zona EXTERNA.** **FW_SERVICES_EXT_UDP # Servicios UDP en la zona EXTERNA.** **FW_SERVICES_EXT_IP # Servicios IP en la zona EXTERNA.** **FW_SERVICES_INT_TCP # Servicios TCP en la zona INTERNA.** **FW_SERVICES_INT_UDP # Servicios UDP en la zona INTERNA.** **FW_SERVICES_INT_IP # Servicios IP en la zona INTERNA.**
10.	Para configurar un servicio en función de su protocolo y puerto, configure añadiéndolo como valor a la variable como en los siguientes ejemplos. Para activar el servicio de SSH en la zona INTERNA. **FW_SERVICES_INT_TCP="22"** Si quisiera añadir otro servicio (como LDAP, por ejemplo) con la misma zona y Protocolo. **FW_SERVICES_INT_TCP="22 389"** Se puede añadir rangos de puertos en un solo servicio, para ello separe el primer y último puerto de dicho rango utilizando el carácter “:”. **FW_SERVICES_INT_TCP="443 23 8080:8085"**

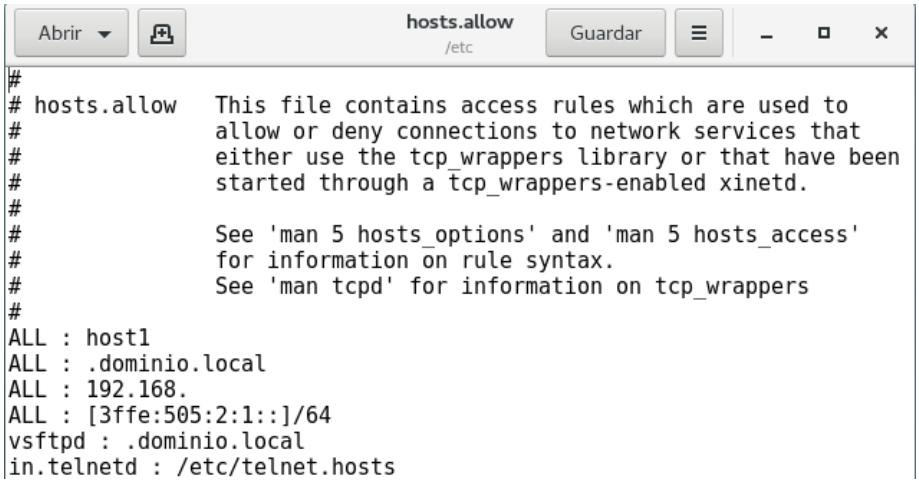
Paso	Descripción
11.	El siguiente paso consiste en activar la defensa de la zona INTERNA. Con este parámetro activo, los equipos de la zona INTERNA sólo podrán acceder a aquellos servicios y puertos que se hayan declarado explícitamente, según los parámetros del punto anterior. **FW_PROTECT_FROM_INT="yes"** Adicionalmente, active la protección contra ataques de denegación de servicio por "source quenching", configurando la siguiente variable. **FW_ALLOW_FW_SOURCEQUENCH="no"**
12.	Si fuera requisito en su organización la desactivación de respuesta a peticiones de ICMP (ping) deberá configurar la siguiente variable. **FW_ALLOW_PING_FW="no"**
13.	Si quisiera evitar revelar más información de la necesaria a posibles atacantes o terceros no autorizados es necesario configurar adecuadamente el siguiente servicio para que reglas del firewall no se reflejen en un fichero de estado. **FW_WRITE_STATUS="no"**
14.	Por último, si el servidor no va a dar servicio a una red IPv6, desactive el soporte de dicho protocolo. **FW_IPv6="no"** **FW_IPv6_REJECT_OUTGOING="yes"**
15.	Continúe configurando el fichero con los parámetros más acordes con su organización. Cuando finalice pulse el botón "**Guardar**" y cierre el editor de texto. Cierre las aplicaciones, guarde el trabajo que pudiera estar realizando y reinicie el sistema.

2. CONTENEDORES TCP (TCP-WRAPPERS)

Paso	Descripción
1.	El siguiente punto restringe el acceso a los distintos servicios de red.
2.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse en "Aplicaciones" y en el apartado "Favoritos" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "**Enter**".
3.	Su configuración es muy sencilla, consta de dos archivos que están en el directorio /etc: **hosts.allow** y **hosts.deny**. – Dentro del hosts.allow se indicará los equipos que tienen permiso para acceder a nuestros servicios. – Dentro del hosts.deny se indicará los equipos que no tienen permiso para acceder a nuestros servicios.

Paso	Descripción
4.	Se recomienda que se deniegue el acceso a todos los equipos, para después otorgárselo a los que sea necesario. Para ello edite el fichero hosts.deny e indique el parámetro 'ALL : ALL', lo que deniega todo lo que no se permita de forma explícita en el fichero hosts.allow. Para ello ejecute el siguiente comando. **$ gnomesu gedit /etc/hosts.deny &>/dev/null** Configure el fichero con los parámetros que más convengan para su organización.  **Nota:** Puesto que las reglas de acceso en hosts.allow son aplicadas primero, tienen preferencia sobre las reglas en hosts.deny. Por lo tanto, si se permite el acceso a un servicio en hosts.allow, una regla negando el acceso al mismo servicio en hosts.deny es ignorada. Las reglas en cada archivo son leídas de arriba hacia abajo y la primera regla que coincida para un servicio dado es la única aplicada. Por lo tanto, el orden de las reglas es extremadamente importante. Si no se encuentra ninguna regla para el servicio en ninguno de los archivos, o si no existe ninguno de los archivos, se concede el acceso al servicio. Cualquier cambio a hosts.allow o a hosts.deny tomará efecto de inmediato sin tener que reiniciar el servicio de red.
5.	A continuación, se procede a dar permiso a todos ellos equipos que requieran acceso en su organización, acotando el acceso por sección de red, servicio, nombre o dominio. Para ello edite el fichero "/etc/hosts.allow". **$ gnomesu gedit /etc/hosts.allow &>/dev/null**
6.	El formato para los ficheros de configuración "/etc/hosts.allow" y "/etc/hosts.deny" son idénticos. Cualquier línea en blanco que comience con un símbolo de numeral o almohadilla (#) será ignorada, y cada regla debe estar en su propia línea. Por tanto, la sintaxis sería la siguiente. **<daemon list>: <client list> [: <option>: <option>: ...]** **Nota:** Se detallan cada uno de los elementos de la sintaxis: - <daemon list> — Una lista separada por comas de los nombres de procesos (no de los nombres de servicios) o el comodín ALL. La lista de demonios también acepta operadores para permitir mayor flexibilidad. - <client list> — Una lista separada por comas de nombres de host, direcciones IP, patrones especiales, o comodines especiales la cual identifica los hosts afectados por la regla. La lista de clientes también acepta operadores para permitir mayor flexibilidad. - <option> — Una acción opcional o una lista separada con punto y coma de acciones realizadas cuando la regla es activada. Los campos de opciones soportan expansiones, lanzan comandos desde el shell, otorgan o prohíben el acceso y alteran el comportamiento de la conexión.

