

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD SOBRE CENTOS 7 (CLIENTE INDEPENDIENTE)



ABRIL 2019

Edita:



© Centro Criptológico Nacional, 2019

NIPO: 083-19-037-7

Fecha de Edición: abril de 2019

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

PRÓLOGO

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).

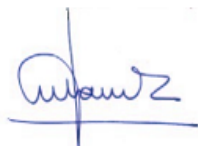
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad 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

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL	6
2. INTRODUCCIÓN	6
3. OBJETO	6
4. ALCANCE	7
5. DESCRIPCIÓN DEL USO DE ESTA GUÍA.....	8
5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA	8
5.2 ESTRUCTURA DE LA GUÍA	10
6. LINUX CENTOS, NUEVAS FUNCIONALIDADES Y PRINCIPALES CAMBIOS	11
6.1 INSTALACIÓN	11
6.1.1 ESCRITORIO	13
6.1.2 SEGURIDAD INICIAL	14
6.1.2.1 CONFIGURACIÓN DE CONTRASEÑAS	14
6.1.2.2 PARTICIONADO Y SISTEMA DE ARCHIVOS	15
6.1.2.3 CONFIGURACIÓN INICIAL	16
6.2 SEGURIDAD	17
6.2.1 AUTENTICACIÓN E INTEROPERATIVIDAD	21
6.2.2 PROTECCIÓN DEL SISTEMA	23
6.2.2.1 PROTECCIÓN DE LAS PARTICIONES	23
6.2.2.2 CONFIGURACIÓN SEGURA DE RED	25
6.2.2.3 CONFIGURACIÓN SEGURA DE PARÁMETROS DEL KERNEL	26
6.2.2.4 CONFIGURACIÓN DE TCP-WRAPPERS	28
6.2.3 LIMITACIÓN DE RECURSOS DE USUARIO	28
6.2.3.1 BLOQUEAR LA GENERACIÓN DE VOLCADOS DE MEMORIA	28
6.2.3.2 LÍMITE DE LOS RECURSOS DISPONIBLES PARA CADA USUARIO	28
6.2.3.3 BLOQUEAR EL USO DE ATAJO CRÍTICOS	29
6.2.3.4 ESTABLECIMIENTO DE CUOTAS DE DISCO	29
6.2.4 LIMITE DE ACCESO AL SISTEMA	29
6.2.4.1 CONTROL DE INFORMACIÓN DIVULGADA POR EL SISTEMA	29
6.2.4.2 CONFIGURACIÓN SEGURA DE SSH	30
6.2.4.3 MÓDULOS PAM DE AUTENTICACIÓN	30
6.2.4.4 LÍMITES DE INTENTO DE ACCESO AL SISTEMA	31
6.2.4.5 LÍMITE DE SERVICIOS DEL SISTEMA	31
6.2.5 ELEMENTOS INNECESARIOS DEL SISTEMA	32
6.2.5.1 PAQUETES INNECESARIOS	32
6.2.5.2 USUARIOS INNECESARIOS	33
6.2.6 PERMISOS Y VARIABLES DE ENTORNO	33
6.2.6.1 FICHEROS DE CONFIGURACIÓN	33
6.2.6.2 DIRECTORIO DE USUARIOS	33
6.2.6.3 PERMISOS EN FICHEROS Y DIRECTORIOS IMPORTANTES	34
6.2.7 KERNEL	34

6.3	REDES Y FIREWALL	36
6.3.1	RED	36
6.3.2	CONFIGURACIÓN DE FIREWALLD	38
6.4	SISTEMA	39
6.4.1	ACTUALIZACIÓN DEL SISTEMA	39
6.4.1.1	ONLINE	40
6.4.1.2	OFFLINE	40
6.4.2	SISTEMA Y SERVICIOS	40
6.4.3	ADMINISTRACIÓN DE RECURSOS	41
6.4.4	ARQUITECTURA	43
6.4.5	ALMACENAMIENTO	44
6.4.6	SISTEMA DE ARCHIVOS	45
6.4.7	ADMINISTRACIÓN Y MANTENIMIENTO	46
6.4.7.1	AUTOMATIZACIÓN DE TAREAS	46
6.4.7.2	LOGS DE SISTEMA	47
6.4.7.3	CONTROL DE INTEGRIDAD DE HARDWARE	48
6.4.7.4	CONTROL DE DISPOSITIVOS EXTRAIBLES	48
6.4.7.5	COPIAS DE SEGURIDAD	49

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Linux (CCN STIC 600), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

3. OBJETO

El presente documento contiene una guía para la configuración segura del sistema operativo CentOS (**CommunityENTERpriseOperatingSystem**) 7.4 Linux, en máquinas en las que posteriormente se instala aplicaciones que requieren un nivel óptimo de seguridad.

La configuración deberá realizarse en máquinas con el sistema operativo recién instalado, si bien también se deben llevar a cabo periódicamente sobre cualquier máquina para comprobar el estado de seguridad de la misma. En un anexo final se incluye un cuadro con cada uno de los chequeos que deben realizarse.

Para manejar información clasificada, la única versión del sistema operativo permitida es Linux CentOS 7.4 Linux (build 1708).

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y, por lo tanto, los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del cliente, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione los servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad, se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica con objeto de asegurar un cliente con el sistema operativo “Linux CentOS”, instalado en español en su versión 7.4 (build 1708). Se incluyen, además, operaciones básicas de administración para la aplicación de las mismas, así como una serie de recomendaciones para su uso.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

- a) Implementación del ENS en un escenario con clientes independientes con el sistema operativo CentOS 7.4.
- b) Implementación de plantillas de seguridad en función de las categorías de seguridad establecidos en el ENS para clientes CentOS 7.4 Linux independientes.
- c) Implementación de seguridad en un escenario de red clasificada clientes independientes CentOS 7.4.

Este documento incluye:

- a) **Descripción de versiones, opciones de mantenimiento** para todos aquellos operadores que tengan experiencia en versiones previas, se proporciona la información sobre las diferentes versiones, opciones de mantenimiento y versiones de las que dispone el sistema.
- b) **Descripción de las nuevas funcionalidades** para todos aquellos operadores que tengan experiencia en las versiones anteriores de CentOS, se incluyen las nuevas características del producto.
- c) **Funcionalidades de seguridad local adicionales.** Completa descripción de aquellas características y servicios que, no encontrándose definidos por defecto, agregan seguridad adicional a una infraestructura de CentOS 7.4 Linux como puesto de trabajo independiente.
- d) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.
- e) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.
- f) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad en clientes CentOS 7.4 Linux independientes.

- g) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de los equipos cliente con respecto a las condiciones de seguridad que se establecen en esta guía.
- h) **Configuración de cifrado de disco.** Establece los mecanismos para la configuración del cifrado que aporta CentOS 7.4 Linux.
- i) **Solucionarios adicionales.** Guías paso a paso para la comprobación de la configuración de operativas sobre el puesto de trabajo

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de securización que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

- a) Implementación de un escenario con cliente CentOS 7.4 Linux independiente.
- b) Deberá implementar la presente guía en función del entorno que requiera su organización.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo puesto cliente con Sistema Operativo CentOS 7.4 Linux en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

Para los entornos de ENS se podrá utilizar la versión de CentOS 7.4, con la opción de instalación deseada, que más se adapte a las necesidades de cada organización.

En un entorno de red clasificada donde se maneja información clasificada la única versión autorizada del Sistema Operativo CentOS 7 x86_64 Everything (build 1708) con la opción de instalación “instalación mínima”.

Las imágenes LiveCD y LiveDVD contienen un sistema de archivos comprimido de arranque, creado por un conjunto de scripts personalizados utilizan un archivo de configuración kickstart. Estas imágenes en vivo también se pueden instalar en el disco duro, obteniendo así una instalación de CentOS totalmente funcional. El conjunto de paquetes instalados de esa manera en un disco duro no se puede ajustar durante la instalación, ya que es una transferencia simple de la imagen existente en CD / DVD a un disco duro. Después de arrancar desde el disco duro, Yum puede usarse para agregar o eliminar paquetes.

Las imágenes MinimalCD contienen un mínimo de paquetes necesarios para una instalación funcional, sin comprometer la seguridad o la usabilidad de la red. Estas imágenes mínimas usan el instalador estándar de CentOS con todas sus características regulares menos la selección de paquetes. Yum se puede usar después de completar la instalación para agregar o eliminar paquetes.

La guía ha sido desarrollada y probada en entorno de uso de servicios Linux con la versión de CentOS 7 x86_64 Everything (build 1708).

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V sobre Windows Server 2012 R2 Datacenter con las siguientes características técnicas:

- a) Servidor Dell PowerEdge™ T320:
 - i. Intel Pentium Xeon CPU ES 2430 2.20GHz.
 - ii. HDD 1 TB.
 - iii. 64 GB de RAM.
 - iv. Interfaz de Red 1 Gbit/s.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de CentOS 7. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 o 32 bits (x64 o i386), con más de 1 GB de memoria RAM ambas versiones.

Se aconseja, no obstante, por seguridad y rendimiento, la implementación de versiones de 64 bits frente a las de 32 bits.

A partir de la versión 7, CentOS solo admite completamente la arquitectura x86-64, mientras que las siguientes arquitecturas no son compatibles:

- a) IA-32 en todas las variantes, tuvo soporte temporalmente en CentOS 7.0.
- b) IA-32 sin extensión de dirección física (PAE), no compatible desde CentOS 6
- c) IA-64 (arquitectura Intel Itanium), fue compatible con CentOS 3 y 4
- d) PowerPC de 32 bits (Apple Macintosh y PowerMac con procesador PowerPC G3 o G4), el soporte beta estaba disponible en CentOS 4
- e) IBM Mainframe (eServer zSeries y S / 390), no compatible desde CentOS 5
- f) Alpha, el soporte estaba disponible en CentOS 4
- g) El soporte SPARC, beta estaba disponible en CentOS 4

Nota: Puede comprobar los requisitos del sistema de CentOS en el siguiente enlace <https://wiki.centos.org/es/About/Product>.

La guía ha sido desarrollada con el objetivo de dotar a las infraestructuras con la seguridad adecuada dependiendo del entorno sobre el que se aplique. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, demonios o características deseadas.

Para garantizar la seguridad de los puestos de trabajo, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio “yum update --security “. Las actualizaciones por lo general están disponibles en los servidores espejo (servidores que replican los propios de RED-HAT), en las siguientes 72 horas después de su publicación por el equipo de RED-HAT. Normalmente estos paquetes están disponibles en 24 horas, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados. Deberá tener en consideración que CentOS está basado en RED-HAT y ofrecen diferentes tiempos de implementación de actualizaciones. En líneas posteriores de la presente guía se tratarán las consideraciones oportunas.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse el hecho de haber probado su configuración y comportamiento en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

Si estuviera aplicando la presente configuración de seguridad en un sistema ya configurado con una versión previa de esta guía, tenga en cuenta los cambios personalizados que hubiera realizado. La aplicación nuevamente de la seguridad a través de los paso a paso correspondientes, puede implicar que tenga que ajustar de nuevo los valores que ya hubiera personalizado.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones sino a servir como línea base de seguridad. Esta línea deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del sistema Linux CentOS dependiendo del entorno sobre el que vaya a ser aplicado, así como una diferenciación de la versión a utilizar.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

- a) **Anexo A:** En este anexo se define la configuración necesaria para adaptar los sistemas Linux CentOS 7 Linux en la versión 7.4 (build 1708) a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).
- b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas Linux CentOS 7 Linux en la versión 7.4 (build 1708) a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotara de la información necesaria y concreta para cada tipo de implementación.

6. LINUX CENTOS, NUEVAS FUNCIONALIDADES Y PRINCIPALES CAMBIOS

La versión 7 de CentOS incorpora nuevas funcionalidades con respecto a sus antecesoras.

Se enumerarán y se dará una breve descripción sobre las mismas, completando, posteriormente, con un detalle más significativo de aquellos elementos más críticos. No obstante, se debe tener en consideración que algunas de las funcionalidades y/o componentes citados no se encontrarán disponibles por defecto en la instalación o bien se encontrarán deshabilitados o limitados con las funcionalidades de seguridad que se aplican tras la fortificación del sistema a través de la presente guía.

Se describen a continuación las partes del sistema que hacen de CentOS la distribución más idónea para entornos clasificados y ENS.

- a) **Estabilidad.** CentOS se desarrolla de forma continua con el fin de ofrecer la plataforma perfecta para el software más reciente. En este proceso no se pierde de vista al aspecto de la compatibilidad con las aplicaciones más antiguas. Cada paso en el desarrollo orientado al futuro siempre se hace pensando en garantizar la estabilidad de los componentes activos. Además, este sistema convence con un gran rendimiento en cuanto a la virtualización (basada en KVM o máquina virtual basada en el núcleo) y con una alta disponibilidad.
- b) **Seguridad.** CentOS como solución corporativa basada en RHEL representa la mejor elección. Gracias a la detección proactiva de vulnerabilidades por parte del equipo de seguridad de Red Hat, su código fuente subyacente cuenta con un elevado nivel en seguridad. Además, a la hora de integrar nuevos programas o actualizar CentOS, la comprobación de la seguridad y de errores tienen prioridad.
- c) **Ciclos largos de mantenimiento y soporte.** Desde la primera versión de CentOS, tanto los lanzamientos grandes como los pequeños han estado estrechamente vinculados a las publicaciones de RHEL. Para la adaptación del código, el equipo de desarrollo prevé un periodo de 2 a 6 semanas (o de unas pocas horas si se trata de pequeños cambios). Los números de cada versión se mantienen (por ejemplo, RHEL 6.2 a CentOS 6.2), aunque desde la versión 7 se añade una marca temporal (timestamp) que hace referencia a la publicación del código base. Así, por ejemplo, la fuente de la versión 7.0-1406 fue publicada en junio de 2014. Además del control de versiones, CentOS también se ha ocupado de las directrices para el periodo de soporte técnico: está previsto un soporte general de hasta 7 años y un suministro de hasta 10 años de actualizaciones de seguridad.

