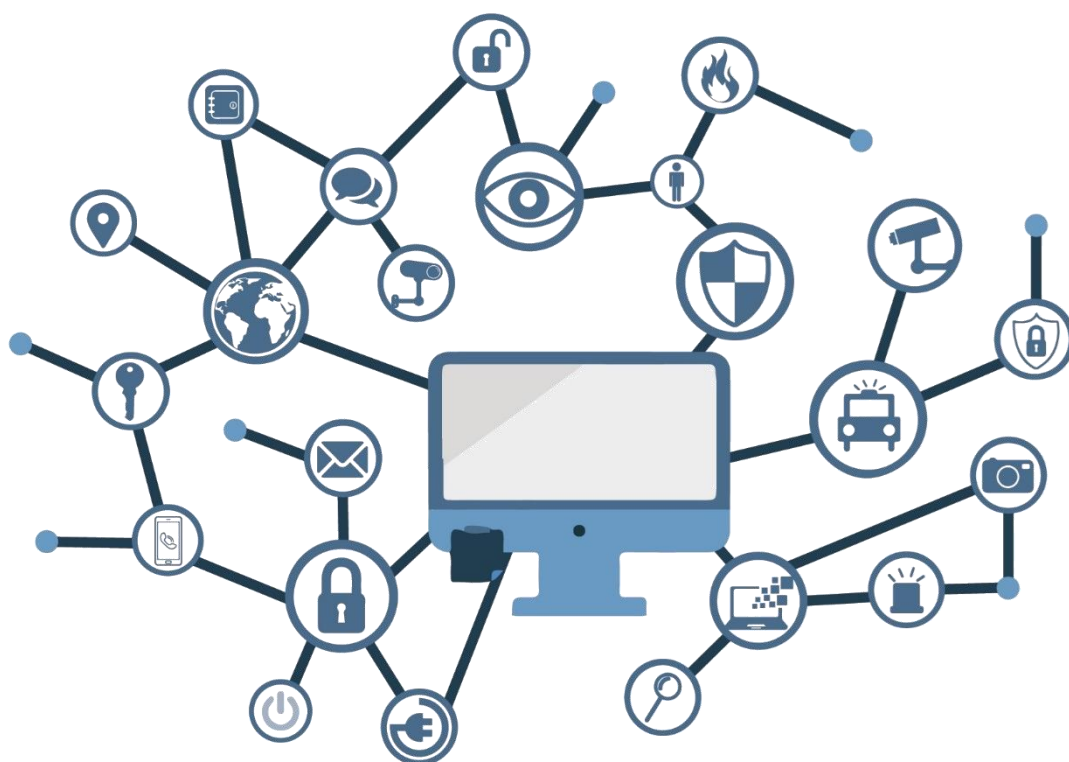


GUÍA DE APLICACIÓN DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX





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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-266-2

Fecha de Edición: octubre de 2022

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.

cpage cpage.mpr.gob.es

ÍNDICE

1. INTRODUCCIÓN	5
2. OBJETO	5
3. ALCANCE	6
4. DESCRIPCIÓN DEL USO DE ESTA GUÍA	7
5. DECLARACIÓN DE RIESGOS	9
5.1 RIESGOS ASOCIADOS A UN EQUIPO RED HAT ENTERPRISE LINUX.....	10
5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO	11
5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO	11
5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA	12
6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES.....	13
7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS	14
ANEXO A. PASO A PASO. CONFIGURACIÓN BASE DE SEGURIDAD SOBRE RED HAT ENTERPRISE LINUX	20
ANEXO A.1. PREPARACIÓN DEL EQUIPO.....	21
ANEXO A.1.1. CONTRASEÑA DE GRUB	23
ANEXO A.1.2. CONFIGURACIÓN DE ROOT Y COMPROBACIÓN DE USUARIOS	23
ANEXO A.2. FORTIFICACIÓN DEL KERNEL	26
ANEXO A.3. CONFIGURACIÓN DE SSH	27
ANEXO A.4. CONFIGURACIÓN Y PROTECCIÓN DE REGISTROS DE ACTIVIDAD	29
ANEXO A.5. CONFIGURACION DE USUARIOS Y POLITICAS DE CREDENCIALES.....	30
ANEXO A.5.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS	30
ANEXO A.5.2. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS	31
ANEXO A.5.3. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS	32
ANEXO A.5.4. CONFIGURACIÓN SEGURA DE GNOME.....	34
ANEXO A.6. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS	36
ANEXO A.6.1. LIMITACIÓN DE SERVICIOS, DEMONIOS Y HERRAMIENTAS	36
ANEXO A.6.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS	39
ANEXO A.7. CONFIGURACIONES ADICIONALES	40
ANEXO A.7.1. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS	40
ANEXO A.7.2. LIMITACIÓN DE DISPOSITIVOS EXTRAÍBLES	41
ANEXO A.7.3. PROTECCIÓN DE SERVICIOS DE RED	44
ANEXO A.7.4. CONFIGURACIÓN DE SEGURIDAD – SELINUX	46
ANEXO A.7.5. INTERFAZ WEB COCKPIT	47
ANEXO A.7.6. APLICACIÓN DE ACTUALIZACIONES	51
ANEXO A.7.7. INSTALACIÓN DE ANTIVIRUS.....	53
ANEXO A.7.8. RESPALDO DE ARCHIVOS CON SISTEMA DE FICHEROS XFS.....	55

ANEXO A.7.9. RESTAURACIÓN DE ARCHIVOS DE RESPALDO.....	57
--	----

1. 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 (incluidos en la serie CCN STIC 600), siendo de aplicación en el cumplimiento del Esquema Nacional de Seguridad (ENS) y para los sistemas que manejen información clasificada.

2. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para aplicar un perfilado de seguridad basado en la realización de un análisis de riesgos, en sistemas que implementen Red Hat Enterprise Linux 9.0

La configuración que se aplica a través de la presente guía se ha diseñado para adaptarse a las características específicas de cada entorno, en función de los resultados obtenidos del análisis de riesgos preceptivo. Se trata de la aproximación del MARCO MODERNO DE SEGURIDAD que desde el Centro Criptológico Nacional se persigue para una adaptación adecuada al ecosistema en cuestión, el cual basa sus pilares fundamentales en los siguientes objetivos.

- a) Las medidas a adoptar estarán condicionadas por el análisis de riesgos preceptivo de cada escenario, la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.
- b) Se tendrán en cuenta los avances tecnológicos y el estado del arte más reciente en ciberseguridad.
- c) Será adaptable en la aplicación de medidas evitando una aplicación monolítica y estanca, utilizando la Declaración de Aplicabilidad como elemento fundamental sobre el que vertebrar la seguridad, en base a responsabilidad compartida.
- d) La Declaración de Aplicabilidad (conjunto de medidas a implementar) utilizará de base los niveles del Esquema Nacional de Seguridad validados por el análisis de riesgos preceptivo utilizado en base a una categorización ENS MEDIO.
- e) Las medidas de seguridad se podrán aplicar a sistemas ya implementados o nuevos sistemas, minimizando el impacto en la producción.
- f) Las guías se revisarán y se actualizarán según las nuevas amenazas y estado del arte tecnológico en ciberseguridad.

Este marco de aplicación basado en un perfilado de seguridad tiene en consideración la diversidad de escenarios que se pueden dar, con sus particularidades, riesgos y amenazas, por lo que será cada organización que implementa las medidas de seguridad la que deba determinar qué medidas serán de aplicación, compensadas o complementadas, en función de sus condiciones específicas, asumiendo una responsabilidad compartida en la puesta en operación del sistema.

Para ayudar a las organizaciones a implementar las medidas de seguridad, se ha considerado la necesidad de crear tres (3) alcances de implementación:

- a) Alcance básico.
- b) Alcance intermedio.
- c) Alcance avanzado.

Para la elaboración de esta guía, se ha hecho un esfuerzo de revisión exhaustiva de las distintas configuraciones de seguridad disponibles en Red Hat Enterprise Linux 9, alineándolas y clasificándolas en función de los riesgos que cada una de ellas mitigan o abordan individualmente.

De esta forma, se pretende dar mayor coherencia al conjunto de medidas resultantes o perfilado de seguridad, siendo necesario aplicar únicamente aquellas medidas que realmente atienden a un riesgo declarado en función de los niveles de alcance señalados anteriormente.

Se trata de implementar medidas con un criterio claro, conociendo los riesgos, el contexto de la amenaza y la superficie de exposición de cada sistema en particular, y adaptando las medidas de seguridad a aplicar en función de ello.

3. ALCANCE

Para ayudar a las organizaciones a identificar los riesgos de seguridad, y por lo tanto realizar el perfilado correspondiente para cada uno de sus sistemas, se ha incorporado a esta guía un apartado denominado declaración de riesgos donde se identifican y se explican los principales riesgos del producto del que trata la guía.

Esta guía se ha elaborado con el objetivo de proporcionar información específica sobre los riesgos y las medidas de mitigación recomendadas para los escenarios planteados. En particular, se incluirá la configuración para aplicar un perfilado de seguridad de un equipo con Red Hat Enterprise Linux 9.0, instalado en español.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante. Hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento y, por lo tanto, deberá prestarse especial atención a dichas publicaciones.

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 de haberla probado 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.

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

Este documento incluye:

- a) Descripción de uso de esta guía. Breve explicación acerca de los pasos a seguir para identificar, seleccionar y aplicar las medidas de seguridad recomendadas.
- b) Declaración de riesgos. En esta sección se identifican los principales riesgos asociados al producto o tecnología del que trata la guía CCN-STIC. Por ejemplo, un servicio web puede tener riesgos relacionados con el acceso remoto, mientras que un controlador de dominio puede tener riesgos relacionados con los procesos de autenticación. La organización podrá hacer uso de los riesgos identificados en este punto y añadir los que considere necesarios para su escenario en particular.
- c) Identificación del valor de riesgo. En esta sección se muestran una serie de tablas o mapas de calor, con tres (3) niveles de superficie de exposición y los valores de riesgo resultantes de la intersección de los niveles de impacto y probabilidad. Se trata de una muestra de cómo alterando alguna de estas variables (superficie de exposición, impacto y probabilidad), los resultados del riesgo de adecúan a cada realidad.
- d) Perfilado de seguridad. En este punto se establecen las medidas de seguridad que se deberán aplicar al producto o tecnología del que trata la guía. Su clasificación se realiza en tres (3) niveles, cada uno de ellos asociado a un conjunto de niveles de riesgos.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

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

- a) **Identificación de riesgos del producto.** Se recomienda realizar un inventario de riesgos que puedan existir por la propia naturaleza del producto o tecnología, como por la funcionalidad prevista por la organización. Para ello, se han identificado una serie de riesgos inherentes al producto o tecnología, los cuales deberán ser completados con los riesgos particulares del sistema que se vaya a implementar.