Paso	Descripción
7.	A continuación, se muestra el fichero "/etc/hosts.allow" con varios ejemplos.




```
#
# hosts.allow   This file contains access rules which are used to
#               allow or deny connections to network services that
#               either use the tcp_wrappers library or that have been
#               started through a tcp_wrappers-enabled xinetd.
#
#               See 'man 5 hosts_options' and 'man 5 hosts_access'
#               for information on rule syntax.
#               See 'man tcpd' for information on tcp_wrappers
#
ALL : host1
ALL : .dominio.local
ALL : 192.168.
ALL : [3ffe:505:2:1::]/64
vsftpd : .dominio.local
in.telnetd : /etc/telnet.hosts
```

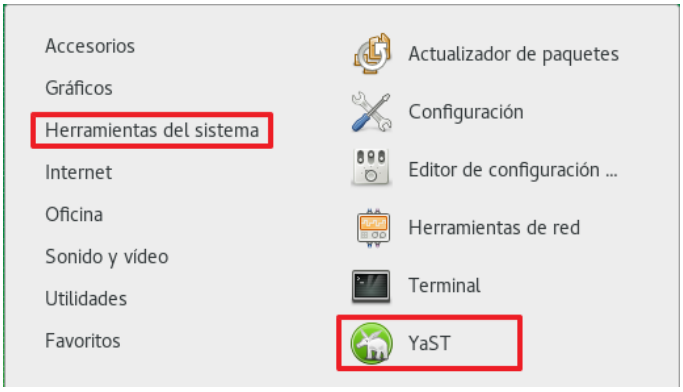
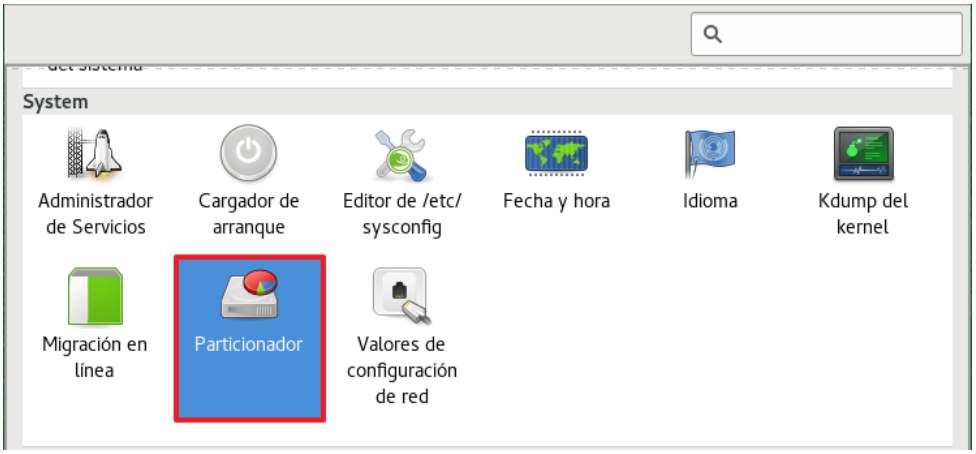
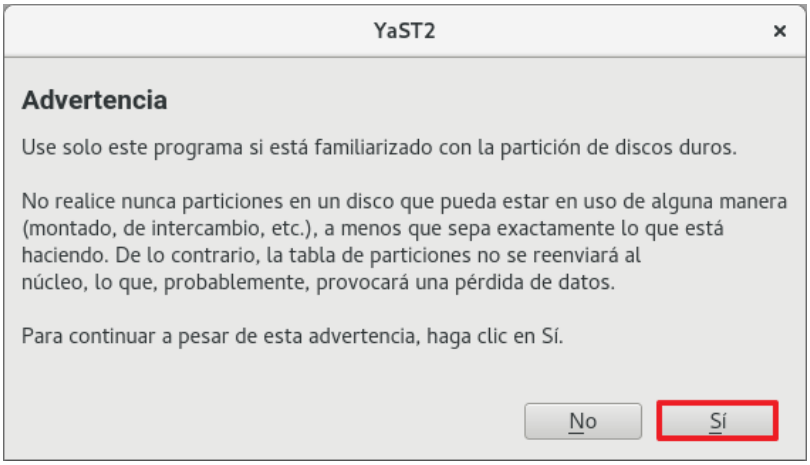
Nota: Se define a continuación cada uno de los elementos del fichero anterior:

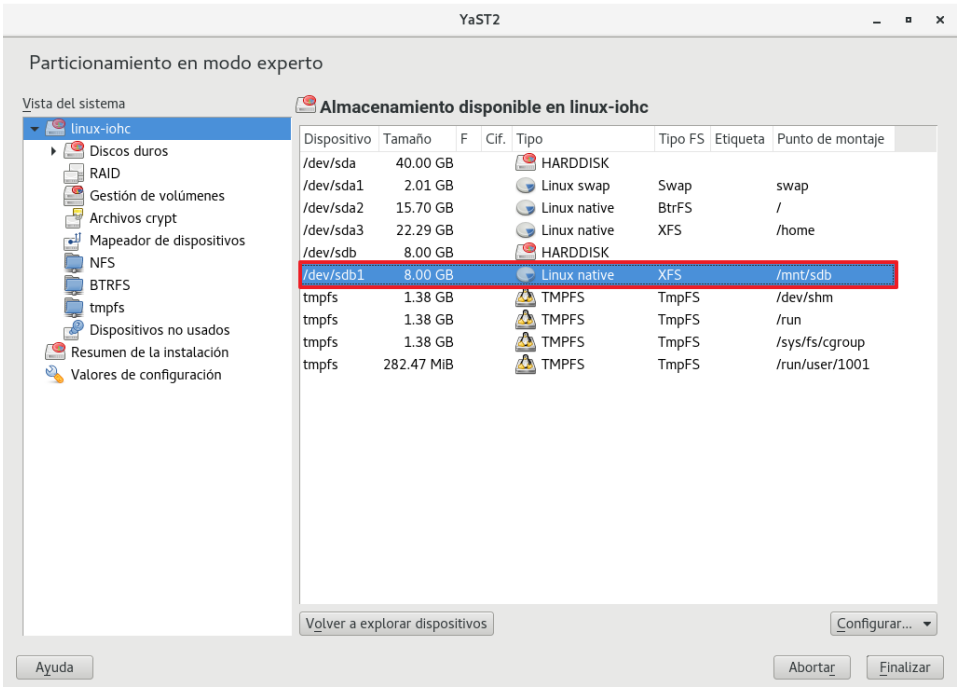
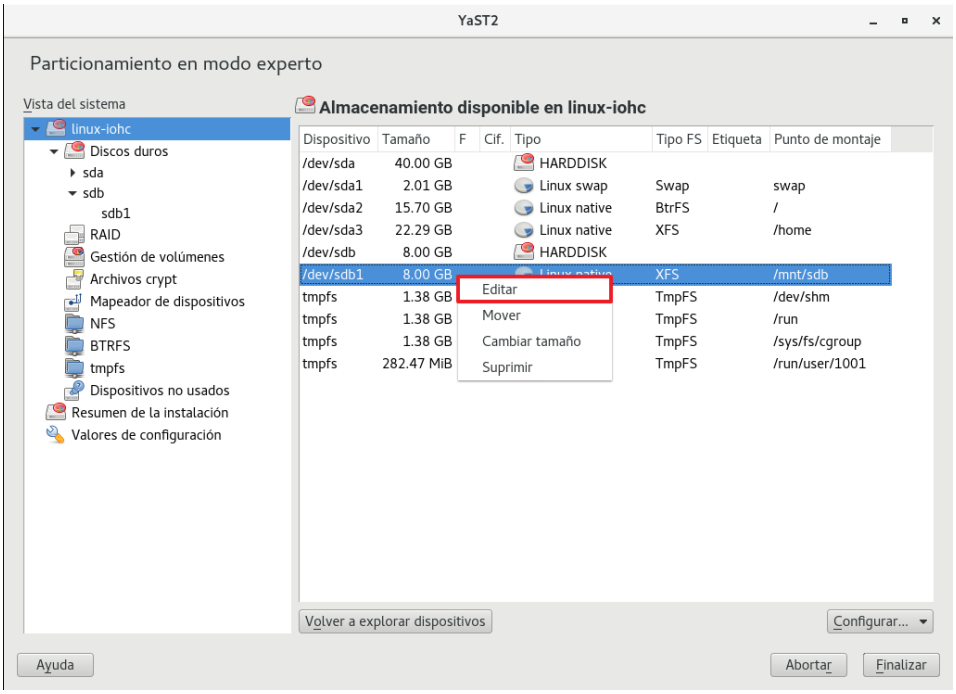
- **ALL : host1** Si se quisiera dar acceso a todos los servicios al host1.
- **ALL : .dominio.local** Nombre de host comenzando con un punto (.). Al colocar un punto al comienzo de un nombre de host, se hace coincidir todos los hosts compartiendo los componentes listados del nombre. El ejemplo aplicaría a cualquier host dentro del dominio "dominio.local".
- **ALL : 192.168.** Dirección IP que termina con un punto (.). Al colocar un punto al final de una dirección IP hace corresponder todos los hosts compartiendo el grupo numérico inicial de una dirección IP. El ejemplo aplicará a cualquier host dentro de la red 192.168.x.x
- **ALL : [3ffe:505:2:1::]/64** Par [Dirección IPv6]/máscara. Los pares [red]/máscara también pueden ser usadas como un patrón de control de acceso a un grupo particular de direcciones IPv6. El ejemplo siguiente aplicaría a cualquier host con una dirección de 3ffe:505:2:1:: hasta 3ffe:505:2:1:ffff:ffff:ffff:ffff:
- **vsftpd : .dominio.local** Esta regla permite conexiones al demonio FTP (vsftpd) desde cualquier host en el dominio ".dominio.local".
- **in.telnetd : /etc/telnet.hosts** La barra oblicua (/).es tratada como una ruta a un nombre de archivo. Esto permite la creación de reglas especificando un gran número de hosts. En el ejemplo se revisa el archivo /etc/telnet.hosts, que contendrá un listado de nombres de hosts, de esta manera se permitirán todas las conexiones Telnet a los hosts incluidos en ese fichero.