6.1 INSTALACIÓN

El interfaz gráfico encargado de la instalación en CentOS 7 Linux es Anaconda, con sus correspondientes cambios con respecto a versiones anteriores:

- a) Se ha rediseñado el interfaz gráfico de Anaconda y ahora tiene soporte para LVM de aprovisionamiento fino y sistema de archivos Btrfs. Posteriormente en el apartado de sistema de archivos se detallarán más a fondo estas nuevas funcionalidades.

Otro punto de interés en la herramienta Anaconda es que soporta geolocalización por GEOIP para detección de idioma y zonas horarias en instalación.

- b) La interfaz del instalador gráfico ahora contiene una pantalla adicional que permite configurar el mecanismo de volcado de daños de kernel **Kdump** durante la instalación. Anteriormente, se configuraba después de la instalación mediante la herramienta **firstboot**, la cual no era accesible sin una interfaz gráfica. Ahora se puede configurar Kdump como parte del proceso de instalación en sistemas sin un entorno gráfico. La nueva pantalla se accede desde el menú principal de instalador.

La pantalla de partición manual ha sido rediseñada para mejorar la experiencia del usuario. Algunos de los controles han sido desplazados a diferentes sitios de la pantalla.

- c) Se han agregado nuevas opciones Kickstart para configuración de puente. El instalador ya no utiliza consolas para desplegar registros. En su lugar, todos los registros están en paneles tmux en la consola virtual 1 (tty1).

```
(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?

(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?

(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?

(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?

(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?

(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?

(anaconda:1131): Gtk-WARNING **: Allocating size to pyanaconda+ui+gui+MainWindow
0x1f5a260 without calling gtk_widget_get_preferred_width/height(). How does the
code know the size to allocate?
```

- d) La interfaz de línea de comandos para Anaconda ahora incluye ayuda completa. La interfaz de línea de comandos le permite ejecutar el instalador en un sistema instalado, el cual es útil para instalaciones de imágenes de disco.

6.1.1 ESCRITORIO

CentOS 7 Linux provee una interfaz Gui (escritorio) que interactúa entre el software instalado en el equipo, los dispositivos hardware y el usuario. Linux ofrece muchas alternativas. Los entornos de escritorio más populares son GNOME, KDE, XFCE, MATE y Cinnamon.

a) GNOME 3

- i. La experiencia del usuario de GNOME 3 es definida ampliamente por GNOME Shell, el cual reemplaza el Shell de escritorio de GNOME 2. Aparte de la administración de ventanas, GNOME Shell proporciona la barra superior en la pantalla, la cual alberga el área de 'estatus del sistema' en la parte superior derecha, un reloj y una esquina que cambia a Vista de actividades, la cual proporciona fácil acceso a aplicaciones y ventanas.
- ii. La interfaz predeterminada de GNOME Shell en CentOS 7 es GNOME Classic, el cual presenta una lista de ventana en la parte inferior de la pantalla, y los menús de las Aplicaciones y los Sitios tradicionales.
- iii. CentOS 7 introduce una herramienta de virtualización de escritorio gráfica liviana para ver y acceder máquinas virtuales y sistemas remotos. GNOME Boxes proporciona una forma de probar diferentes sistemas operativos y aplicaciones desde el escritorio, mediante una configuración mínima.
- iv. Para obtener más información sobre GNOME 3, consulte la ayuda de GNOME.

6.1.2 SEGURIDAD INICIAL

Para asegurar de forma correcta cualquier sistema operativo, es recomendable seguir una serie de pautas de configuración desde el inicio. Por ello, se tendrán en cuenta configuraciones iniciales de instalación tales como el particionado, el sistema de archivos a utilizar o la complejidad de contraseñas entre otros.

Las contraseñas son las llaves del sistema. Deben ser lo más seguras posibles para evitar inicios de sesión no autorizados, que es el primer paso hacia problemas de seguridad mayores. El uso de contraseñas lo suficientemente fuertes como para amortizar un ataque es un paso decisivo y a la vez sencillo que ahorrará muchos problemas en el futuro.

6.1.2.1 CONFIGURACIÓN DE CONTRASEÑAS

Muchas contraseñas utilizadas por usuarios son bastante fáciles de adivinar. CentOS Linux proporciona diferentes maneras de proveer autenticación al sistema, incluyendo contraseñas encriptadas con el comando **crypt**, las contraseñas **shadow**, **Kerberos**... Etc. En cualquier situación en la cual se elija una contraseña como parte de un esquema de autenticación, la seguridad de ese esquema estará por lo menos parcialmente a la merced de la complejidad de la contraseña elegida.

Una contraseña segura tiene que tener al menos estas características:

- a) Tener una longitud mínima de 8 caracteres
- b) Mayúsculas y minúsculas alternadas
- c) Tantos signos de puntuación y números como sea posible
- d) Evitar palabras o frases comunes que puedan figurar en cualquier diccionario
- e) No tener relación evidente con datos personales del usuario: Nombre, fecha de nacimiento, etc.

Otro factor a tener en cuenta es la **caducidad de contraseñas**. Dentro de las tareas frecuentes que se realizan en Linux, se encuentra la de administrador de cuentas de usuario, tanto en su creación y edición, como en establecimiento o modificación de la caducidad y el vencimiento de las contraseñas de los usuarios, siendo política de seguridad modificar regularmente la misma.

Para esto, puede ser útil el comando **chage** el cual es usado para modificar la información de caducidad de la contraseña de un usuario específica, permite ver la información de antigüedad de la cuenta de un usuario o cambiar el número de días entre los cambios de contraseña y la fecha de la última contraseña.

En esta guía se configurará de manera permanente una caducidad de contraseña para nuevos usuarios y modificará la política de seguridad de los usuarios ya existentes para que cumplan estos requisitos de seguridad establecidos. Las recomendaciones de configuración en cuanto a la caducidad de las contraseñas se configurarán en el fichero **/etc/login.defs** y serán las siguientes:

- El periodo máximo durante el que se puede mantener una contraseña será de 60 días
- La longitud mínima de la contraseña será de 8 caracteres.
- El período mínimo durante el que se debe mantener una contraseña será de 15 días.
- El período durante el que el sistema avisará de una futura caducidad de la contraseña será de 15 días.

6.1.2.2 PARTICIONADO Y SISTEMA DE ARCHIVOS

Se debe establecer la cantidad y tamaño de las particiones, así como el sistema de archivos a utilizar. Aunque estos factores dependen en gran medida del uso que se vaya a hacer del sistema, se van a dar una serie de recomendaciones para ayudar a su correcta elección.

Para realizar una correcta elección del sistema de archivos hay que tener en cuenta los tipos de archivos más comunes que existen en Linux.

Sistema de archivos	Sistema operativo	Descripción
FAT	Heredado	Sistema de archivos heredado que se ha adoptado universalmente. FAT12, FAT16 y FAT32.
Ext2	Linux	El segundo Filesystem: Sigla de "Extended Graphics Array" utilizado por muchas distribuciones Linux.
Ext3	Linux	El tercero Filesystem: Se añadió registro diario (journaling), utilizado por muchas distribuciones Linux.
Ext4	Linux	El cuarto Filesystem: utilizado por muchas distribuciones Linux. "Extiende los límites de almacenamiento."
JFS	Linux	Journal File System: fue introducido por IBM y aún se admite, pero ha sido sustituido por Ext4.
XFS	Linux/Red-HAT/CentOS	Sistema de archivos de 64 Bits, actualmente opción por defecto en Red Hat/CentOS Linux.
ReiserFS	Linux/SUSE	Se trataba de un formato de archivo que estaba en uso en varias distribuciones, pero ha sido reemplazado por Ext3.
Btrfs	Linux/SUSE	CentOS/Red-Hat tienen soporte para este sistema de archivos, SUSE ofrece este sistema por defecto, recomendándolo para particiones críticas del sistema.

Se optará por elegir **XFS** como sistema de archivos recomendado.

A continuación, Se muestra una organización de las particiones como ejemplo, siendo viables alternativas en función de los usos del sistema.

PARTICIÓN	TAMAÑO
/	120 GiB xfs
/boot	500 MiB xfs
/boot/efi	Default MiB vfat
/var	50 GiB xfs
/tmp	25 GiB xfs
/var/log	35 GiB xfs
/home	200 GiB xfs
/var/log/audit	15 GiB xfs
/var/www	50 GiB xfs
swap	½ Memoria RAM Equipo

Posteriormente, una vez instalado el sistema se recomienda cifrar las particiones aumentando la seguridad de la misma e impidiendo que personal no autorizado pueda acceder a datos críticos.

6.1.2.3 CONFIGURACIÓN INICIAL

Por defecto el sistema operativo, crea ciertas configuraciones para facilitar el acceso al usuario, habilitando la mayor parte de funcionalidades y aumentando la velocidad de instalación del mismo. Estas configuraciones en muchas ocasiones pueden ser motivo de posibles brechas de seguridad.

Para evitar brechas innecesarias, se configurarán ciertos parámetros de manera correcta:

- a) **GRUB.** GNU Grand Unified Boot loader (GRUB) es un gestor de arranque múltiple desarrollado inicialmente para el sistema GNU Hurd. El gestor de arranque grub tiene varias funciones, pero sin duda su misión principal es seleccionar qué sistema operativo instalado o kernel cargar en el momento de arranque del sistema. Permite también que el usuario transmita argumentos al kernel. Por estos motivos Grub solo tiene que ser accesible por root y mediante contraseña, aplicando los pasos de esta guía que se describirán posteriormente conseguiremos:
 - i. Bloquear el acceso a la línea de comandos del Grub.
 - ii. Bloquear la posibilidad de edición de las entradas del Grub.
 - iii. Bloquear la posibilidad de ejecución de todas las entradas del Grub.

- b) **Contraseña segura para Root.** Cuando se habla de root, se refiere a la cuenta superusuario en Linux, aquella que posee todos los privilegios y permisos para realizar acciones sobre el sistema. Para ciertas acciones que afectan al sistema de archivos, se requiere tener acceso root. Sin embargo, se debe tener un conocimiento sobre las acciones que se realizan, ya que una acción realizada de manera errónea podría ocasionar daños importantes en el sistema. Para evitar el uso de instrucciones con privilegios de superusuario la cuenta root tiene que estar dotada con una contraseña segura que evite que cualquier usuario malintencionado pueda comprometer de algún modo el sistema.
- c) **Usuarios UID 0.** En el fichero `/etc/passwd/` existe un campo UID por cada usuario, que corresponde al identificador de cada usuario. Algunas distribuciones de Linux por defecto, crean varios usuarios con UID 0 que corresponde al identificador de superusuario. Si existen varios superusuarios en el sistema la probabilidad de vulnerar el mismo es mayor, por este motivo se deben limitar los usuarios con UID 0 únicamente a root, siendo el único usuario habilitado para tener control total sobre el sistema.
- d) **Cuentas sin contraseñas.** En Linux existe la opción de configurar una cuenta de usuario sin contraseña, aunque ese usuario no pertenezca a los denominados “sudores” (administradores). En el sistema no debe de haber ningún usuario sin contraseña, esto supondría una vulnerabilidad, ya que cualquier usuario podría acceder a información sensible sin necesidad de estar autorizado para ello.
- e) **Arranque por defecto.** A partir de la versión 7 de RHEL, CentOS Linux, cambia los niveles de ejecución ya no pasa por modificar el archivo `/etc/inittab` y cambiar el id de runlevel tal y como se hacía hasta la versión 6. Ahora, tanto para controlar los niveles de ejecución como los servicios (systemd) se utiliza el comando `systemctl` con los parámetros correspondientes. Por lo que se procederá a configurar por medio de `systemctl` el modo por defecto (`systemctl set-default`) texto (`multi-user.target`).

6.2 SEGURIDAD

Linux es un sistema operativo multiusuario, lo que significa que puede tener más de un usuario trabajando al mismo tiempo desde sus diferentes estaciones de trabajo. A raíz de esto, el sistema debe proteger a unos usuarios frente a otros y a sí mismo.

En Linux se adopta como norma básica de seguridad, asignarle a cada uno de los usuarios, sólo los permisos mínimos y necesarios para que este pueda realizar su trabajo, sin comprometer el de los demás y la integridad del sistema.