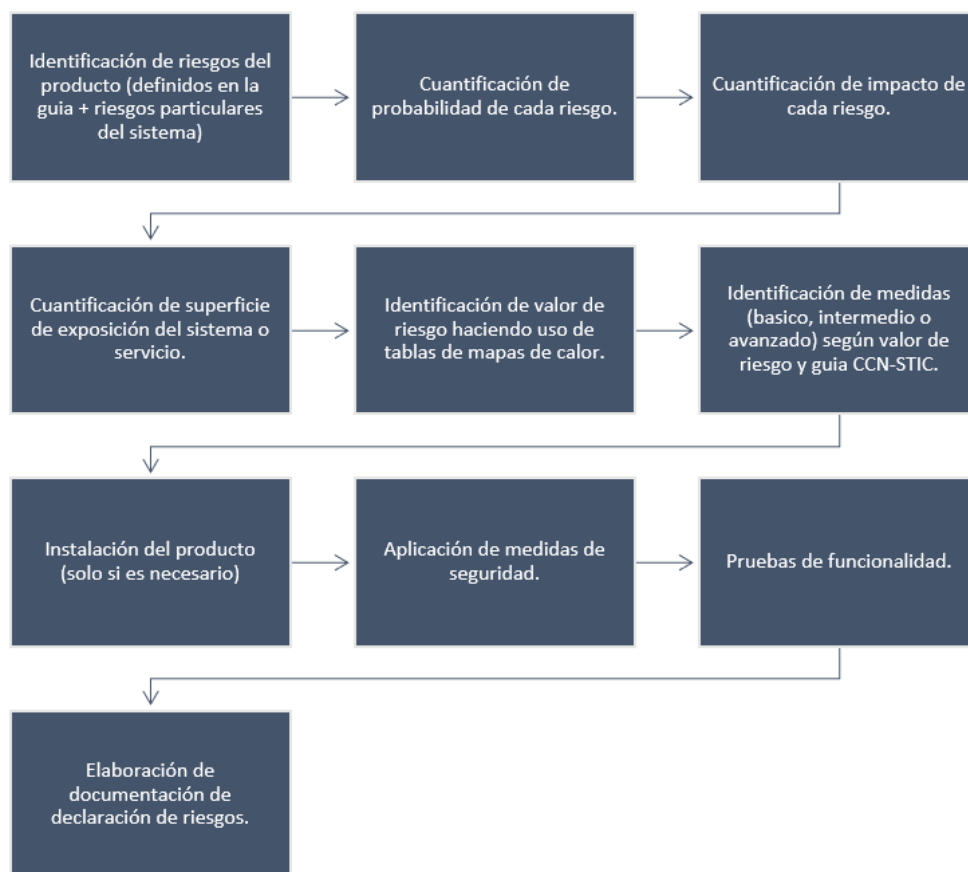
Para la identificación inicial de riesgos, se ha empleado la metodología MAGERIT y la herramienta PILAR, sobre un escenario basado en Red Hat Enterprise Linux 9.0.

- b) **Cuantificación de probabilidad de cada riesgo.** Se deberá cuantificar la probabilidad de ocurrencia de cada riesgo en función de las condiciones particulares que cada organización conoce de sus sistemas.
- c) **Cuantificación de impacto de cada riesgo.** Se deberá cuantificar el impacto en las operaciones y en el negocio, en función de las condiciones particulares que cada organización conoce de sus sistemas.
- d) **Cuantificación de superficie de exposición del sistema o servicio.** La organización deberá determinar el nivel de superficie de exposición que tendrá el activo (servicio que presta o información que maneja).
- e) **Identificación del valor de riesgo haciendo uso de tablas de mapas de calor.** Para cada guía se han desarrollado una serie de tablas de mapas de calor, permitiendo calcular e identificar donde se sitúa cada uno de los riesgos identificados en los primeros pasos. Una vez identificado el nivel de riesgo, en el siguiente paso se procederá a aplicar la medida mitigadora correspondiente a dicho nivel de riesgo.

- f) **Identificación de medidas (básico, intermedio o avanzado) según valor de riesgo y guía CCN-STIC.** La lista de medidas de seguridad está agrupada en categorías y ordenada según el nivel de riesgo resultado de los cálculos anteriores. Es importante señalar que cada categoría puede conllevar la necesidad de aplicar una o varias medidas de seguridad, que a su vez se pueden traducir en distintas configuraciones, directivas de seguridad o la instalación de software de protección.

Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de flexibilidad a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta guía de seguridad se identifican qué medidas de seguridad serán necesarias aplicar, pero el cómo aplicarlas se deja a elección de las propias organizaciones.