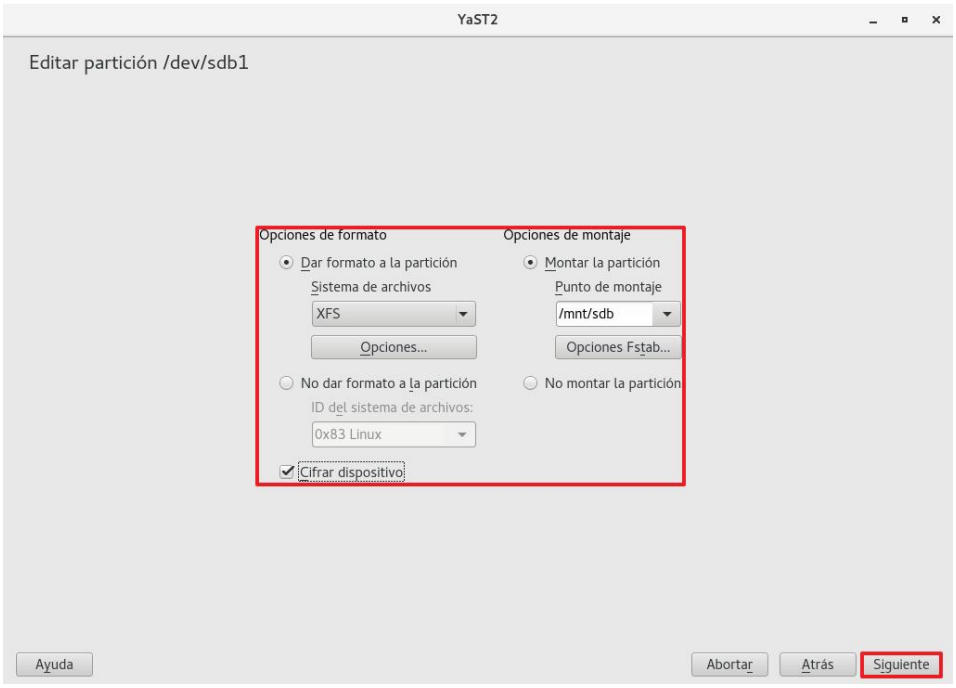
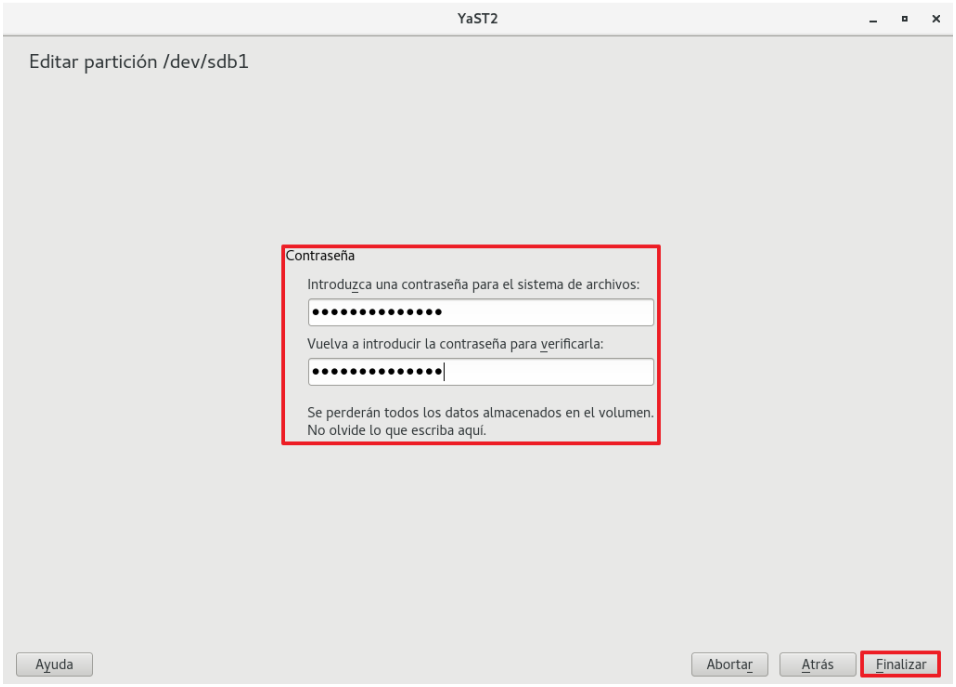
ANEXO A.6.2. PROTECCIÓN DEL DISCO. CIFRADO

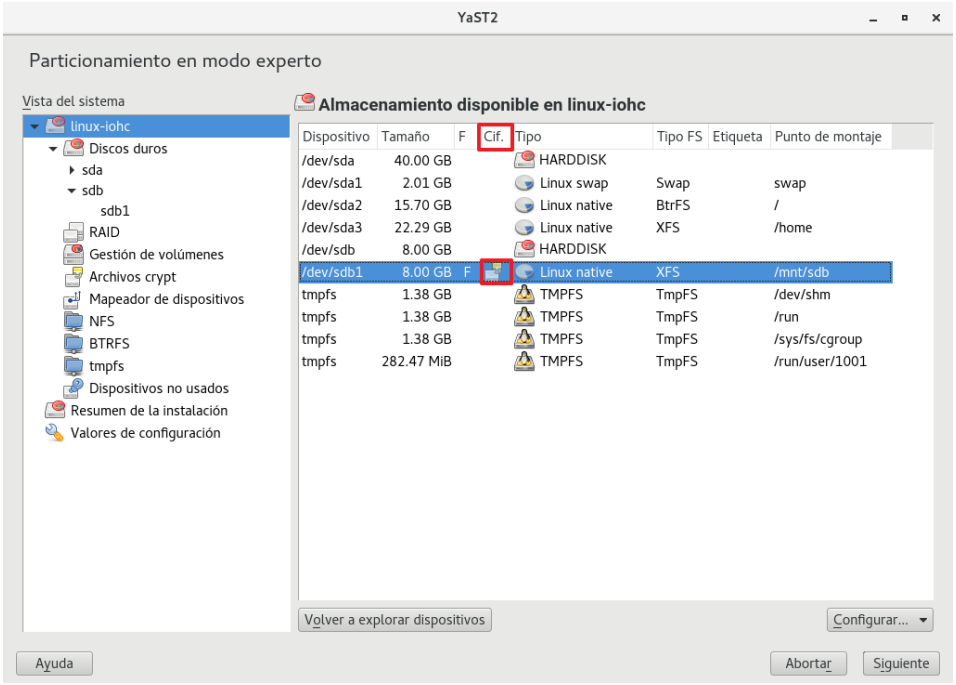
Paso	Descripción
1.	Este apartado es de aplicación para sistemas con particionado separado por puntos de montaje y para particiones independientes al sistema operativo por defecto. Se recomienda realizar el cifrado en el momento de la instalación.

Nota: Se recomienda cifrar las particiones sensibles del sistema operativo y la partición "**/home**" de los usuarios en el momento de la instalación. se mostrará un ejemplo de cómo cifrar una partición ajena a las definidas por defecto en la instalación 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. Deberá adaptar los parámetros aquí definidos a los que más convenga con su organización.