El sistema de archivos de Linux sigue el estándar de Unix, posee una estructura determinada y compatible con los demás sistemas Unix. Estos tienen su origen en la denominada raíz" o "root" que es representado por `/`. De este directorio se desprenden todos los Archivos (Archivos ordinarios - Directorios - Archivos Especiales) a los que el sistema operativo tiene acceso.

Estos son los cambios realizados en las herramientas de CentOS 7 que abordan el tema de la seguridad:

a) **OpenSSH** versión 6.6.1p1.

i. Acceso de shell chroot con OpenSSH.

- Por lo general, a cada usuario de Linux se le asigna un usuario de SELinux mediante la política de SELinux, lo cual permite a los usuarios heredar las restricciones impuestas a los usuarios de SELinux. Hay una asignación predeterminada para el usuario **unconfined_u** de SELinux.
- La opción ChrootDirectory para ejecutar chroot puede utilizarse para usuarios no confinados sin necesidad de cambio, pero para usuarios confinados, tales como **staff_u**, **user_u**, o **guest_u**, se debe establecer la variable de SELinux **selinuxuser_use_ssh_chroot**. Se recomienda a los administradores usar el usuario **guest_u** para todos los usuarios a los que se ha ejecutado chroot cuando se usa la opción ChrootDirectory para obtener alta seguridad.

ii. El conjunto de herramientas OpenSSH, agrega varias funcionalidades relacionadas con la criptografía:

- El intercambio de llave mediante curva elíptica Diffie-Hellman en Curve25519 de Daniel Bernstein está ahora soportada. Este método ahora es el predeterminado tanto el servidor como el cliente lo soportan.
- Se agregó soporte para el uso del esquema de firma de curva elíptica Ed25519 como un tipo de llave pública. Ed25519, el cual puede utilizarse para llaves de usuario y de host, ofrece más seguridad y rendimiento que ECDSA y DSA.
- Se ha agregado un nuevo formato de llave que utiliza la función de derivación de claves bcrypt (KDF). Este formato es el predeterminado para llaves Ed25519, pero también puede solicitarse para otros tipos de llaves.
- Se agregó una nueva cifra de transporte, chacha20-poly1305@openssh.com. Combina la cifra de corriente de Daniel Bernstein ChaCha20 con el código de autenticación del mensaje Poly1305 (MAC).

b) **Se requiere múltiple autenticación.** CentOS 7 soporta múltiple autenticación en la versión 2 del protocolo SSH, mediante la opción **AuthenticationMethods**. Esta opción listal una o más nombres de métodos de autenticación separados por coma. El correcto de todos los métodos en cualquier lista requiere autenticación para completar. Esto permite, por ejemplo, que un usuario tenga que autenticarse mediante una llave pública o GSSAPI antes de que se les ofrezca autenticación de contraseña.

- c) **Proxy GSS.** Es el servicio de sistemas que establece contexto de Kerberos API de GSS a nombre de otras aplicaciones. Esto trae beneficios de seguridad, por ejemplo, en una situación el acceso a keytab del sistema se comparte entre varios procesos, un ataque contra ese proceso conlleva a la personificación de Kerberos para todos los procesos.
- d) **Cambios en NSS.** Los paquetes **nss** han sido mejorados a la versión 3.15.2 de la corriente principal de desarrollo. Las firmas del algoritmo Message-Digest 2 (MD2), MD4, y MD5 ya no se aceptan para el protocolo de estatus de certificado en línea (OCSP) o las listas de revocación de certificado (CRL), consistentes con su manejo para las firmas generales de certificado.
- e) El paquete **Cipher** (RFC 5288 y RFC 5289) del Modo de contador Galois Estándar de cifrado avanzado (AES-GCM), ha sido añadido para usar cuando se negocia TLS 1.2. Específicamente, ahora tienen soporte los siguientes paquetes de cifras:
 - i. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - ii. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - iii. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 - iv. TLS_RSA_WITH_AES_128_GCM_SHA256
- f) **SELinux CentOS 7.** Linux soporta la extensión del kernel SELinux (Security Enhanced Linux), un producto de código abierto que cuenta con la colaboración de Red Hat y la NSA. Este programa implementa controles de autorización para el uso de los recursos informáticos, protegiendo, de este modo, contra accesos no autorizados. En la version CentOS 7.4 se implementan las siguientes características:
 - i. Nuevo almacén de módulos SELinux admite prioridades. El concepto de prioridad proporciona la capacidad de anular un módulo de sistema con un módulo de mayor prioridad.
 - ii. SELinux Common Intermediate Language (CIL) proporciona una sintaxis clara y simple que es fácil de leer, analizar y generar mediante compiladores de alto nivel, herramientas de análisis y herramientas de generación de políticas.
 - iii. Las costosas operaciones de SELinux, como las instalaciones de políticas o la carga de nuevos módulos de políticas, ahora son mucho más rápidas.

Nota: La ubicación predeterminada de los módulos SELinux permanece en el directorio `/etc/selinux/` en CentOS 7, mientras que la versión ascendente usa `/var/lib/selinux/`. Para cambiar esta ubicación para la migración, establezca la opción `store-root =` en el archivo `/etc/selinux/semanage.conf`.

g) **Firewalld** versión 0.4.3.2.

- i. Mejoras de rendimiento: firewalld se inicia y se reinicia significativamente más rápido gracias al nuevo modelo de transacción que agrupa reglas que se aplican simultáneamente. Este modelo usa los comandos de restauración de iptables. Además, las herramientas firewall-cmd, firewall-offline-cmd, firewall-config y firewall-applet se han mejorado teniendo en cuenta el rendimiento.
- ii. El usuario ahora puede controlar la configuración de zona para las conexiones en NetworkManager. Además, las configuraciones de zona para las interfaces también están controladas por firewalld y en el archivo ifcfg.
- iii. Opción de registro predeterminado: con la nueva configuración LogDenied, el usuario puede depurar fácilmente y registrar paquetes denegados.
- iv. Compatibilidad con distintos ipset:
 - hash:net
 - hash:ip
 - hash:ip,port
 - hash:ip,port,ip
 - hash:ip,port,net
 - hash:ip,mark
 - hash:net,net
 - hash:net,port
 - hash:net,port,net
 - hash:net,iface

h) **Audit** versión 2.7.6. Los paquetes de **Audit** contienen las utilidades de espacio de usuario para almacenar y buscar los registros de auditoría que han sido generados por el subsistema de auditoría en el kernel de Linux. Los paquetes de Audit se han actualizado a la versión 2.7.6, que proporciona una serie de mejoras y correcciones de errores sobre la versión anterior. Cambios notables incluyen lo siguiente:

- i. El daemon de auditoría ahora incluye una nueva técnica de descarga denominada incremental_async, que mejora su rendimiento aproximadamente 90 veces.
- ii. El sistema de Audit ahora tiene muchas más reglas que se pueden crear en una política de auditoría. Algunas de estas nuevas reglas incluyen soporte para la Guía de Implementación Técnica de Seguridad (STIG), Estándar de Seguridad de Datos PCI y otras capacidades tales como auditar la ocurrencia de llamadas de sistema de 32 bits, uso de energía significativo o carga de módulos.
- iii. El archivo de configuración auditd.conf y el comando auditctl ahora admiten muchas opciones nuevas.

- iv. El sistema de auditoría ahora admite un nuevo formato de registro enriquecido (enriched), que resuelve el UID, GID, syscall, arquitectura y direcciones de red. Esto ayudará en el análisis de registros en una máquina que diferente de donde se generó el registro.
- v. La utilidad **ausearch** tiene una nueva opción de salida de formato. La opción de texto de formato presenta un evento como una frase en inglés que describe lo que está sucediendo. La opción `--format csv` normaliza los registros en un sujeto, objeto, acción, resultados y cómo se produjo, además de algunos campos de metadatos que se imprimen en el formato de valores separados por comas (CSV). Esto es adecuado para enviar información de eventos a una base de datos, hoja de cálculo u otros programas analíticos para ver, trazar o analizar eventos de auditoría.
- vi. La utilidad **auditctl** ahora puede restablecer el contador de eventos perdidos en el kernel a través de la opción de línea de comandos `--reset-lost`. Esto facilita la verificación de eventos perdidos ya que puede restablecer el valor a cero diariamente.
- vii. **ausearch** y **aureport** ahora tienen una opción de arranque para la opción de línea de comandos `--start` para encontrar eventos desde que el sistema inició.
- i) **pam faillock**. El módulo **pam_faillock** ahora permite especificar usando la opción `unlock time = never` que el bloqueo de autenticación de usuario causado por múltiples fallas de autenticación nunca debería expirar.
- j) **USBGuard** Proporciona protección del sistema contra dispositivos USB intrusivos mediante la implementación de funciones básicas de listas blancas y listas negras basadas en los atributos del dispositivo. Para hacer cumplir una política definida por el usuario, utiliza la función de autorización del dispositivo USB del kernel de Linux. USBGuard proporciona los siguientes componentes:
 - i. Un componente daemon para procesos internos de comunicación (IPC).
 - ii. Interfaz de línea de comandos para interactuar con la instancia de USBGuard.
 - iii. Un lenguaje de reglas para escribir políticas de autorización a dispositivos USB.
 - iv. La API C ++ para interactuar con el componente daemon implementado en una biblioteca compartida.

6.2.1 AUTENTICACIÓN E INTEROPERATIVIDAD

La autenticación es el proceso por el que se comprueba la identidad de alguien o algo, para ver si es lo que dice ser. Ese "alguien" o "algo" se denomina principal. La autenticación requiere pruebas de identidad, denominadas credenciales. Por ejemplo, una aplicación cliente puede presentar una contraseña como sus credenciales. Si la aplicación cliente presenta las credenciales correctas, se asume que es quien dice ser.

Posteriormente se definen algunas nuevas características implementadas en la versión CentOS 7.4 Linux de acuerdo a la autenticación e interoperatividad:

- a) Nueva implementación de confianza.
- b) El uso del ID de usuario o el ID de grupo definido en el directorio activo en lugar del ID de usuario o ID de grupo generado desde el identificador de seguridad, ahora tiene soporte para clientes de CentOS/Red-HAT Linux 6.3. Esta implementación de confianza es útil si los atributos de POSIX están definidos en el directorio activo.
- c) Se actualizó el complemento slapi-nis.
- d) Se actualiza un complemento de servidor de directorio, slapi-nis, el cual permite a los usuarios de directorio activo autenticar en clientes de legado.
- e) Mecanismo de respaldo y restauración para IPA.
- f) Samba 4.6.2.
- g) CentOS 7 incluye los paquetes de samba mejorados a la versión más reciente de la corriente de desarrollo principal, la cual introduce varias correcciones de errores y mejoras, lo más notable es el soporte para el protocolo SMB3 en las herramientas de servidor y de cliente.
- h) Además, SMB3 permite conexiones de transporte cifradas a los servidores de Windows que soportan SMB3, al igual que los servidores de Samba. También, Samba 4.6.2 añade soporte para operaciones de copia del lado del servidor. Los clientes que hacen uso del soporte de copia de lado del servidor, tales como los lanzamientos más recientes de Windows, deberán experimentar mejoras para operaciones de copia de archivos.

Nota: Los paquetes actualizados de samba retiran varias opciones de configuración que ya están depreciadas. Las más importantes son la de los roles de servidor `security=share` y `security=server`. También la herramienta de configuración de web SWAT ha sido retirada completamente. Hallará más información en las notas de lanzamiento de Samba 4.0 ,4.1 y 4.6:

- <https://www.samba.org/samba/history/samba-4.0.0.html>
- <https://www.samba.org/samba/history/samba-4.1.0.html>
- <https://www.samba.org/samba/history/samba-4.6.0.html>
- <https://www.samba.org/samba/history/samba-4.6.2.html>

Observe que varios archivos tdb han sido actualizados. Esto significa que todos los archivos tdb se actualizarán tan pronto como usted inicie la nueva versión del demonio `smbd`. No podrá pasar a una versión anterior de Samba a menos que tenga copias de seguridad de los archivos tdb.

- i) Uso de proveedores sudo de AD y LDAP
- j) El proveedor AD es un segundo plano para conectar a un servidor de directorio activo. En CentOS 7.0, el uso del proveedor sudo AD junto con el proveedor LDAP está soportado. Para habilitar el proveedor sudo AD, añada el parámetro **`sudo_provider=ad`** en la sección de dominio del archivo `sssd.conf`.

6.2.2 PROTECCIÓN DEL SISTEMA

En la actualidad, al menos en algún momento, importantes organizaciones, tanto públicas como privadas, han sufrido ataques a sus sistemas informáticos. Estos ciberataques no sólo afectan a ciertas compañías, sino que pueden llegar a afectar a la seguridad nacional.

Por esta y por muchas razones es prioritario proteger cualquier sistema que tenga cierta criticidad. Esta parte se centrará en la protección de las partes más vulnerables del sistema, evitando dejar configuraciones por defecto y permisos innecesarios.

6.2.2.1 PROTECCIÓN DE LAS PARTICIONES

Para proteger el uso indebido de las diferentes particiones y los ficheros alojados en ellas, se deberá analizar cuál es el uso principal de cada partición, y así determinar las opciones que se utilizarán para montarlas. Estas opciones se reflejarán en el fichero **/etc/fstab**.

Las opciones que se configuren en el fichero **/etc/fstab** se aplicarán de forma automática en el inicio de montaje de cada partición.