- g) **Instalación del producto (en nuevas instalaciones).** Una vez conocidos los riesgos y las medidas de mitigación de éstos, se procederá con la instalación del sistema operativo, en el caso de nuevas implementaciones. En caso de que el sistema ya se encuentre instalado, se puede saltar este paso.
- h) **Aplicación de medidas de seguridad.** En este paso se aplicarán las medidas de seguridad recomendadas según el nivel de riesgo resultante para hacer efectiva la mitigación, reducción o eliminación del riesgo. Es lo que se denomina el perfilado de seguridad. Cada organización puede tener un perfilado distinto y como se ha indicado anteriormente, se deberán aplicar las medidas de seguridad en función de dicho perfilado.
- i) **Pruebas de funcionalidad.** Se recomienda diseñar y ejecutar un plan de pruebas de funcionalidad posterior a la aplicación de medidas, dado que alguna de ellas puede haber deshabilitado o bloqueado funcionalidades que requiere la organización. En ese caso se podrán establecer directivas de excepción para revertir los cambios, asumiendo el riesgo que ello conlleva.
- j) **Elaboración de documentación de declaración de riesgos.** Se recomienda elaborar un documento de declaración de riesgos donde se establezca claramente cada uno de los riesgos identificados y las medidas de seguridad aplicadas.



5. DECLARACIÓN DE RIESGOS

Se trata del primer paso a realizar para la aplicación de las medidas de seguridad acordes a la realidad y condiciones donde estará operando el sistema.

Con motivo de la aparición de nuevas versiones y cambios en el software de base, como los sistemas operativos, es altamente recomendable contar con unas medidas de seguridad y de evaluación constantes que puedan detectar, de forma proactiva y previa a su aplicación, cualquier vulnerabilidad, amenaza o riesgo.

El análisis de riesgos permitirá elaborar un perfilado para la aplicabilidad de medidas acorde a los resultados obtenidos, minimizando los vectores de ataque, brechas o malas configuraciones de seguridad sobre los activos, e intentando también que estas medidas no afecten a la funcionalidad o usabilidad del sistema y sus objetivos.

Esta guía de seguridad tiene como uno de sus objetivos ayudar a la implementación de las medidas de seguridad, por lo tanto, para la elaboración de la propia guía se ha realizado un análisis de riesgos específico para un sistema basado en Red Hat Enterprise Linux 9.0.

Para la ejecución del presente Análisis de Riesgos, se han definido dos (2) escenarios base, los cuales se consideran esenciales y estándar de uso del sistema.

- El primer escenario será un sistema aislado en red, quiere decir que estará conectando a elementos de red internos dentro de una organización o entidad, pero no realizará conexiones externas hacia redes no seguras como Internet.
- El segundo escenario será un sistema conectado a redes no seguras como puede ser Internet, quiere decir que tendría la capacidad de establecer conexiones con elementos de red externos de una organización o entidad.

5.1 RIESGOS ASOCIADOS A UN EQUIPO RED HAT ENTERPRISE LINUX

A continuación, se identifican los resultados de este análisis, los cuales forman parte de la declaración de riesgos y constituye, como ya se ha indicado, el primer paso a realizar en la implementación de esta guía de seguridad. Estos riesgos se deberán tener en consideración cuando la organización diseñe y elabore su propio análisis de riesgos.

Para facilitar la tarea de identificar, cuantificar y valorar cada uno de los riesgos, se ha elaborado la tabla de control que se presenta en la siguiente página, donde se podrá ir registrando en cada caso los niveles de probabilidad e impacto asociados a cada riesgo para un equipo en concreto.

EXP	NOMBRE DEL EQUIPO			
	SISTEMA OPERATIVO		BUILD	
	FUNCION PRINCIPAL		FECHA DE AA.RR.	
NUM	RIESGOS	APLICA (S/N)	PROBABILIDAD [1...5]	IMPACTO [1...5]
1.	[A.3] Manipulación de los registros de actividad.			
2.	[A.4] Manipulación de los ficheros de configuración.			
3.	[A.5] Suplantación de la identidad.			
4.	[A.6] Abuso de privilegios de acceso.			
5.	[A.8] Difusión de software dañino.			
6.	[A.11] Acceso no autorizado.			
7.	[A.15] Modificación de la información.			
8.	[A.19] Revelación de información.			
9.	[A.22] Manipulación de programas.			
10.	[A.23] Manipulación del hardware.			
11.	[A.24] Denegación de servicio.			
12.	[A.25] Robo de equipos.			
13.	[A.29] Extorsión.			
14.	[A.30] Ingeniería social.			
15.	[E.25] Pérdida de equipos.			

5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO

El siguiente paso, será cuantificar la probabilidad de cada uno de los riesgos. Los valores de probabilidad podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) muy poco probable y cinco (5) muy probable:

- a) **Probabilidad 1:** Es muy poco probable que se materialice el riesgo, ya sea por las condiciones específicas del sistema en la organización o porque existan salvaguardas ya implementadas que hagan que el riesgo prácticamente desaparezca.
- b) **Probabilidad 2:** Es poco probable que se materialice el riesgo, aunque se puede materializar.
- c) **Probabilidad 3:** Es probable que se materialice el riesgo dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.
- d) **Probabilidad 4:** Es bastante probable que se materialice el riesgo, dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.
- e) **Probabilidad 5:** Es muy probable que se materialice el riesgo, dadas las condiciones específicas del sistema en la organización o porque no existen salvaguardas que reduzcan la probabilidad de materialización del riesgo. Las medidas de seguridad a aplicar cuando se da este nivel pueden ser más estrictas que en niveles inferiores.