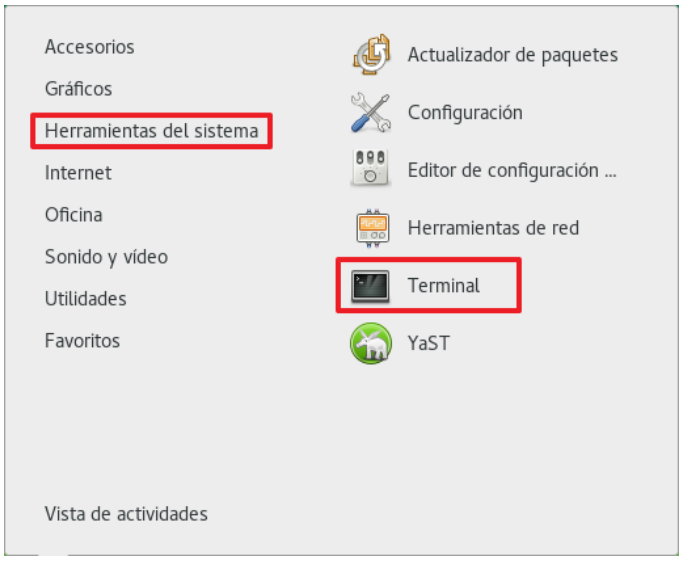
Paso	Descripción
2.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “YaST”. 
3.	En el apartado “System” pulse “Particionador”. 
4.	Aparecerá un mensaje de “Advertencia”, al cual se elegirá la opción “Sí”.  **Nota:** Tenga en cuenta que al realizar un cifrado con LUKS, formateará el volumen seleccionado, perdiéndose todos los datos existentes en la partición. A continuación, se mostrará un ejemplo de cómo cifrar una partición ajena a las definidas por defecto en la instalación con LUKS.

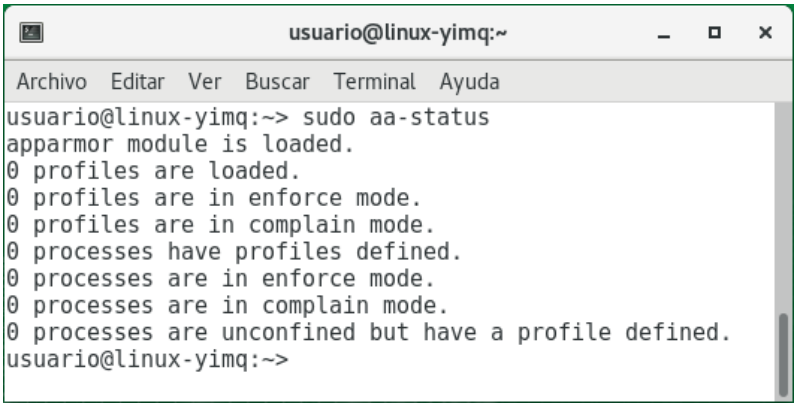
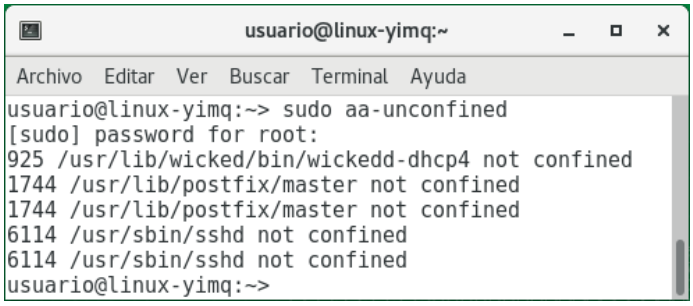
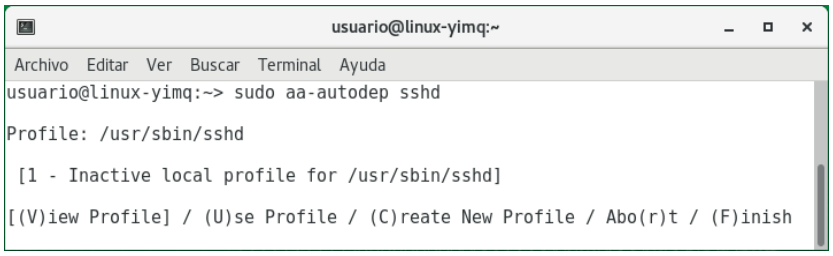
Paso	Descripción
5.	Seleccione la partición a cifrar. 
6.	Abriendo el menú contextual, selecciones la opción “Editar”. 

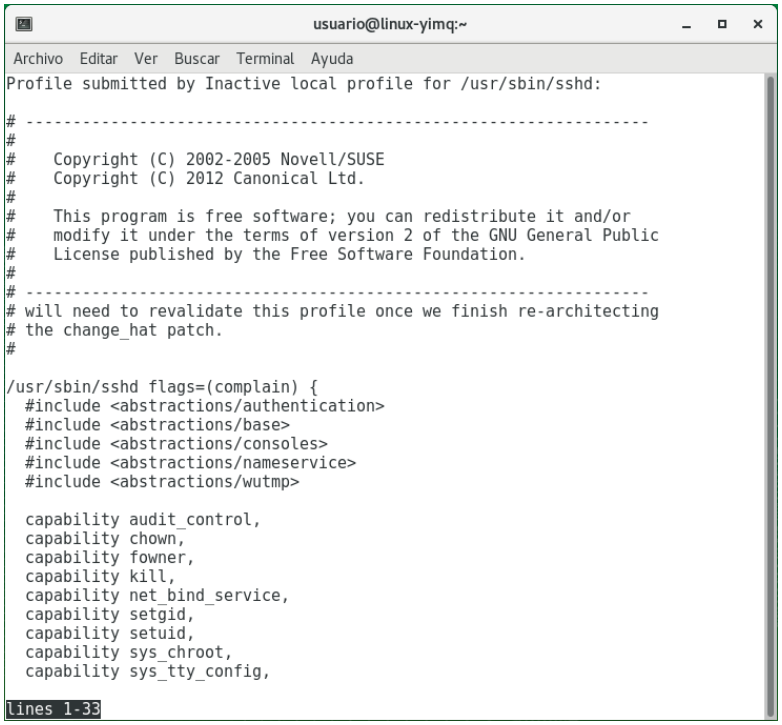
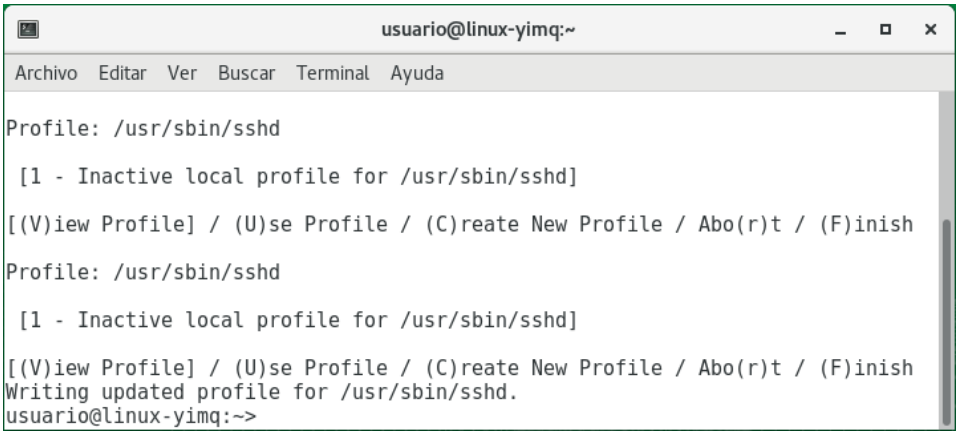
Paso	Descripción
7.	En el menú editar la partición seleccione el sistema de archivos deseado y las opciones de montaje que más convengan a su organización. Posteriormente seleccione la opción “Cifrar dispositivo” y pulse “Siguiente” para continuar. 
8.	Introduzca la contraseña con los parámetros de seguridad requeridos y pulse “Finalizar” para continuar. 
9.	Comenzará el proceso de formateo y cifrado de la partición, no presione ninguna tecla mientras el proceso está activo.