Las particiones se pueden montar de distintas formas para que limiten determinados permisos:

- a) **Noauto**: La partición no se montará automáticamente.
- b) **Noexec**: La partición no admitirá la ejecución de ficheros desde la misma.
- c) **Nodev**: La partición no admitirá la instalación de dispositivos.
- d) **Permisos (ro), (rw)**: La partición se configurará con permisos read-only (ro, solo lectura), read-write (rw, lectura y escritura).

Nota: Hay que tener en cuenta que la opción default monta la partición con las opciones **rw, suid, dev, exec, auto, nouser, async**.

A continuación, se listan las particiones más importantes y las recomendaciones seguras de montaje:

- a) **/boot**: Contiene información sobre el arranque del sistema.
 - i. Se montará con las opciones **noauto, noexec, nodev, nosuid, ro**.
- b) **/boot/efi**.
 - i. Se montará con los siguientes parámetros **umask=0077, shortname=winnt <dump> 0 <pass> 0**.
- c) **/usr y /opt**: Contienen ficheros ejecutables del sistema.
 - i. Se montará con las opciones **nodev, ro**.
- d) **/var**: Contiene archivos muy variables del sistema (logs, BBDD, contenido web, etc.)
 - i. Se montará con las opciones **defaults, nosuid**.
- e) **/var/log**: Contiene los logs del sistema.
 - i. Se montará con las opciones **nodev, noexec, nosuid, rw**.

- f) **/var/log/audit:** Contiene información y logs de la herramienta Audit.
 - i. Se montará con las opciones **nodev, noexec, nosuid, rw**.
- g) **/var/www:** Contiene principalmente el contenido Web.
 - i. Se montará con las opciones **nodev, noexec, nosuid, rw**.
- h) **/home y /tmp:** Contienen los archivos del usuario y los temporales del sistema.
 - i. Se montará con las opciones **nodev, noexec, nosuid, rw** y especialmente en /home se le asignará **cuota de disco**.
- i) **/media/XXX:** Contiene montaje de particiones de dispositivos extraíbles.
 - i. Se montará con las opciones **noauto, nodev, nosuid, rw**.
- j) **/:** Contiene la partición raíz del sistema.
 - i. Se montará con la opción de **lectura y escritura (rw)**.
- k) **Swap:** Se trata de la memoria de intercambio, memoria que usará el sistema cuando necesite espacio en memoria RAM.
 - i. Se montará con la opción **defaults, <dump> 0 <pass> 0**.

Excepciones. Para realizar ciertas acciones en determinados momentos se modificará la forma de montaje.

- l) **/boot:** Si se tuviera que actualizar el kernel, será necesario montar la partición temporalmente en lectura y escritura (**rw**).
- m) **/usr y /opt:** Si se desea instalar una nueva aplicación o actualizar una ya existente, será necesario montar la partición correspondiente manualmente en modo de lectura y escritura (**rw**).

Nota: <dump> - Utilizado por el programa dump («volcado») para decidir cuándo hacer una copia de seguridad. Dump comprueba la entrada en el archivo fstab y el número de la misma le indica si un sistema de archivos debe ser respaldado o no. Las entradas posibles son 0 y 1. Si es 0, dump ignorará el sistema de archivos, mientras que, si el valor es 1, dump realizará una copia de seguridad. La mayoría de los usuarios no tendrán dump instalado, por lo que deben poner el valor 0 para la entrada <dump>.

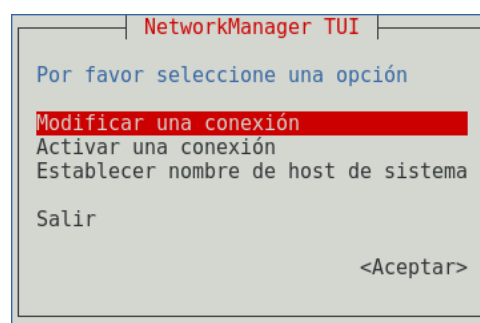
<pass> - Utilizado por fsck para decidir el orden en el que los sistemas de archivos serán comprobados. Las entradas posibles son 0, 1 y 2. El sistema de archivos raíz («root») debe tener la más alta prioridad: 1 - todos los demás sistemas de archivos que desea comprobar deben tener un 2-. La utilidad fsck no comprobará los sistemas de archivos que vengan ajustados con un valor 0 en <pass>.

Una vez realizadas todas las modificaciones debe quedar el fichero **/etc/fstab** de esta manera:

Particiones	Sistema de archivos	Permisos
dev/mapper/centos-root/	xfs	defaults 1 1
UUID=xxxxxxxxxxxxxxxxxx/boot	xfs	noauto,noexec,nodev,nosuid,ro 1 2
UUID=xxxxxxxxxxxxxxxxxx/boot/efi	xfs	umask=0077,shortname=winnt 0 0
/dev/mapper/centos-home/usr	xfs	nodev,ro 1 2
/dev/mapper/centos-home/opt	xfs	nodev,ro 1 2
/dev/mapper/centos-home/home	xfs	nodev,noexec,nosuid,rw 1 2
/dev/mapper/centos-tmp/tmp	xfs	nodev,noexec,nosuid,rw 1 2
/dev/mapper/centos-var/var	xfs	defaults,nosuid 1 2
/dev/mapper/centos-var_log/var/log	xfs	nodev,noexec,nosuid,rw 1 2
/dev/mapper/centos-var_log_audit/var/log/audit	xfs	nodev,noexec,nosuid,rw 1 2
/dev/mapper/centos-var_www/var/www	xfs	nodev,noexec,nosuid,rw 1 2
/dev/mapper/centos-swap swap	swap	defaults 0 0

6.2.2.2 CONFIGURACIÓN SEGURA DE RED

Siempre que sea posible deberá configurarse la red de forma estática, asignando direcciones IP de forma manual a cada sistema en lugar de utilizar los protocolos DHCP o BOOTP. Para ello podrá utilizarse el asistente **nmtui**(NetworkManager) o se podrán realizar manualmente los cambios en los ficheros **/etc/sysconfig/network-scripts/ifcfg-enpXXX** (configuración de los interfaces), y **/etc/resolv.conf** (servidores de resolución de nombres).



Es recomendable deshabilitar ciertos protocolos que pueden afectar a la vulnerabilidad del sistema y que están orientados a usuarios sin conocimientos de administración de redes, uno de estos protocolos es el protocolo **Zeroconf**.

Zeroconf o APIPA (Automatic Private Ip Address), es un protocolo que se encarga de la asignación automática por parte del sistema operativo de una ip tipo 169.254.X.X con máscara 255.255.0.0. De éste modo, dos equipos sin configuración de red, podrían comunicarse entre sí por medio de este protocolo.

Del mismo modo, el protocolo de enrutamiento **IPV6** está diseñado para resolver muchos de los problemas que se producen en la versión actual del conjunto de protocolo de Internet (conocido como IPv4) en relación con el agotamiento de direcciones, la configuración automática, la extensibilidad, etc. Este protocolo debe de ser desactivado en caso de que no sea necesaria su utilización para el buen funcionamiento de la red.

Al igual que el protocolo **RPC** (Remote Procedure Call) para IPV6 debe ser deshabilitado si no se contempla administración remota del sistema por medio de redes IPV6.

Para prevenir ataques a las posibles vulnerabilidades en la implementación de algunos protocolos de la pila de red de Linux (dccp, sctp, rds, tipc) se añaden archivos **.conf** al directorio **/etc/modprobe.d** para que se ejecute la shell **/bin/false** en lugar de cargar el módulo del protocolo indicado.

6.2.2.3 CONFIGURACIÓN SEGURA DE PARÁMETROS DEL KERNEL

El kernel Linux permite modificar una gran cantidad de parámetros sin necesidad de volverlo a compilar. Estos parámetros afectan al funcionamiento del sistema en mayor o menor medida así que conviene tener conocimiento de cómo modificarlos. El comando **sysctl** suele ser la forma más común de hacerlo. Los valores se almacenan en el directorio **/proc/sys**.

Hay que tener en cuenta que cuando se modifican los parámetros del kernel vía **sysctl** los cambios surten efecto al instante, pero estos cambios se perderán en el momento que el equipo se reinicie, por eso conviene guardar los cambios en el fichero de configuración de **sysctl** **/etc/sysctl.conf**.

En esta guía se verá como configurar el sistema con ciertos parámetros que afectan a la seguridad ya sea directa o indirectamente.

- a) **No responder a peticiones icmp.** Los mensajes ICMP pueden ser utilizados por atacantes remotos, ya sea para identificar ciertas máquinas activas o para intentar explotar las debilidades del protocolo ICMP. Este se ha diseñado para comunicaciones unidireccionales que no requieren autenticación, lo cual habilita a los atacantes a desencadenar ataques DoS o ataques que brindan acceso a los paquetes entrantes y salientes a individuos desautorizados como pueden ser ataques por flujo de ping, por flujo ICMP_ECHO y ataques "smurf".
- b) **No responder a peticiones broadcast.** Cuando una máquina envía un paquete a la dirección de broadcast (por ejemplo, 192.168.1.255), éste es entregado a todas las máquinas existentes en la red local. A continuación, todas las máquinas deben enviar un mensaje ECHO del protocolo ICMP. Esto puede provocar una congestión de la red, a la vez que permite determinar que sistemas están activos en la red.
- c) **Deshabilitar source routing.** El source routing (o encaminamiento en origen) es una funcionalidad propia del protocolo IP que permite enviar dentro del mismo paquete de datos la información necesaria para su enrutamiento, es decir, la dirección IP de cada uno de los dispositivos de red intermedios que deben cruzarse hasta llegar al destino final. Esto permite al emisor de un paquete dictar la ruta por la que deberá transmitirse a lo largo de la red. Esta característica presenta un grave riesgo de seguridad. De hecho, la mayoría de los routers ignoran ya por defecto esta opción.

- d) **Protegerse ante ataques tcp syn.** El "ataque SYN" (también denominado "inundación TCP/SYN") consiste en saturar el tráfico de la red aprovechando el mecanismo de negociación de tres vías del protocolo TCP comenzando varias veces el proceso de establecimiento de conexión a una máquina, sin llegar a completarlo.
- e) **Deshabilitar la redirección icmp.** Si un host envía un paquete por una ruta no válida, los routers utilizarán los mensajes de redireccionamiento ICMP para informarle a los hosts en el link de datos que está disponible una ruta mejor para el destino en particular. Dicho mensaje origina que el host modifique sus tablas de enrutamiento. Sin embargo, si un atacante tiene la capacidad de enviar este tipo de mensajes de redirección, podría modificar las tablas de enrutamiento a voluntad, pudiendo conseguir que todo su tráfico saliente se enrutara a otra máquina controlada por el atacante. Por lo tanto, y a pesar de las ventajas que supone en sí mismo este tipo de redirección, podría ser interesante ignorarla a fin de evitar una posible vía de ataque.
- f) **Deshabilitar la redirección ip.** La redirección IP se refiere a la capacidad que dispone un sistema de varias interfaces de conexión a distintas subredes, de recibir por una los paquetes destinados a cualquier otra. Este comportamiento es correcto en equipos o dispositivos que actúen como routers o cortafuegos, pero no en un equipo ordinario.
- g) **Ignorar los mensajes de error mal formados.** El protocolo ICMP, dispone de mensajes de error para notificar alguna situación anormal en la red. Sin embargo, esta característica se puede utilizar para atacar a los equipos, ya que se les puede inducir a pensar que la red está en un estado distinto al real. En muchas ocasiones, un mensaje de error mal formado indica que se está cometiendo un ataque.
- h) **Protección frente a ip spoofing.** Esta protección impide que el sistema sea utilizado para el envío de paquetes IP cuya dirección de destino sea inválida, lo que puede ser indicativo de que se está cometiendo un ataque con el fin de saturar los recursos de comunicación suplantando una dirección ip válida.
- i) **Logging de actividades sospechosas.** Mediante esta protección se consigue que el sistema anote en sus registros (logs) la ocurrencia de paquetes con dirección IP inválida (conocido como ataque "IP spoofing"), paquetes que indiquen cambios de rutas (por ejemplo, por haberse activado en el origen el "source routing") y la ocurrencia de otros paquetes anormales o excepcionales.
- j) **Protección frente a buffer overflow.** ASLR (Address Space Layout Randomization) es una técnica de seguridad implicada en la protección de los ataques de desbordamiento de la pila.
- k) **Bloqueo IPv6.** La mayoría de las distribuciones *Linux* es que *IPv6* venga configurado por defecto. Sin embargo, no son muchos los usuarios que, aun teniendo esta configuración, hagan uso de alguna aplicación o servicio sobre *IPv6*, al menos conscientemente. Sus equipos pueden cambiar a trabajar en modo *IPv6* en cualquier momento, y a veces en el menos inesperado, haciendo que sea víctima de algún ataque de red que afecte a *IPv6*, como son el de envenenamiento de vecinos - algo similar al ARP-Spoofing pero con paquetes *ICMPv6* spoofeados que realizan aplicaciones como *insane6*, *parasite6* o *Scapy*, a un ataque de Rogue *DHCPv6* que configure un servicio de DNS o una puerta de enlace maliciosa o a un ataque de Man in the middle por medio del protocolo *SLAAC*.