5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO

Al igual que sucede con la cuantificación de la probabilidad, se deberá cuantificar el grado de impacto en el servicio o negocio en el supuesto de que el riesgo se materialice. Los valores de impacto podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) cuando no tiene un impacto conocido o es muy pequeño y cinco (5) cuando el impacto es muy importante:

- a) **Impacto 1:** El riesgo, en el caso de que se materialice, no tiene un impacto conocido o es muy pequeño, prácticamente despreciable. Los datos y el servicio no se ven comprometidos y el sistema funciona correctamente. Este nivel de impacto puede requerir la aplicación de medidas de prevención.
- b) **Impacto 2:** El riesgo, en el caso de que se materialice, tiene un impacto pequeño. No se han comprometidos los datos ni el servicio, sin embargo, es posible que, si no se corrige, el sistema se vuelva inestable o pueda existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención.
- c) **Impacto 3:** El impacto en el sistema es preocupante. No se han comprometido los datos, sin embargo, el servicio puede continuar de forma limitada y a corto plazo podría haber una degradación de la seguridad del sistema. Si no se aplican las medidas necesarias puede existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención, pero también medidas de corrección.

- d) **Impacto 4:** El impacto en el sistema es importante. Es posible que algunos datos hayan sido comprometidos y los servicios se hayan visto afectados. También es posible que el sistema se haya vuelto inestable o comience a ser vulnerable. Se debe actuar lo antes posible para restablecer el correcto funcionamiento.
- e) **Impacto 5:** El impacto en el sistema es muy importante. Afecta directamente a la disponibilidad del servicio, imposibilitando el acceso a la información. El sistema ha sido comprometido, y algunos o todos los datos han sido comprometidos. Un atacante externo puede haber obtenido acceso privilegiado y puede estar controlando el sistema. Se deben aplicar medidas de recuperación de forma inmediata.

5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA

Por último, se deberá tener en cuenta el nivel o grado de exposición del sistema a las amenazas y riesgos externos. Este valor actuará como modulador a la hora de calcular el valor final de cada uno de los riesgos.

Por ejemplo, ante un riesgo cuyo impacto y probabilidad son altos o muy altos, si el sistema se encuentra en un nivel de superficie de exposición bajo, es lógico pensar que el valor final del riesgo se vea atenuado en parte por las condiciones de exposición en las que encuentra el sistema. Por el contrario, si un riesgo tiene unos niveles de impacto y probabilidad bajos, ante un nivel de superficie de exposición alto, es lógico pensar que el valor final del riesgo se vea incrementado por este mismo motivo.

Es evidente que pueden existir multitud de escenarios y configuraciones de red, siendo prácticamente imposible reflejar todas ellas en una sola guía de seguridad. Sin embargo, para una mejor comprensión y simplificación de las medidas que se deberán adoptar, se han agrupado en tres (3) niveles las distintas opciones de superficie de exposición:

- a) **Nivel de superficie de exposición 1:** Representa aquellos sistemas que no están expuestos a riesgos externos, procedentes de redes interconectadas o redes no confiables como Internet. En este nivel se encuentran los sistemas aislados, sin ningún tipo de comunicación con otras redes.
- b) **Nivel de superficie de exposición 2:** Representa aquellos sistemas que tienen algún tipo de conexión de red local o de interconexión con otras redes. Estos sistemas se conectan únicamente con redes confiables. En este nivel se encuentran los sistemas compuestos por más de un equipo conectado a través de una red local (LAN) o varios sistemas que están interconectados entre sí a través de otros medios, pero que no son accesibles desde Internet o redes no confiables.
- c) **Nivel de superficie de exposición 3:** Representa aquellos sistemas accesibles desde o con conexión directa o indirecta con Internet y otras redes. Dado que Internet se considera una red no confiable, el riesgo de explotación de vulnerabilidades de ejecución remota es mucho mayor que en los niveles inferiores. En este nivel se encuentra la mayoría de los sistemas en producción de las organizaciones.

6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES

Una vez identificados los distintos riesgos inherentes al sistema y después de calcular los valores de probabilidad, impacto y superficie de exposición de cada uno de ellos, el siguiente paso será determinar el valor final de cada riesgo. Tal y como ya se ha indicado, este valor variará en función de cada una de las tres variables que se han tenido en cuenta.

Para facilitar su cálculo, se han elaborado las siguientes tablas con un diseño de mapas de calor, que varían según la superficie de exposición que tendrá el sistema. Cada una de ellas servirá como referencia para determinar el valor final del riesgo, el cual se podrá anexar a la tabla de riesgos del punto “5.1 RIESGOS ASOCIADOS A UN EQUIPO RED HAT ENTERPRISE LINUX”.

SUPERFICIE DE EXPOSICIÓN		1			
PROBABILIDAD	NIVEL DE RIESGO				
5	5	6	7	7	8
4	4	5	6	7	7
3	3	4	5	6	7
2	2	3	4	5	6
1	2	2	3	4	5
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN		2			
PROBABILIDAD	NIVEL DE RIESGO				
5	6	7	7	8	9
4	5	6	7	7	8
3	4	5	6	7	7
2	3	4	5	6	7
1	2	3	4	5	6
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN		3			
PROBABILIDAD	NIVEL DE RIESGO				
5	7	7	8	9	10
4	6	7	7	8	9
3	5	6	7	7	8
2	4	5	6	7	7
1	3	4	5	6	7
IMPACTO	1	2	3	4	5

7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS

A continuación, se muestran las categorías o agrupación de medidas de seguridad que deberán ser aplicadas a Red Hat Enterprise Linux 9, en función de los resultados obtenidos por el análisis de riesgos y la cuantificación de cada uno de éstos.

Para una mejor comprensión, se han agrupado las medidas en tres (3) alcances de implementación, cada uno de ellos asociado a un grupo de niveles de riesgos:

- a) Alcance básico.
- b) Alcance intermedio.
- c) Alcance avanzado.