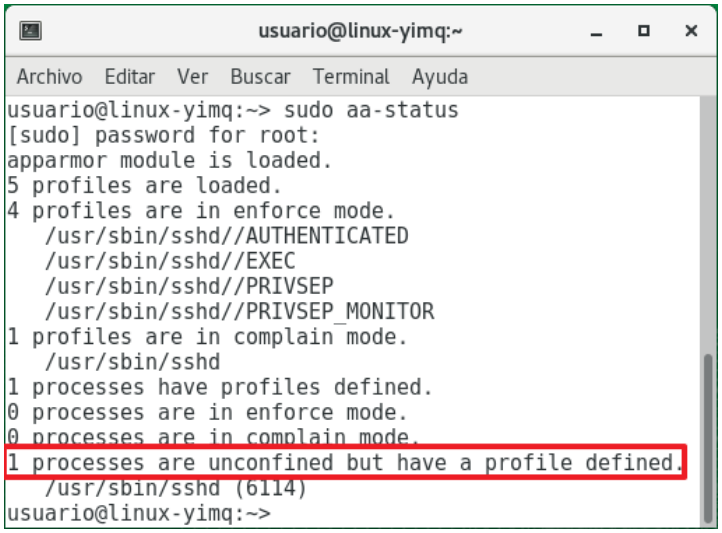
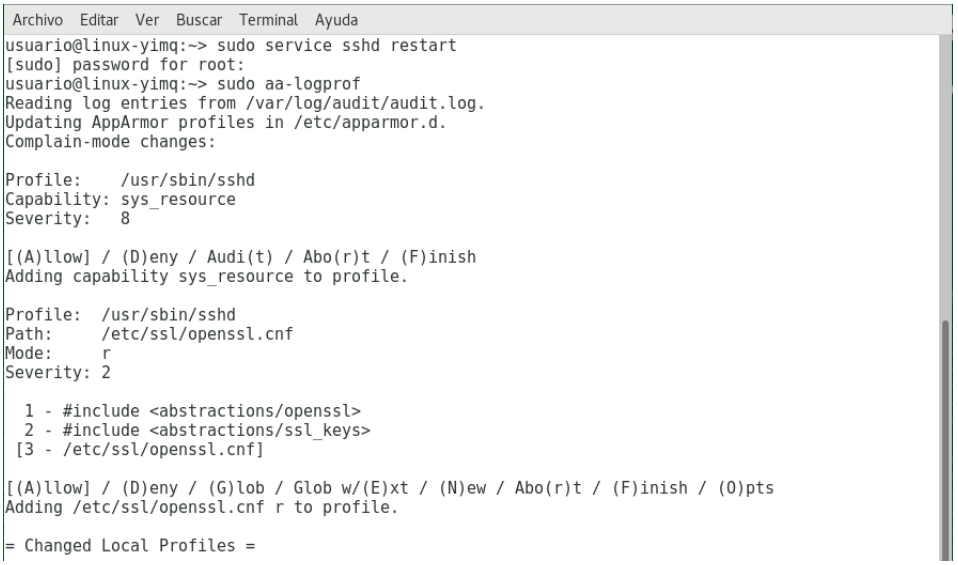
Paso	Descripción
10.	Después del proceso de formateo y cifrado volverá a la pantalla inicial, donde deberá comprobar que el proceso ha finalizado correctamente. 