- l) **Activar la protección “DEFRAGGING”**. Esta protección se debería aplicar en equipos que actúen como Gateway y que se dediquen a enmascarar tráfico interno (conocido como “IP-masquerading”). A través de este parámetro se le permitiría dividir los paquetes que lo atraviesan, a fin de evitar un consumo excesivo de recursos. Añadiendo la siguiente línea:

i. `net.ipv4.always_defrag = 1`

6.2.2.4 CONFIGURACIÓN DE TCP-WRAPPERS

Para restringir un servicio a pesar de que éste esté abierto, de forma que sólo las máquinas que deban usarlo puedan acceder se emplearán los TCP-wrapper. CentOS Linux ya tiene instalado el TCP-wrapper, pero está sin configurar y permite el acceso a todos los usuarios. Su configuración es muy sencilla, consta de dos archivos que están en el directorio **/etc: hosts.allow** y **hosts.deny**.

- a) Dentro del archivo **/etc/hosts.allow** se indicará los equipos que tienen permiso para acceder a nuestros servicios.
- b) Dentro del archivo **/etc/hosts.deny** se indicará los equipos que no tienen permiso para acceder a nuestros servicios.

La sintaxis es la siguiente: **<demonio>:<equipo o grupo de equipos>**. En un principio, se denegará el acceso a todos los equipos, para después otorgárselo a los que sea necesario. Para ello en el **/etc/hosts.deny** se indicará **'ALL : ALL'**, lo que deniega todo lo que no se permita explícitamente en el fichero **hosts.allow**.

A continuación, en el archivo **/etc/hosts.allow** se otorgarán permiso a todos aquellos equipos que lo requieran. Posteriormente se explicará más detalladamente y con ejemplos ilustrativos la manera más segura de configurar los ficheros anteriores.

6.2.3 LIMITACIÓN DE RECURSOS DE USUARIO

Con el fin de limitar los recursos que puede utilizar un usuario en el sistema y las acciones que los programas que ejecuta pueden llevar a cabo, es necesario aplicar ciertas configuraciones.

6.2.3.1 BLOQUEAR LA GENERACIÓN DE VOLCADOS DE MEMORIA

Para prevenir la creación de volcados de memoria (core dumps) de programas que abortan su ejecución (ya que esta información puede revelar datos confidenciales, y únicamente tiene valor para desarrolladores), se limitará **soft - core** y **hard - core** a **0**.

6.2.3.2 LÍMITE DE LOS RECURSOS DISPONIBLES PARA CADA USUARIO

Se debe limitar la cantidad de **procesos** que un usuario puede tener simultáneamente en el sistema. Del mismo modo se debe limitar la cantidad de **memoria** residente de la que hace uso un usuario. Además de los límites anteriores, se debe limitar las **conexiones** simultáneas al sistema que cada usuario puede realizar. Todos estos parámetros se configuran en el siguiente fichero de configuración **/etc/security/limits.conf**.

Por último, hay que limitar la cantidad de hilos concurrentes que se ejecutan en el sistema, evitando que cualquier programa que se ejecute aumente hasta provocar una denegación de servicio, esta configuración se realizará en **/etc/sysctl.conf**.

6.2.3.3 BLOQUEAR EL USO DE ATAJO CRÍTICOS

Para prevenir reinicios del sistema no deseados al utilizar la combinación de teclas **Ctrl-Alt-Supr**, se debe deshabilitar en los sistemas Core. Para distribuciones de GNU/Linux que utilizan Systemd (CentOS 7 Linux) como sistema de gestión de tareas y servicios durante el inicio, el comportamiento de teclas Ctrl-Alt-Supr se determina por un enlace simbólico denominado **/usr/lib/systemd/system/ctrl-alt-del.target** que apunta hacia el archivo `reboot.target`, localizado dentro del mismo directorio.

6.2.3.4 ESTABLECIMIENTO DE CUOTAS DE DISCO

El uso de cuotas de disco permite limitar la cantidad de espacio en disco que utiliza un usuario. La diferencia respecto a los sistemas de archivos extendidos (extended file system o ext) es que XFS requiere habilitar las cuotas a través del parámetro de kernel "rootflags" en tiempo de arranque (boot). Se debe entonces añadir el parámetro de kernel en la configuración de grub. La variable que contiene los parámetros es "GRUB_CMDLINE_LINUX".

Una vez activada la característica, se debe de asignar parámetros de cuotas a la partición que se requiera limitar por usuarios, comúnmente se suele asignar cuotas a la partición **/home**, puesto que en ella suelen estar los archivos personales de cada usuario.

6.2.4 LIMITE DE ACCESO AL SISTEMA

Esta guía se basa en la asunción de que no puede haber ningún sistema perfecto, libre de bugs o errores. Dado que cada entorno cuenta con millones de líneas de código e interacciones software/hardware. Un error crítico en cualquiera de estas interacciones puede ser suficiente para que un software malicioso pueda tomar el control de un sistema.

Por esto mismo se debe limitar al máximo los accesos al sistema, así como los permisos, evitando en la medida de lo posible los automatismos y las posibles formas de intrusión. Reduciendo las consecuencias e incluso previniendo los problemas legales.

6.2.4.1 CONTROL DE INFORMACIÓN DIVULGADA POR EL SISTEMA

Ciertos ficheros del sistema contienen información que se muestra a los usuarios que intentan acceder al sistema. Esta información deberá revisarse para comprobar que no se está divulgando información confidencial. Así mismo, se sustituirá esa información por avisos legales previniendo las consecuencias del acceso no autorizado al sistema.

6.2.4.2 CONFIGURACIÓN SEGURA DE SSH

Para evitar el uso de versiones inseguras del protocolo SSH se comprobará que la configuración del cliente SSH fuerza la versión 2 del protocolo modificando en el fichero de configuración `/etc/ssh/ssh_config` la línea correspondiente al protocolo. Por parte del servidor de SSH se requerirán más directrices que se configurarán en el fichero de configuración `/etc/ssh/sshd_config`:

- a) Se forzará el uso de la versión 2 del protocolo.
- b) Se denegará el uso de aplicaciones gráficas de modo remoto por medio de X11
- c) Se configurarán los usuarios no administradores como acceso denegado.
- d) Se limitará el tiempo total para hacer login en 120 segundos.
- e) Se establecerá el tiempo mínimo de inactividad antes de la desconexión.
- f) SSH puede emular el comportamiento del comando `rsh` obsoleto al permitir a los usuarios habilitar el acceso inseguro a sus cuentas a través de archivos `.rhosts`. por lo que se procederá a eliminar este comportamiento.
- g) La autenticación criptográfica basada en host de SSH es más segura que la autenticación `.rhosts`. Sin embargo, no se recomienda que los hosts confíen unilateralmente entre sí, incluso dentro de una organización. Por lo que se procederá a eliminar esta característica.
- h) Se denegarán los inicios de sesión root por medio de SSH.
- i) Se denegarán los accesos por medio de usuarios sin contraseña.
- j) Se configurará correctamente un banner que disuada a los posibles atacantes.
- k) Se garantizará que los usuarios no puedan usar variables de entorno al demonio SSH.
- l) Se configurará el uso únicamente del protocolo SSH con los algoritmos de cifrado permitidos.

6.2.4.3 MÓDULOS PAM DE AUTENTICACIÓN

Los administradores de sistemas de una organización deben decidir cuánto acceso administrativo se les otorga a los usuarios dentro de la organización a sus máquinas. A través de un módulo PAM llamado **pam_console.so**, se permiten algunas actividades normalmente reservadas para superusuarios, tales como el reinicio o el montaje de medios removibles, al primer usuario que se conecte en la consola física. Sin embargo, otras tareas importantes de administración de sistemas, tales como la modificación de las configuraciones de la red, configurar un nuevo ratón o montar dispositivos de red, son imposibles sin privilegios administrativos. En consecuencia, los administradores deben decidir cuánto acceso administrativo deberían recibir los usuarios en su sistema.

En el siguiente apartado se definen las acciones recomendadas para el modulo **pam_faillock.so**:

- a) Se contabilizarán los intentos fallidos de acceso o cambio de privilegios mediante su.
- b) Se bloquearán aquellas cuentas que superen 5 intentos fallidos.
- c) Para evitar que la cuenta root se bloquee intencionadamente se fijará manualmente un máximo de intentos fallidos.
- d) Se recordarán las 7 últimas contraseñas utilizadas por cada usuario y no permitirá su repetición.
- e) Se limitará el acceso de usuarios wheel a cuentas administrativas

6.2.4.4 LÍMITES DE INTENTO DE ACCESO AL SISTEMA

En este apartado se configurarán limitaciones al sistema mediante el componente shadow-utils, evitando ataques por fuerza bruta y logrando tener un mayor control sobre los intentos de acceso al mismo.

Hay que tener en cuenta que los parámetros que se configurarán en el archivo de configuración **/etc/login.defs** controlan el comportamiento de las herramientas del componente **shadow-utils**. Ninguna de estas herramientas utiliza el mecanismo PAM, y las utilidades que usan PAM (como el comando **passwd**) deben configurarse en lugar correspondiente.

Se procederá a seguir las siguientes recomendaciones:

- a) Número máximo de intentos de acceso fallidos conste de 3 intentos.
- b) El tiempo máximo permitido para acceder al sistema sea de 60 segundos.
- c) Evitar que el sistema indique cuando el usuario es desconocido para el mismo.
- d) El tiempo de retardo tras un intento fallido será de 10 segundos.
- e) Se registrarán los intentos fallidos de acceso al sistema.

6.2.4.5 LÍMITE DE SERVICIOS DEL SISTEMA

Como se comentó en otras partes de la guía se necesita minimizar la superficie de ataque, eliminando elementos innecesarios. Por ello no se deben mantener servicios activos que no son necesarios para el correcto funcionamiento del sistema.

En las distribuciones de Linux RHEL 7 y CentOS 7, la forma de controlar los servicios del sistema cambia con respecto a sus antecesoras. Se pasa del uso del comando “**service**” y del control de servicios a través de “**/etc/init.d**” a la gestión a través del **service manager systemctl**.

Se pueden listar fácilmente todos los servicios del sistema que corren al inicio mediante el comando **systemctl list-unit-files**. Procediendo a deshabilitar los que no sean necesarios.

Es posible usar el asistente **ntsysv** que muestra de manera más gráfica una lista de servicios disponibles los cuales se pueden seleccionar y definir para que arranquen automáticamente junto con el sistema.



La versión ntsysv 1.7.4 de Red Hat es la versión que viene por defecto en CentOS 7

6.2.5 ELEMENTOS INNECESARIOS DEL SISTEMA

En este punto es necesario tratar siempre de deshabilitar todos aquellos elementos del sistema que no sean necesarios, minimizando la superficie de posibles ataques al mismo.

6.2.5.1 PAQUETES INNECESARIOS

Una de las características del software libre es su carácter colaborativo. De esta manera existen cientos de miles de librerías disponibles, que permiten a los desarrolladores crear una aplicación sin tener que empezar de cero. Disponiendo de componentes de diferentes tamaños con un objetivo o funcionalidad específica y que permiten hacer la aplicación más robusta.

De esta característica se nutren las distribuciones Linux. Para que esas aplicaciones se ejecuten correctamente, se necesita que estén instalados el resto de paquetes. De esta forma, cuando se instala una aplicación, también se instalan aquellos paquetes necesarios para su funcionamiento.

Estos paquetes necesarios son los que se conocen como dependencias. Sin embargo, hay que tener en cuenta el momento de en la desinstalación de una aplicación, puesto que al desinstalar el paquete padre (aplicación principal) no siempre se desinstalan las dependencias. Al contrario, esas dependencias quedan instaladas en el equipo ocupando un espacio innecesario. Estos paquetes son los que se conoce como **paquetes huérfanos**.

En este punto se hará hincapié en eliminar todos aquellos paquetes que se encuentren por defecto en la instalación propia de CentOS Linux o sean innecesarios para el correcto funcionamiento del sistema. Así mismo se procederá con sus correspondientes dependencias.

6.2.5.2 USUARIOS INNECESARIOS

Como se ha comentado anteriormente, por defecto el sistema operativo, crea configuraciones para facilitar el uso del mismo, una de esas configuraciones, son los usuarios predefinidos como ftp, games, etc. Estos usuarios tienen permisos y configuraciones para ciertas partes del sistema operativo. El tener usuarios predefinidos en el S.O puede ser motivo de posibles brechas de seguridad.

Por esto, los usuarios de un sistema operativo tienen que ser los mínimos necesarios e indispensables, eliminando los que no sean necesarios y restringiendo ciertos permisos a los que por necesidad deban mantenerse.

6.2.6 PERMISOS Y VARIABLES DE ENTORNO

Las variables de entorno forman un conjunto de valores dinámicos que normalmente afectan al comportamiento de los procesos en un sistema. Las variables de entorno contienen información a la que se accede a través del nombre de la variable (al igual que ocurre en los lenguajes de programación).