Una vez obtenido el nivel de riesgo de cada uno de los riesgos identificados, se aplicará la siguiente tabla para determinar las medidas necesarias en cada nivel.

Esta tabla indica que, si se ha obtenido un valor menor o igual a tres (3), se deberán aplicar las categorías de perfilado de seguridad de alcance básico. Si el valor obtenido para un riesgo determinado está entre cuatro (4) y seis (6), se deberán aplicar las categorías de perfilado de seguridad de alcance intermedio. Por último, si el valor obtenido es siete (7) o superior, se deberán aplicar las categorías de perfilado de alcance avanzado.

NIVEL DE RIESGO	ALCANCE		
	(B)ÁSICO	(I)NTERMEDIO	(A)VANZADO
9	SI	SI	SI
8	SI	SI	SI
7	SI	SI	SI
6	SI	SI	
5	SI	SI	
4	SI	SI	
3	SI		
2	SI		
1	SI		

En la siguiente tabla se muestra la asociación entre los riesgos identificados en el primer paso de esta guía y las categorías de perfilado de seguridad que mitigan, controlan o reducen dicho riesgo.

Como se puede observar, pueden existir categorías de perfilado de seguridad que actúen sobre uno o varios riesgos. Por lo tanto, para una mejor identificación, se han codificado cada una de las categorías, asociándolas al primer riesgo que mitigan, obteniendo la siguiente nomenclatura de categorías:

- a) A.3: corresponde con el código de riesgo que especifica la herramienta PILAR.
- b) SEC-RHEL1: corresponde con la categoría de seguridad 1 para dicho riesgo. El número se incrementará en uno para cada nueva categoría que se haya identificado.

La siguiente tabla define qué conjunto de medidas de seguridad deben ser aplicadas, en función de los niveles de riesgo obtenidos.