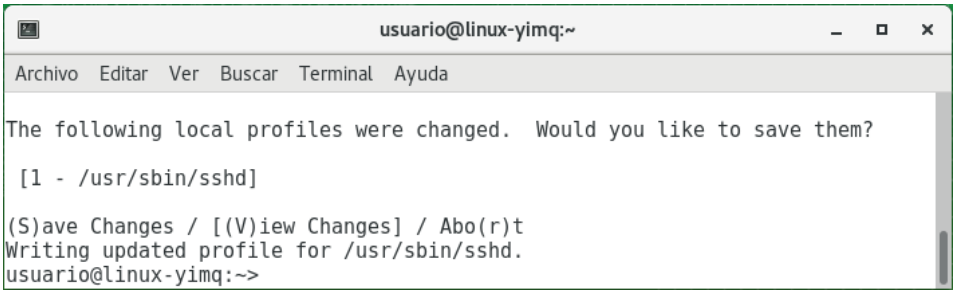
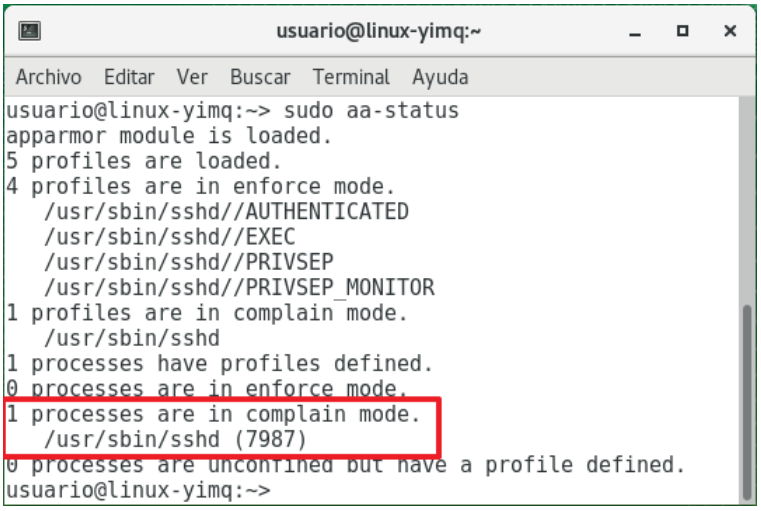
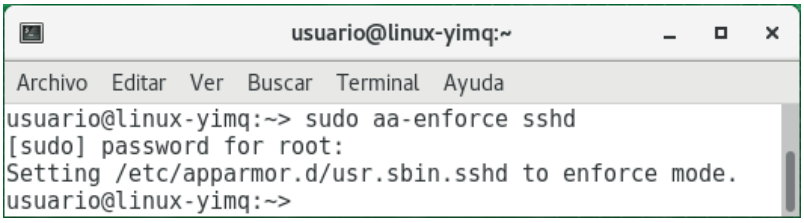
ANEXO A.6.3. CONFIGURACIÓN ADICIONAL DE SEGURIDAD – APPARMOR

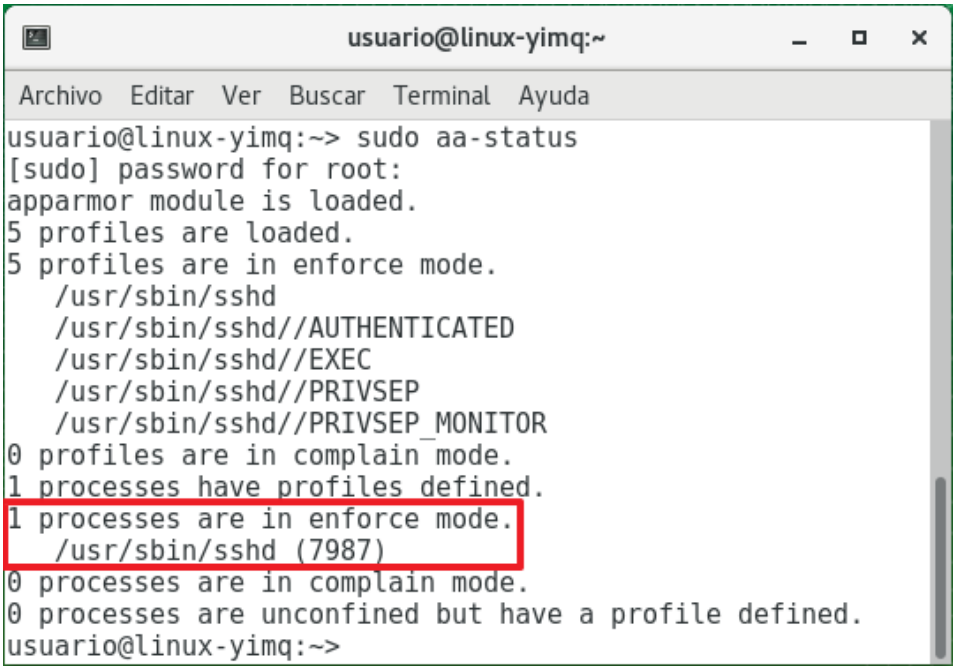
Paso	Descripción
1.	Se va a proceder a revisar el estado de AppArmor así como su configuración.
2.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
3.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o Sudoers.
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando “**cd /**” y pulse la tecla “**Enter**”.

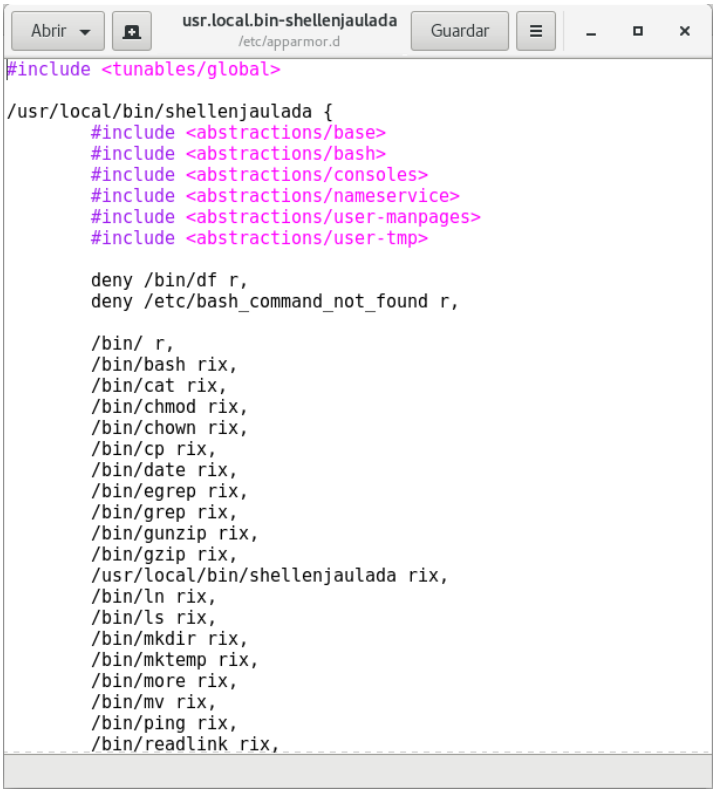
Paso	Descripción
6.	Se va a proceder a revisar el estado de los perfiles de AppArmor. Ejecute el siguiente comando. **$ sudo aa-status** 
7.	Ahora se va a proceder a revisar los procesos no confinados. Ejecute el siguiente comando. **$ sudo aa-unconfined**  **Nota:** Sin confinar (unconfined): son los procesos que no son vigilados ni confinados por apparmor, bien porque no hay perfil para ellos, bien porque el perfil se deshabilitó con **aa-disable**.
8.	Una vez revisados los procesos no confinados del sistema, se va a configurar un perfil para uno de ellos, en este caso se creará un perfil para el servidor ssh. **$ sudo aa-autodep sshd** 