6.2.6.1 FICHEROS DE CONFIGURACIÓN

Los ficheros **/etc/profile** y **/etc/bashrc** contienen las variables de entorno generales para todos los usuarios del sistema. Aunque su revisión está recomendada, hay que prestar especial atención a los siguientes puntos:

- a) **/etc/profile**:
 - i. En el PATH no debe figurar el directorio actual (**.**). Para validar que esto también se cumple en el caso de root, se comprueba la salida del comando “echo \$PATH”.
 - ii. Se restringe el tiempo máximo de inactividad en el sistema estableciendo el valor 600 para la variable TMOU
 - iii. Se restringe el tamaño del historial del intérprete de comandos al valor 1000 para los usuarios con la variable HISTSIZE.
- b) **/etc/bashrc**:
 - i. Se comprueba que la máscara por defecto de los usuarios es restrictiva comprobando que la directiva **umask** tiene el valor **027**

Nota: Otros ficheros de entorno que puedan existir en los directorios de los usuarios deberán ser revisados para evaluar su potencial peligrosidad. Por ejemplo, los ficheros **.netrc** deberán ser eliminados, ya que suponen un riesgo para el sistema.

6.2.6.2 DIRECTORIO DE USUARIOS

Se comprobará que los directorios **/home** de los usuarios no permiten a otros usuarios acceder ni modificar su contenido. Para ello será necesario que estos directorios cuenten con permisos **740** o más restrictivos.

6.2.6.3 PERMISOS EN FICHEROS Y DIRECTORIOS IMPORTANTES

Ciertos ficheros y directorios contienen información de carácter crítico, por lo que sus permisos deben ser revisados cuidadosamente para evitar problemas. Los ficheros más importantes son **/etc/passwd**, **/etc/group** y **/etc/shadow**. Por ello, se deben de tomar ciertas medidas para evitar el acceso a la lectura o la modificación de los mismos por personal no autorizado.

El propietario de los tres debe ser **root**, con grupo **root**; los permisos de los dos primeros deben permitir la lectura por parte de todos los usuarios del sistema y la modificación únicamente por root, mientras que el fichero de contraseñas shadow únicamente debe ser leído por root.

En cuanto a los directorios, todos aquellos en los que los usuarios del sistema tengan permisos de escritura deberán proteger sus contenidos utilizando el “**sticky bit**”, que previene que usuarios del sistema borren contenidos creados por otros usuarios.

También será necesario identificar ficheros cuyos permisos puedan representar un riesgo para el sistema. En especial será necesario identificar aquellos ficheros que puedan ser modificados por todos los usuarios, independientemente de los permisos que posean. A demás de aquellos ficheros que tengan activado el bit de **SUID** o de **SGID**.

6.2.7 KERNEL

El sistema de Linux está conformado por dos partes importantes, la primera es el Kernel y la segunda son los programas y herramientas propios de cada distribución. El Kernel es la parte del sistema que funciona a más bajo nivel y es el encargado de administrar la comunicación con el hardware, correr los programas del usuario y mantiene la seguridad e integridad de todo el sistema.

CentOS 7 se distribuye con la versión de kernel 3.10, la cual proporciona una cantidad de nuevas funcionalidades, de las cuales se listan las más importantes a continuación:

- a) **Soporte para grandes tamaños de Crashkernel.** CentOS 7 soporta el mecanismo de volcado en sistemas con memoria grande (hasta de 3TB).
- b) **Crashkernel con más de 1 CPU.** CentOS 7 permite el arranque de Crashkernel con más de una CPU. Esta función se soporta como muestra previa de tecnología.
- c) **Compresión de memoria swap.** CentOS 7 introduce la nueva funcionalidad, compresión de memoria swap. La compresión de memoria swap se realiza mediante zswap, un segundo plano delgado para frontswap. El uso de tecnología de compresión de memoria swap garantiza una reducción de E/S significativa y ganancia en rendimiento.
- d) **Programación de NUMA-Aware y asignación de memoria.** El kernel reasigna automáticamente procesos y memoria entre nodos NUMA en el mismo sistema, para mejorar rendimiento en sistemas con acceso de memoria no uniforme (NUMA).
- e) **Virtualización APIC.** La Virtualización de registros de controlador de interruptor programable avanzada (APIC) se apoya en el uso de funcionalidades de capacidades de hardware de nuevos procesadores para mejorar el manejo de interrupciones de monitor de máquina virtual (VMM).

- f) **VMCP construido en el Kernel.** El módulo de kernel vmcp está construido en el kernel. Esto garantiza que el nodo de dispositivo vmcp está siempre presente, y los usuarios puedan enviar comandos de programa de control de hipervisor IBM z/VM sin tener que cargar primero el módulo de kernel vmcp.
- g) **Mecanismo de reporte de errores de hardware.** Actualmente, el mecanismo de reporte de errores de hardware en Linux puede ser problemático, principalmente debido a las varias herramientas (mcelog y EDAC) que recolectan errores de diversas fuentes con diferentes métodos y herramientas (tales como mcelog, edac-utils, y syslog) para reportar eventos de errores.

Los problemas de reporte de errores de hardware pueden dividirse en dos partes:

- i. Los mecanismos de recolección de datos de diferentes errores que recolectan varios datos y algunas veces duplicados.
- ii. y herramientas que reportan estos datos en diferentes sitios con diferentes marcas de tiempo, lo cual dificulta la correlación de los eventos.

La meta del nuevo mecanismo de reporte de errores de hardware o **HERM**, es unificar la recolección de datos de errores de varias fuentes y reportar los eventos de errores al espacio de usuario en una línea de tiempo secuencial y sitio individual. HERM introduce el nuevo demonio de espacio de usuario, rasdaemon, el cual recoge y maneja todos los eventos de errores de Confiabilidad, disponibilidad y servicio (RAS) que surgen de la infraestructura de rastreo de kernel y los registra. HERM también provee las herramientas para resolver errores y es capaz de detectar diferentes tipos de errores tales como errores de ráfagas y de dispersión.

- h) **Soporte total para DynTick.** El nohz_full como parámetro de arranque extiende la funcionalidad de kernel tickless cuando el tick (ciclo de reloj) puede ser detenido.
- i) **La puesta en lista negra de los módulos de kernel.** La utilidad modprobe permite a los usuarios la puesta en lista negra de los módulos de kernel en el momento de instalación. para desactivar globalmente la carga automática de un módulo.
- j) **Parche de kernel dinámico.** Kpatch es un parche de kernel dinámico. Permite a los usuarios manejar una colección de parches de kernel binario que se pueden usar de forma dinámica para parchear el kernel sin necesitar de reiniciar.
- k) **Controlador Emulex ocrdma.** El controlador Emulex ocrdma proporciona capacidades de acceso directo de memoria remota (RDMA) en adaptadores Emulex específicos.
- l) **Destino dm-era.** Se introduce el mapeador de dispositivo dm-era mantiene el rastro de los bloques que fueron escritos dentro de un determinado tiempo de usuario denominado "era". Cada instancia de destino de "era" la mantiene como un contador de 32 bits que aumenta de forma lineal. Este destino permite que software de respaldo pueda rastrear bloques que hayan cambiado desde la última copia de respaldo. También permite la invalidación parcial del contenido de la memoria cache para restaurar coherencia tras volver a la instantánea de distribuidor. Se espera principalmente que el destino dm-era sea emparejado con el destino dm-cache.

6.3 REDES Y FIREWALL

6.3.1 RED

CentOS 7 Linux es una versión que plantea algunos cambios incluye nuevos comandos y cambia algunas formas de administrar el sistema. En CentOS 7 Linux al arrancar el sistema, las interfaces de red estarán desactivadas. Este es el comportamiento predeterminado del sistema y es por ello que tienes que configurar y activar las interfaces de red manualmente.

- a) **Coordinación de red.** La coordinación de red ha sido introducida como una alternativa para vincular una reunión de enlaces. Está diseñada para facilitar el mantenimiento, depuración y extensión. Ofrece al usuario mejoras en rendimiento y flexibilidad y debe evaluarse para todas las nuevas instalaciones.
- b) **NetworkManager.** Se ha realizado una serie de mejoras a NetworkManager para hacerlo más útil en las aplicaciones de servidores. En particular, NetworkManager ya no supervisa los cambios de archivos de configuración de forma predeterminada, tales como los realizados por editores o herramientas de implementación. Esto permite a los administradores estar atentos de cambios externos mediante el comando `nmcli connection reload`.

Los cambios a través de D-Bus API de NetworkManager con la herramienta de línea de comandos de NetworkManager, `nmcli`, aún se efectúan inmediatamente.

La herramienta `nmcli` se introduce para permitir a los usuarios y scripts interactuar con NetworkManager.

- c) **Nuevas funcionalidades en Libreswan.** La implementación de Libreswan de VPN IPsec, ha sido actualizada a la versión 3.12, la cual añade varias funcionalidades y mejoras:
 - i. Se agregaron nuevas cifras.
 - ii. El soporte IKEv2 ha sido mejorado.
 - iii. Se agregó soporte de cadena de certificados intermediarios en IKEv1 e IKEv2.
 - iv. Se mejoró el manejo de conexión.
 - v. Se mejoró la interoperabilidad con sistemas OpenBSD, Cisco, y Android.
 - vi. Se mejoró el soporte para `systemd`.
 - vii. Se agregó soporte para CERTREQ en hash y estadísticas de tráfico.
- d) **systemd-hostnamed.** Con esta actualización, NetworkManager utiliza el servicio `systemd-hostnamed` para leer y escribir el nombre de host estático, que se almacena en el archivo `/etc/hostname`. Debido a este cambio, las modificaciones manuales hechas al archivo `/etc/hostname` ya no son recogidas automáticamente por NetworkManager; los usuarios deben cambiar el nombre de host del sistema a través de la utilidad `hostnamectl`. Además, el uso de la variable `HOSTNAME` en el archivo `/etc/sysconfig/network` ahora está en desuso.

- e) **Paquete chrony.** El grupo de paquetes de herramientas chrony está disponible para actualizar el reloj del sistema en sistemas que no se ajustan a la categoría de trabajo de red convencional, siempre encendido, de servidor dedicado. El grupo de paquetes chrony, debe considerarse para todos los sistemas que están frecuentemente suspendidos o desconectados de forma intermitente y reconectados a la red. Por ejemplo, los sistemas móviles y virtuales.
- f) **Firewalld.** Es un demonio dinámico, el cual proporciona Firewall administrado de forma dinámica con soporte para "zonas" de red que asignen un nivel de confianza a una red y sus conexiones e interfaces asociadas. Tiene soporte para parámetros de Firewall IPv4 e IPv6. Soporta puentes Ethernet y tiene una separación de tiempo de ejecución y opciones de configuración permanentes. También tiene una interfaz para servicios o aplicaciones para añadir directamente reglas de Firewall.
- g) **DNSSEC.** Es una serie de Extensiones de seguridad de nombre de dominio de sistema (DNSSEC) que permite a un cliente DNS autenticarse y verificar la integridad de respuestas de un servidor de nombre DNS, verificar su origen y determinar si se han interferido en tránsito.
- Soporte DNSSEC en Administración de identidades
 - Los servidores de Administración de identidades con el DNS integrado ahora soportan Extensiones de seguridad DNS (DNSSEC). Las zonas DNS alojadas en servidores de Administración de identidades pueden ser firmadas de forma automática con DNSSEC. Las llaves criptográficas se generan y rotan de forma automática.
 - Observe que los servidores de Administración de identidades con DNS integrado usan DNSSEC para validar preguntas DNS obtenidas desde otros servidores DNS. Esto podría afectar la disponibilidad de zonas DNS que no están configuradas según las prácticas de denominación descritas en Red Hat Enterprise Linux Networking Guide:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Host_Names.html#sec-Recommended_Naming_Practices

Nota: Se aconseja a los usuarios que decidan proteger sus zonas DNS con DNSSEC que consulten los siguientes documentos:

- DNSSEC Operational Practices, Version 2: <http://tools.ietf.org/html/rfc6781#section-2>
- Secure Domain Name System (DNS) Deployment Guide: <http://dx.doi.org/10.6028/NIST.SP.800-81-2>

- h) **OpenLMI.** Proporciona una infraestructura común para el manejo de sistemas de Linux. Permite a los usuarios configurar, administrar y monitorizar hardware, sistemas operativos y servicios de sistemas. OpenLMI tiene la finalidad de simplificar la tarea de configuración y administración de servidores de producción. Está diseñado para proporcionar una interfaz de administración común para varias versiones de Red-Hat/CentOS. Se construye por encima de las herramientas existentes, y proporciona una capa de abstracción que oculta mucha de su complejidad del sistema subyacente de los administradores de sistemas. OpenLMI consiste en un conjunto de agentes de administración de sistemas, instalado en un sistema administrado, el controlador OpenLMI, el cual administra los agentes y les proporciona una interfaz y aplicaciones de clientes o scripts que llaman a agentes de administración de sistemas a través del controlador OpenLMI.

OpenLMI permite a los usuarios:

- i. Configurar, administrar y monitorizar tanto servidores de producción en vacío como huéspedes virtuales;
- ii. Configurar, administrar y monitorizar sistemas locales y remotos;
- iii. Configurar, administrar y monitorizar almacenamiento y redes;
- iv. Llamar a funciones de administración de sistemas desde C/C++, Python, Java, o la interfaz de línea de comandos.
- v. El software es completamente funcional, sin embargo, algunas operaciones pueden consumir recursos excesivos.