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log).	[A.3.SEC-RHEL1] Se auditan los inicios de sesión.			
	[A.3.SEC-RHEL2] Se controla quien puede acceder a los registros de seguridad y auditoría.			
	[A.3.SEC-RHEL3] Se controla el cambio de hora del sistema.			
	[A.3.SEC-RHEL4] Se controla quién puede generar o modificar reglas de audit.			
	[A.3.SEC-RHEL5] Se ha implementado la auditoría detallada basada en subcategorías.			
	[A.3.SEC-RHEL6] Se garantiza al menos 90 días de registros de actividad.			
	[A.3.SEC-RHEL7] Se auditan las modificaciones del fichero sudoers, así como los cambios en permisos, usuarios, grupos y contraseñas.			
	[A.3.SEC-RHEL8] Se auditan los cambios en la configuración de Cron y en tareas programadas incluyendo los de scripts de inicio.			
	[A.3.SEC-RHEL9] Se auditan los intentos de acceso a elementos críticos.			
	[A.3.SEC-RHEL10] Se audita toda operación de montaje en el sistema y modificaciones en la memoria de intercambio.			
	[A.3.SEC-RHEL11] Se auditan modificaciones en ficheros PAM.			
[A.4] Manipulación de los ficheros de configuración.	[A.4.SEC-RHEL1] Los usuarios estándar no disponen de permisos de administrador local ni se encuentran incluidos en un grupo sudoer.			
	[A.4.SEC-RHEL2] El sistema tiene un antivirus y este está actualizado.			
	[A.4.SEC-RHEL3] Se modifican los permisos por particiones			
[A.5] Suplantación de la identidad.	[A.5.SEC-RHEL1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-RHEL2] Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.			
	[A.5.SEC-RHEL3] Se controla el acceso a las claves de cifrado.			
	[A.5.SEC-RHEL4] Se han deshabilitado los algoritmos de cifrado inseguros.			
	[A.5.SEC-RHEL5] Se exige el cambio de contraseña de forma recurrente.			
	[A.5.SEC-RHEL6] Se hace uso de protocolos seguros para los procesos de autenticación de red.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX	ALCANCE		
		B	I	A
	[A.5.SEC-RHEL7] Se controla la inactividad de la sesión de red.			
	[A.5.SEC-RHEL8] Se controla la inactividad de consola local y remota.			
[A.6] Abuso de privilegios de acceso.	[A.6.SEC-RHEL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC-RHEL2] Se restringen accesos en modo recuperación incluido el modo modificación de inicio de grub.			
	[A.6.SEC-RHEL3] Se limita la shell de usuarios de servicio a "/bin/false".			
	[A.6.SEC-RHEL4] Se restringe el uso de sesiones con usuario "root".			
	[A.6.SEC-RHEL5] Se modifica la máscara global del sistema para ser más restrictiva.			
	[A.6.SEC-RHEL6] Se eliminan los grupos y usuarios innecesarios del sistema.			
[A.8] Difusión de software dañino.	[A.8.SEC-RHEL1] Se controla quién puede instalar software en el sistema.			
	[A.8.SEC-RHEL2] El sistema operativo está actualizado.			
	[A.8.SEC-RHEL3] El sistema tiene un firewall local activado.			
	[A.8.SEC-RHEL4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC-RHEL5] Se controla la ejecución de aplicaciones.			
	[A.8.SEC-RHEL6] Se dispone de medidas anti ransomware habilitadas.			
	[A.4.SEC-RHEL2] El sistema tiene un antivirus y éste está actualizado.			
	[A.8.SEC-RHEL7] Está habilitado el arranque cifrado con contraseña que evite modificaciones (GRUB protegido).			
	[A.5.SEC-RHEL1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-RHEL2] Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.			
	[A.6.SEC-RHEL6] Se eliminan los grupos y usuarios innecesarios del sistema.			
	[A.8.SEC-RHEL8] Se audita la descarga de archivos			
	[A.8.SEC-RHEL9] Están deshabilitados los compiladores del sistema			
[A.11] Acceso no autorizado.	[A.11.SEC-RHEL1] Se controla el inicio de sesión local en el sistema.			
	[A.11.SEC-RHEL2] Se ha reforzado la seguridad del protocolo SSH.			
	[A.11.SEC-RHEL3] Se dispone de una política de credenciales robusta.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX	ALCANCE		
		B	I	A
	[A.11.SEC-RHEL4] Durante el inicio de sesión, el sistema muestra un texto en cumplimiento con las normas o directivas de la organización.			
	[A.11.SEC-RHEL5] Se controla el acceso al sistema a través de la red.			
	[A.11.SEC-RHEL6] Sólo se permiten algoritmos de cifrado robustos en accesos al sistema.			
	[A.3.SEC-RHEL4] Se controla quién puede generar o modificar reglas de audit.			
	[A.5.SEC-RHEL1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-RHEL2] Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.			
	[A.6.SEC-RHEL6] Se eliminan los grupos y usuarios innecesarios del sistema.			
	[A.11.SEC-RHEL7] Se limita el tiempo de inactividad del GUI.			
	[A.11.SEC-RHEL8] Se muestra un banner disuasorio.			
	[A.11.SEC-RHEL9] Se deshabilita la lista de usuarios.			
	[A.11.SEC-RHEL10] Se deshabilita recordar el historial de ficheros.			
	[A.11.SEC-RHEL11] Se deshabilita combinación de teclas para iniciar el inspector GTK			
	[A.11.SEC-RHEL12] Se deshabilita el auto montaje de dispositivos extraíbles en el sistema.			
[A.15] Modificación de la información.	[A.15.SEC-RHEL1] Se controla el uso de medios de almacenamiento extraíbles.			
	[A.5.SEC-RHEL6] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.6.SEC-RHEL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.11.SEC-RHEL2] Se ha reforzado la seguridad del protocolo SSH.			
	[A.11.SEC-RHEL6] Sólo se permiten algoritmos de cifrado robustos en accesos al sistema.			
[A.19] Revelación de información.	[A.19.SEC-RHEL1] Se controla el acceso al árbol de carpetas y ficheros.			
	[A.19.SEC-RHEL2] Se aplican medidas para la protección de las cuentas.			
	[A.19.SEC-RHEL3] Está habilitado un algoritmo robusto y la complejidad de contraseñas			
	[A.3.SEC-RHEL2] Se controla quien puede acceder a los registros de seguridad y auditoría.			
	[A.5.SEC-RHEL3] Se controla el acceso a las claves de cifrado.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX	ALCANCE		
		B	I	A
	[A.5.SEC-RHEL6] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.6.SEC-RHEL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC-RHEL2] Se restringen accesos en modo recuperación incluido el modo modificación de inicio de grub.			
[A.22] Manipulación de programas.	[A.6.SEC-RHEL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC-RHEL2] Se restringen accesos en modo recuperación incluido el modo modificación de inicio de grub.			
	[A.6.SEC-RHEL3] Se limita la shell de usuarios de servicio a "/bin/false".			
	[A.8.SEC-RHEL4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC-RHEL6] Se dispone de medidas anti ransomware habilitadas.			
[A.23] Manipulación del hardware.	[A.23.SEC-RHEL1] Se controla la instalación y uso de cualquier dispositivo conectado al equipo.			
	[A.15.SEC-RHEL1] Se controla el uso de medios de almacenamiento extraíbles.			
	[A.23.SEC-RHEL2] Se restringe el montaje y desmontaje dinámico de sistemas de archivos			
[A.24] Denegación de servicio.	[A.24.SEC-RHEL1] Se controlan los privilegios que afectan al rendimiento del sistema.			
	[A.24.SEC-RHEL2] Se controla quien puede apagar el sistema.			
	[A.8.SEC-RHEL6] Se dispone de medidas anti ransomware habilitadas.			
	[A.3.SEC-RHEL3] Se controla el cambio de hora del sistema.			
	[A.3.SEC-RHEL4] Se controla quién puede generar o modificar reglas de audit.			
[A.25] Robo de equipos.	[A.25.SEC-RHEL1] El disco del sistema está cifrado.			
	[A.25.SEC-RHEL2] El disco de datos está cifrado.			
[A.29] Extorsión.	[A.4.SEC-RHEL2] El sistema tiene un antivirus y éste está actualizado.			
	[A8.SEC-RHEL1] Se controla quién puede instalar software en el sistema.			
	[A.8.SEC-RHEL2] El sistema operativo está actualizado.			
	[A.8.SEC-RHEL3] El sistema tiene un firewall local activado.			
	[A.8.SEC-RHEL4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA RED HAT ENTERPRISE LINUX	ALCANCE		
		B	I	A
	[A.8.SEC-RHEL5] Se controla la ejecución de aplicaciones.			
	[A.8.SEC-RHEL6] Se dispone de medidas anti ransomware habilitadas.			
[A.30] Ingeniería social.	[A.30.SEC-RHEL1] Existe una política de bloqueo de cuentas ante inicios de sesión incorrectos.			
[E.25] Pérdida de equipos.	[A.25.SEC-RHEL1] El disco del sistema está cifrado.			
	[A.25.SEC-RHEL2] El disco de datos está cifrado.			