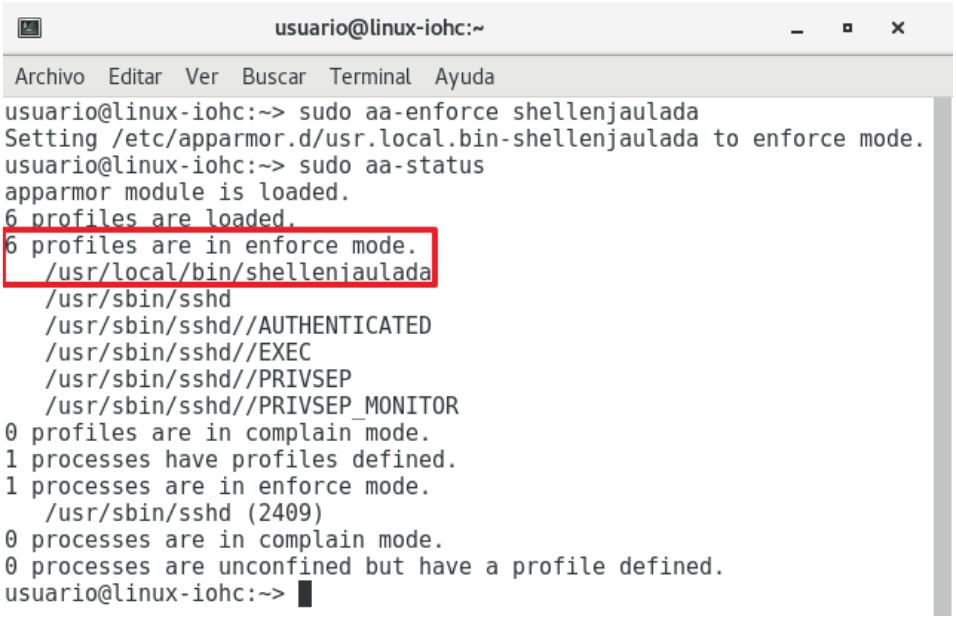
Paso	Descripción
9.	Introduzca **"V"** para revisar el perfil preconfigurado que posee AppArmor. Una vez revisado, pulse la tecla **"q"**. 
10.	A continuación, pulse **"U"** para usar el perfil que propone AppArmor. 

Paso	Descripción
11.	Se revisa la correcta aplicación del perfil, ejecutando el siguiente comando nuevamente. **$ sudo aa-status** 
12.	Posteriormente se reiniciará el servicio “ssh” y se ejecutará el comando “aa-logprof”. Para ello ejecute los siguientes comandos. **$ sudo service sshd restart** **$ sudo aa-logprof**
13.	Se contestará a los cambios propuestos con la tecla **“A”**, para contestar “**[(A)llow]**”.  **Nota:** Básicamente el comando “aa-logprof” leerá las entradas de logs de la herramienta audit, y determinará las violaciones de acceso, ofreciendo alternativas para evitarlas.

Paso	Descripción
14.	Finalmente, el sistema avisará si se quieren guardar los cambios y se pulsará la tecla **"S"** para que coincida con la elección **(S)ave Changes** (Guardar cambios). 
15.	Se revisa la correcta aplicación del perfil, revisando que se encuentra el proceso en "complain mode" ejecutando el siguiente comando nuevamente. **$ sudo aa-status** 
16.	Si se quisiera confinar el servicio se ejecutará el siguiente comando. **$ sudo aa-enforce sshd** 

Paso	Descripción
17.	Se revisa la correcta aplicación del perfil, revisando que se encuentra el proceso en "" ejecutando el siguiente comando nuevamente. **$ sudo aa-status**  **Nota:** Si en algún momento, se debiera aumentar los permisos, podría establecerlo otra vez en aprendizaje y repetir la operación con **aa-logprof**.
18.	Por último, se configurará un perfil para un usuario en particular con un ejemplo de permisos mínimos. Para ello lo primero será crear una un link de la shell bash a shellenjaulada, para poder modificar las opciones de AppArmor de forma independiente. Ejecute para ello el siguiente comando. **$ sudo ln -s /bin/bash /usr/local/bin/shellenjaulada**
19.	Una vez creado el enlace, se modificará la shell por defecto del usuario que se quiera restringir, en este ejemplo el usuario se llamará usuarioSSH. **$ sudo chsh -s /usr/local/bin/shellenjaulada usuarioSSH**
20.	Posteriormente se creará el fichero "usr.local.bin.shellenjaulada" en el directorio de AppArmor. **$ sudo touch /etc/apparmor.d/usr.local.bin.shellenjaulada**

Paso	Descripción
21.	Se editará el fichero configurando los parámetros que más convengan a su organización. En el siguiente ejemplo se configura de una manera restrictiva el fichero que contendrá los parámetros de la shell "enjaulada". Para ello ejecute el siguiente comando. **$ gnomesu gedit /etc/apparmor.d/usr.local.bin.shellenjaulada &>/dev/null** Pulse "Guardar" y cierre el editor.  **Nota:** Hay que tener en cuenta, que la imagen anterior es solo un fragmento como ejemplo. La configuración de una shell predeterminada para un usuario genera un documento muy extenso y se tiene que adecuar a las necesidades específicas de su organización.
22.	Ejecute el siguiente comando para activar shellenjaulada en AppArmor **$ sudo aa-enforce shellenjaulada** 

Paso	Descripción
23.	Se debe comprobar que se está aplicando la nueva shell restrictiva. Para ello ejecute el siguiente comando. **$ sudo aa-status** 
24.	Por último, si quisiera añadir esta configuración al inicio de grub ejecute el siguiente comando y modifique la línea señalada en la imagen. **$ gnomesu gedit /etc/default/grub &>/dev/null**