Nota: Para obtener más información sobre comandos de referencia entre EXT4 y XFS, consulte la siguiente dirección URL. <http://docs.openlmi.org/en/latest/#>

- i) **Conexión de red confiable.** CentOS 7 introduce funcionalidad de conexión de red de confianza NAC (Control de Acceso a la Red). NAC se utiliza con soluciones de Control de acceso de red, tales como TLS, 802.1x, o IPSec para recoger información de sistema de punto final, tal como parámetros de configuración del sistema operativo, paquetes instalados, y otros, denominados como medidas de integridad. La conexión de red de confianza se utiliza para verificar estas medidas con el acceso de políticas antes de permitir el punto final para acceder a la red.

6.3.2 CONFIGURACIÓN DE FIREWALLD

Una de las medidas incluidas en los Sistemas Operativos para aumentar los niveles de seguridad y establecer un control sobre las conexiones entrantes y salientes del sistema es el firewall.

Es muy importante conocer todo lo que un Firewall ofrece a nivel de protección y en CentOS 7 Linux la solución incluida a nivel de Firewall es llamada FirewallD la cual ofrece las siguientes ventajas:

- a) Es un cortafuegos dinámico.
- b) Estable.
- c) Múltiples opciones de configuración.
- d) Soporta configuraciones Ipv4, Ipv6 y puentes de Ethernet.
- e) Se pueden definir diversas formas de configuración de FirewallD (continua y en ejecución).

En Firewalld existen diversos términos a los cuales es importante prestar atención ya que estarán de forma continua en la configuración del mismo:

- a) **Zona:** Una zona de red es aquella cuya función es definir el nivel de confianza que tendrá la conexión de red.
- b) **Drop:** Es el nivel de confianza más bajo, ya que todos los paquetes de entrada son rechazados de forma automática y solo habilita los paquetes salientes.
- c) **Block:** Este nivel de confianza es similar a Drop con la diferencia que los paquetes entrantes son rechazados con mensajes icmp-host-prohibited para IPv4 y icmp6-adm-prohibited para IPv6
- d) **Public:** Este nivel de confianza hace referencia a las redes públicas no confiables, solo acepta conexiones confiables.
- e) **External:** Este tipo de nivel es usando cuando se utiliza el Firewall como puerta de enlace y su enmascaramiento está habilitado por los routers.
- f) **DMZ:** Este nivel es usado en equipos situados en una zona DMZ (Desmilitarizada), es decir, tiene acceso público con restricción a la red interna. Solo acepta conexiones aceptadas.
- g) **Work:** Este nivel es usado en áreas de trabajo por lo cual la mayor parte de los equipos de la red tendrán acceso a ella.
- h) **Home:** Este tipo de nivel es usado en un entorno de hogar y son aceptadas la mayoría de equipos.
- i) **Internal:** Este tipo de nivel es usado en redes internas por lo que todos los equipos de la red serán aceptados.
- j) **Trusted:** Este es el nivel más alto y confía en todas las conexiones entrantes.

En Firewalld es posible crear dos tipos de reglas:

- a) **Permanentes:** Si se desea que una regla sea permanente se utiliza el parámetro `--permanent`, de esta manera la regla se mantendrá después de apagar el equipo.
- b) **Inmediatas:** Cuando se edita una regla mediante este modo, el cambio se verá de manera automática, pero al siguiente inicio de sesión esta regla será revertida.

6.4 SISTEMA

6.4.1 ACTUALIZACIÓN DEL SISTEMA

Las actualizaciones del sistema son mejoras que se realizan al núcleo del sistema operativo y a diversas aplicaciones que se ejecutan en este sistema, con la finalidad de mantener su funcionamiento óptimo y reparar en la medida de lo posible fallos, errores y vulnerabilidades que se puedan presentar.

Todo sistema debe de estar actualizado, pero dependiendo de la criticidad del sistema que se deba actualizar, es posible que se necesite aislar del resto de sistemas o aislar su comunicación con redes externas e internet. Por este motivo ciertos sistemas necesitarán una actualización fuera de línea.

En esta guía se diferenciará la actualización por parte del fabricante de manera “online” y mediante parches y actualizaciones de manera “offline”.

6.4.1.1 ONLINE

CentOS Linux es un sistema operativo Linux empresarial impulsado por la comunidad. Se deriva directamente del sistema operativo Red Hat Enterprise Linux. CentOS utiliza el gestor de paquetes de software para instalar, administrar y eliminar paquetes de software. Los paquetes de software Yum están en un repositorio en línea. Puedes utilizar el comando "**Yum**" para listar las actualizaciones disponibles para el software instalado, actualizar el sistema operativo y todo el software instalado, y actualizar un solo paquete.

6.4.1.2 OFFLINE

CentOS Linux no posee un soporte por parte del fabricante al igual que RED-HAT, por ello, se recomienda añadir las actualizaciones en formato CDROM o .ISO, pudiendo grabar físicamente el CDROM o añadiendo las actualizaciones en dispositivos extraíbles configurando un repositorio para tal efecto.

6.4.2 SISTEMA Y SERVICIOS

Linux ofrece multitud de servicios, estos pueden iniciar o arrancar junto con la carga del sistema o pueden arrancar a petición del usuario, lo que para muchos servicios será lo recomendable. Parte esencial de la administración de sistemas Linux es continuamente trabajar con los servicios que este proporciona.

SYSTEMD. Es un gestor de sistema y servicios para Linux, el cual reemplaza SysV utilizado en lanzamientos anteriores de CentOS Linux. systemd es compatible con SysV y scripts init de Linux Standard Base.

Systemd ofrece, entre otras, las siguientes capacidades:

- a) Capacidades de paralelización agresiva
- b) Uso de activación de socket y D-Bus para servicios de inicio.
- c) Inicios On-demand de demonios.
- d) Manejo de grupos de control
- e) Creación de instantáneas de estado del sistema y restauración de estado del sistema.

6.4.3 ADMINISTRACIÓN DE RECURSOS

CentOS Linux 7 introduce los grupos de control, un concepto para procesos de organización en un árbol de grupos nominados para propósitos de administración de recursos. Los grupos de control proporcionan una forma de agrupar por jerarquías y procesos de etiquetas y una forma de aplicar límites de recursos a estos grupos. En CentOS Linux 7, los grupos de control se manejan de forma exclusiva a través de **systemd**.

Los grupos de control, abreviados como **cgroups**, son una función de kernel de Linux que le permite asignar recursos, como tiempo de CPU, memoria del sistema, ancho de banda de red o combinaciones de estos recursos, entre grupos ordenados jerárquicamente de procesos que se ejecutan en un sistema. Mediante el uso de cgroups, los administradores del sistema obtienen un control detallado sobre la asignación, priorización, denegación, administración y supervisión de los recursos del sistema.

Los recursos de hardware se pueden dividir inteligentemente entre aplicaciones y usuarios, aumentando la eficiencia general. Cgroups se configuran en archivos de unidades de systemd y se manejan con las herramientas de la interfaz de línea de comandos(CLI).

CentOS 7 traslada la configuración de administración de recursos del nivel de proceso al nivel de aplicación vinculando el sistema de jerarquías de cgroup con el árbol de unidades systemd. Por lo tanto, puede administrar los recursos del sistema con los comandos **systemctl**, o modificando los archivos de la unidad **systemd**.

En versiones anteriores de CentOS Linux, los administradores del sistema creaban jerarquías de cgroup personalizadas con el uso del comando **cgconfig** del paquete **libcgroup**. Este paquete ahora está en desuso, y no se recomienda su uso ya que puede crear conflictos con la jerarquía predeterminada de cgroup. Sin embargo, libcgroup todavía está disponible para cubrir ciertos casos específicos, donde systemd aún no fuera aplicable.

Las herramientas mencionadas proporcionan una interfaz de alto nivel para interactuar con los controladores cgroup (también conocidos como subsistemas) en el kernel de Linux. Los controladores principales de cgroup para la gestión de recursos son cpu, memory y blkio.

Un controlador de recursos, también llamado subsistema cgroup, representa un único recurso, como el tiempo de CPU o la memoria. El kernel de Linux proporciona una gama de controladores de recursos, que systemd monta automáticamente. la lista de controladores de recursos actualmente se encuentra en /proc/cgroups, otra opción es usar la herramienta de supervisión **lssubsys**. En CentOS 7, systemd monta los siguientes controladores por defecto:

- a) **blkio**: establece límites en el acceso de entrada / salida hacia y desde dispositivos de bloque.
- b) **CPU**: utiliza el programador de la CPU para proporcionar acceso a las tareas de cgroup a la CPU. Se monta junto con el controlador cpuacct en el mismo soporte.
- c) **cpuacct**: crea informes automáticos sobre los recursos de la CPU utilizados por las tareas en un cgroup. Se monta junto con el controlador de la CPU en el mismo soporte.
- d) **cpuset**: asigna CPU individuales (en un sistema multinúcleo) y nodos de memoria a tareas en un cgroup.
- e) **devices**: permite o deniega el acceso a dispositivos para tareas en un cgroup.
- f) **freezer**: suspende o reanuda tareas en un grupo cg.
- g) **memory**: establece límites en el uso de memoria por tareas en un grupo de cg y genera informes automáticos sobre los recursos de memoria utilizados por esas tareas.
- h) **net_cls**: etiqueta paquetes de red con un identificador de clase (classid) que permite que el controlador de tráfico de Linux (el comando tc) identifique los paquetes que se originan de una tarea particular de cgroup. Un subsistema de net_cls, net_filter (iptables) también puede usar esta etiqueta para realizar acciones en dichos paquetes. Net_filter etiqueta los sockets de red con un identificador de firewall (fwid) que permite que el firewall de Linux (el comando iptables) identifique los paquetes (skb → sk) que se originan de una tarea particular de cgroup.
- i) **perf_event**: habilita la supervisión de cgroups con la herramienta perf.
- j) **hugetlb**: permite utilizar páginas de memoria virtual de gran tamaño y aplicar límites de recursos en estas páginas.

6.4.4 ARQUITECTURA

A partir de la versión 7.0 de CentOS, no distribuye una versión específica de 32bits.

Se muestra la siguiente tabla comparativa con las diferentes versiones de CentOS:

	CentOS Linux 5	CentOS Linux 6	CentOS Linux 7
CPU lógicas máximas			
x86_64	160/255	160/4096	160/5120
POWER	128/128	128	En evaluación
System z	101 (zEC12)	101 (zEC12)	En evaluación
Memoria máxima			
x86_64	1 TB	3 TB soportados/64 TB	3 TB soportados/64 TB
POWER	512 GB mínimo/1 TB recomendado	2 TB	2 TB
System z	3 TB (z196)	3 TB (z196)	3 TB (z196)
Mínimo requerido			
x86_64	512 MB mínimo/1 GB por CPU lógica recomendada	1 GB mínimo/1 GB por CPU lógica recomendada	1 GB mínimo/1 GB por CPU lógica recomendada
POWER	1 GB/2 GB recomendado	2 GB/2 GB por instalación	2 GB/2 GB por instalación
System z	512 MB	512 MB	1 GB ¹
Límites de sistemas de archivos y almacenamiento			
Tamaño máximo de archivo: XFS	16 TB	16 TB	16 TB
Tamaño máximo de archivo: ext4	16 TB	16 TB	50 TB
Tamaño máximo de archivo: Btrfs	N/A	En evaluación	En evaluación
Tamaño máximo de sistema de archivos: XFS	100 TB ²	100 TB	500 TB
Tamaño máximo de sistema de archivos: ext4	16 TB	16 TB	50 TB
Tamaño máximo de sistema de archivos: Btrfs	N/A	En evaluación	50 TB
Tamaño máximo de LUN de arranque	2 TB	16 TB ³	50 TB
Tamaño máximo de dirección por proceso: x86_64	2 TB	128 TB	128 TB

¹ Se recomienda mayor de 1 GB para instalación en IBM System z.

² La versión de CentOS 5.5 o mayor soporta un tamaño de sistema de archivos XFS hasta de 100 TB.

³ Observe que se requiere soporte UEFI y GPT para soportar LUN de arranque mayor que 2 TB.

6.4.5 ALMACENAMIENTO

En Linux, casi todo está representado por un archivo. Esto incluye hardware como unidades de almacenamiento, que se representan en el sistema como archivos en el directorio **/dev**. Normalmente, los archivos que representan dispositivos de almacenamiento comienzan con **sd** o **hd** seguido de una letra. Por ejemplo, la primera unidad en un servidor suele ser algo así como **/dev/sda**.

Las particiones en estas unidades también tienen archivos dentro de **/dev**, representados al agregar el número de partición al final del nombre de la unidad. Por ejemplo, la primera partición en el disco del ejemplo anterior sería **/dev/sda1**.

Mientras que los archivos del dispositivo **/dev/sd*** y **/dev/hd*** representan la forma tradicional de referirse a unidades y particiones, existe una desventaja significativa al usar estos valores por sí mismos. El kernel de Linux decide qué dispositivo obtiene qué nombre en cada arranque, por lo que esto puede generar escenarios confusos en los que los dispositivos cambian los nodos del dispositivo.

Para evitar este problema, el directorio **/dev/disk** contiene subdirectorios correspondientes con formas diferentes y más persistentes para identificar discos y particiones en el sistema. Estos contienen enlaces simbólicos que se crean en el inicio de los archivos correctos **/dev/[sh]da***. Los enlaces se nombran de acuerdo con el rasgo de identificación del directorio (por ejemplo, mediante la etiqueta de partición en el directorio **/dev/disk/by-partlabel**). Estos enlaces siempre apuntan a los dispositivos correctos, por lo que pueden usarse como identificadores estáticos para espacios de almacenamiento.

Como novedades implementadas en la versión de CentOS 7 Linux y posteriores se enumeran las más importantes:

- a) **Rápidos dispositivos de bloques que almacenan dispositivos de bloques más lentos.** La disponibilidad de tener dispositivos de bloques rápidos que actúen como una memoria cache para dispositivos de bloques más lentos, se introduce como muestra previa de tecnología en CentOS 7.0. Esta funcionalidad permite al dispositivo SSD de PCIe actuar como memoria cache para almacenamiento directo vinculado (DAS) o para red de almacenamiento estándar (SAN), el cual mejora el rendimiento del sistema de archivos.
- b) **LVM cache.** Esta funcionalidad permite a los usuarios crear volúmenes lógicos con un dispositivo pequeño y rápido como una cache a dispositivos más grandes y lentos. El redimensionado LVM (Logical Volume Manager) de aprovisionamiento fino, permite que el disco preparado para ser redimensionado mediante LVM no utilice el total de espacio designado para la partición como ocurría en el aprovisionamiento grueso.
- c) **DIF/DIX.** Se introduce soporte para DIF/DIX que es una adición al estándar de SCSI. DIF/DIX aumenta el tamaño de 512 bytes de bloque de disco utilizado comúnmente a 520 bytes, y adiciona el Campo de integridad de datos (DIF). El DIF almacena un valor de suma de verificación para el bloque de datos que es calculado por el Adaptador de bus de host (HBA) cuando ocurre una escritura. El dispositivo de almacenamiento confirma entonces la suma de verificación en recepción y guarda los datos y la suma de verificación. Igualmente, cuando se presenta una lectura, la suma de verificación puede ser revisada por el dispositivo de almacenamiento y por el HBA que recibe.

- d) **Soporte para NFS en paralelo.** El soporte de NFS paralelo (pNFS) es una parte del estándar NFS v4.1 que permite a los clientes acceder a dispositivos de almacenamiento de forma directa en paralelo. La arquitectura pNFS puede mejorar la escalabilidad y rendimiento de servidores NFS para varias cargas de trabajo comunes.
- e) **pNFS.** Define 3 protocolos o distribuciones de almacenamiento diferentes: archivos, objetos y bloques. El cliente de CentOS 7.0 soporta completamente las distribuciones de archivos, objetos y bloques.

Nota: Para obtener más información sobre pNFS, consulte la siguiente dirección URL.

<https://www.panasas.com/products/architecture/panfs-parallel-file-system/>

6.4.6 SISTEMA DE ARCHIVOS

Un sistema de archivos es el sistema que estructura los datos, controla cómo se escribe y recupera la información del disco subyacente. Sin un sistema de archivos, no podría usar el dispositivo de almacenamiento para ninguna operación relacionada con archivos.

El sistema de archivos para una instalación basada en Anaconda de CentOS 7.0 ahora es XFS, el cual reemplaza el Cuarto sistema de archivos extendido (ext4) utilizado como predeterminado en CentOS/Red Hat Enterprise Linux 6. El sistema de archivos ext4 y el sistema de archivos Btrfs (B-Tree) pueden utilizarse como alternativos para XFS.

XFS es un sistema de archivos escalable de alta disponibilidad, el cual fue diseñado originalmente en Silicon Graphics, Inc. Fue creado para soportar sistemas de archivos de hasta 16 Exabytes (aproximadamente 16 millones de terabytes), y estructuras de directorios que contienen decenas de millones de entradas. XFS soporta diario de metadatos, lo cual facilita recuperación de daños de una forma más rápida. Los sistemas de archivos XFS también se pueden desfragmentar y expandir cuando están montados y activos.

Tabla de comandos de referencia para ext4 y XFS:

Tarea	Ext4	XFS
Creación de un sistema de Archivos	mkfs.ext4	mkfs.xfs
Montaje de un sistema de Archivos	mount	mount
Cambiar el tamaño de un sistema de Archivos	resize2fs	xfs_growfs ⁴
Reparar un sistema de archivos	e2fsck	xfs_repair
Cambiar la etiqueta en un sistema de archivos	e2label	xfs_admin -L
Informes sobre el espacio en disco y el uso de archivos	quota	quota
Depuración de un sistema de archivos	debugfs	xfs_db
Guardar metadatos críticos del sistema de archivos en un archivo	e2image	xfs_metadump

Nota: Para obtener más información sobre comandos de referencia entre EXT4 y XFS, consulte la siguiente dirección URL.

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/appe-ext4-to-xfs-command-reference

⁴ El tamaño de los sistemas de archivos XFS no se puede reducir; el comando se usa solo para aumentar el tamaño.

Por otra parte, el sistema de archivos **Btrfs** es uno de los sistemas de archivos más nuevo que hay disponibles en Linux. La meta de Btrfs es implementar algunas características importantes que faltan en los sistemas de archivos en Linux, tales como pooling, snapshots y checksums, entre otras. Una de las motivaciones principales es proveer de soporte confiable para sistemas de archivos grandes, por lo cual puede ser de interés para cualquier organización que tenga muchos usuarios y/o que posea un almacenamiento grande.

La biblioteca **libhugetlbfs** ahora tiene soporte en la arquitectura IBM System z. La biblioteca permite explotación transparente de páginas grandes en programas C y C++. Los programas y aplicaciones de Middleware pueden aprovechar los beneficios de rendimiento o páginas grandes sin cambios o recompilaciones.

6.4.7 ADMINISTRACIÓN Y MANTENIMIENTO

Tanto la Administración como el mantenimiento de servidores o equipos Linux es una tarea que necesita una vigilancia constante para asegurar la estabilidad del sistema.

El mantenimiento de servidores debe realizarse desde el primer momento en que estos comienzan a funcionar. Y es que, aunque en un primer momento parezca que el mantenimiento no es una tarea demasiado relevante, es importante sentar las bases para el medio y largo plazo, cuando el tráfico sea más elevado y los recursos almacenados en el servidor sean mayores.

6.4.7.1 AUTOMATIZACIÓN DE TAREAS

En un sistema cualquier tarea automatizada puede ser motivo de fallo de seguridad, por lo que hay que tener identificadas las tareas automatizadas que suceden en nuestro sistema, además de tener protegidos los programas y servicios que las crean.

La herramienta que se usa para automatizar procesos es **cron**. Esta herramienta no es más que un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero **Crontab**.

A demás existe el comando **"at"**. Esta herramienta permite programar tareas que se ejecutarán una única vez.

Para limitar la generación de tareas periódicas a usuarios que no estén autorizados (generalmente se considerará únicamente el usuario root como usuario autorizado para tal efecto) se crearán los ficheros **/etc/cron.allow** y **/etc/at.allow** en los que se incorporarán los nombres de los usuarios que pueden utilizar estos servicios.

Se puede establecer esto mismo mediante lista negra en lugar de lista blanca, si es así se crearán los ficheros **/etc/cron.deny** y **/etc/at.deny**, en los que aparecerán los nombres de los usuarios que no pueden utilizar los servicios de los planificadores de tareas.

Nota: Tanto en **CRON** como en **AT** los usuarios incluidos en los ficheros **.allow** tienen preferencia con respecto a los usuarios incluidos en el fichero **.deny**.

6.4.7.2 LOGS DE SISTEMA

El encargado principal de recoger todos los logs para tener una visión global del sistema en Red-Hat/CentOS Linux 7 es la herramienta **Audit**.

El sistema **Audit** de Linux proporciona una forma de rastrear información relevante para la seguridad en su sistema. Según las reglas pre configuradas, **Audit** genera entradas de registro para registrar la mayor cantidad posible de información sobre los eventos que suceden en su sistema. Esta información es crucial en entornos de misión crítica para determinar quién viola las políticas de seguridad y cuáles son las acciones se han realizaron. La auditoría no proporciona seguridad adicional a su sistema; más bien, se puede usar para descubrir infracciones de las políticas de seguridad utilizadas en su sistema. Estas violaciones pueden evitarse con medidas de seguridad adicionales como SELinux.

Entre las partes del sistema que Audit es capaz de recoger información se encuentran las siguientes:

- a) Fecha y hora, tipo y resultado de un evento.
- b) Etiquetas más detalladas de sujetos y objetos.
- c) Asociación de un evento con la identidad del usuario que activó el evento.
- d) Todas las modificaciones a la configuración de auditoría e intentos de acceso a los archivos de registro de auditoría.
- e) Todos los usos de los mecanismos de autenticación, como SSH, Kerberos y otros.
- f) Cambios en cualquier base de datos confiable, como `/etc/passwd`.
- g) Intentos de importación o exportación de información hacia o desde el sistema.
- h) Incluir o excluir eventos en función de la identidad del usuario, las etiquetas de tema y objeto, y otros atributos.
- i) Por la criticidad de los datos que contiene esta aplicación, se procederá a configurar los accesos a la misma de forma segura. Además se hará hincapié en la creación de reglas que proporcionen la mayor información posible sobre lo que pueda ocurrir en el sistema.

6.4.7.3 CONTROL DE INTEGRIDAD DE HARDWARE

AIDE es una alternativa libre a Tripwire, que se emplea principalmente para detectar cambios en los ficheros de configuración y binarios importantes, generalmente generando un resumen cifrado único de los ficheros a ser verificados, y almacenándolos en un lugar seguro. Con un procedimiento regular (mediante el planificador cron), los resúmenes originales se comparan con los generados a partir de la copia actual de cada fichero, para determinar si el fichero ha cambiado. Se le proporcionará a AIDE parámetros, para controlar al menos los siguientes puntos:

- a) La información referente a permisos (**parámetro p**)
- b) La información de los inodos (**parámetro i**)
- c) La cantidad de enlaces (duros y blandos) a cada fichero y al directorio (**parámetro n**)
- d) El propietario de cada fichero (**parámetro u**)
- e) El grupo propietario de cada fichero (**parámetro g**)
- f) El tamaño de cada fichero (**parámetro s**)
- g) La cantidad de bloques utilizados por cada fichero (**parámetro b**)
- h) Las fechas de modificación (**parámetro m**) y creación (**parámetro c**) de cada fichero
- i) El tipo de fichero (**parámetro ftype**)
- j) Las listas de control de acceso (**parámetro acl**)
- k) Las modificaciones en SELinux (**parámetro selinux**)
- l) Los atributos extendidos de ficheros (**parámetro xattrs**)
- m) A demás se generará un resumen en **sha512** por medio del parámetro sha512.

6.4.7.4 CONTROL DE DISPOSITIVOS EXTRAIBLES

En la actualidad el volumen de datos que se puede copiar rápidamente a dispositivos de almacenamiento extraíbles es más que notorio. Aunque este tipo de dispositivos puede fomentar en gran medida la productividad, su potencial para minar la seguridad de los datos y las directivas de control también es muy grande. Entre las amenazas que entrañan estos dispositivos destacan las siguientes:

- a) Usuarios malintencionados que copian grandes cantidades de información sin que se refleje en el seguimiento de la auditoría.
- b) Usuarios de buena fe que desechan o extravían dispositivos con información confidencial.
- c) Malware y códigos nocivos que se infiltran en la red por medio de dispositivos infectados.
- d) Infracciones de normativas como HIPAA, SOX, GLBA y otras regulaciones como consecuencia de la copia y el transporte de datos confidenciales que no se han cifrado.

Por este motivo, se limitarán los dispositivos extraíbles que tienen acceso al sistema, siendo los usuarios con permiso de administración los habilitados con privilegios para la activación de esta característica.

En esta guía se recomienda la instalación del software **USBGUARD**, añadiendo mayor seguridad y control sobre los dispositivos extraíbles que se introduzcan en el sistema.

6.4.7.5 COPIAS DE SEGURIDAD

La realización de copias de seguridad debe responder a una política definida y preestablecida que determine claramente:

- a) Qué información es importante incluir en la copia de seguridad: documentos de usuarios, ficheros de configuración, registros de log, etc.
- b)Cuál será la política de nombrado de los ficheros de copias de seguridad, para su rápida localización en caso de necesidad. Dicha política debe permitir la rápida localización por parte de los administradores del sistema, pero sin dar excesiva información a alguien externo acerca del contenido de las copias de seguridad.
- c) La periodicidad de realización de estas copias de seguridad y el modo de copia (total, incremental, etc.).
- d) El soporte, sistema, localización física, etc. en la que se almacenará la copia de seguridad. Siempre que sea posible, deberán almacenarse dos copias de seguridad, una de fácil acceso para ser utilizada en caso de pérdida de datos, y otra en una localización diferente para prevenir posibles desastres en la localización original de los datos.
- e) Las medidas de protección a aplicar a cada copia de seguridad: control de integridad, confidencialidad, etc. No hay que olvidar que los datos en las copias de seguridad tienen los mismos requisitos de seguridad que los archivos originales.