ANEXO A. PASO A PASO. CONFIGURACIÓN BASE DE SEGURIDAD SOBRE RED HAT ENTERPRISE LINUX

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento de los sistemas Red Hat Enterprise Linux 9, según los aspectos definidos en cada uno de los puntos anteriores de este documento.

Esta configuración se ofrece a modo de referencia o ejemplo de aplicabilidad de medidas en función de unos resultados concretos del análisis de riesgos ejecutado. Es posible que en otros escenarios y con otra superficie de exposición, el perfilado de aplicación de medidas sea diferente.

Es necesario remarcar que la línea base de seguridad establecida dentro del presente anexo corresponde con un **perfilado intermedio**.

Nota: En caso de que el perfilado de seguridad y superficie de exposición obtenidos, en base al análisis realizado, requieran de una **configuración de seguridad avanzada, será necesario implementar medidas adicionales de seguridad**. Por el contrario, en caso de que el resultado de dicho análisis indique que la necesidad de configuración solo deba establecerse según el perfilado básico, será posible evitar ciertas medidas de seguridad de las establecidas en el presente anexo.

Por otro lado, es necesario indicar que ciertas categorías de seguridad no pueden ser aplicadas por medio de configuraciones exactas, por ello se ha dedicado un apartado específico que permita establecer ejemplos de configuración sobre este tipo de categorías las cuales deberán ser adaptadas por cada organización.

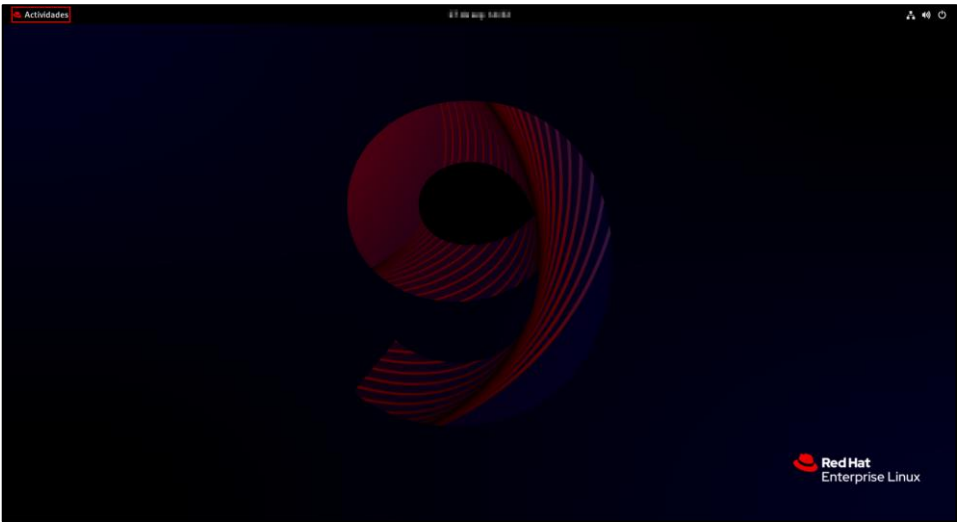
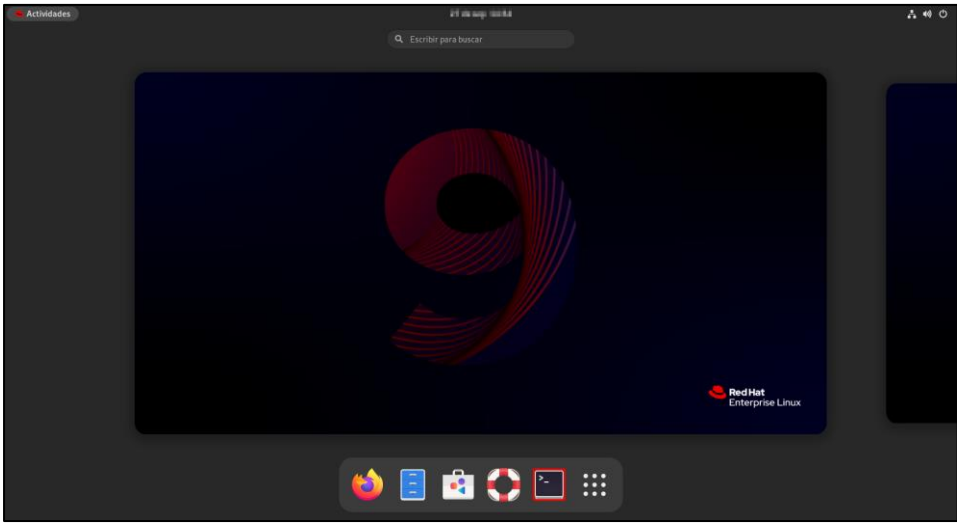
Debe tenerse en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

A modo de ejemplo, se procede a realizar un perfilado intermedio de seguridad, aplicado a un sistema operativo Red Hat Enterprise Linux 9, conectado por red a repositorios oficiales de Red Hat. El sistema se encuentra alojado en un equipo con una configuración de BIOS en modo "LEGACY" y un sistema de ficheros "XFS".

ANEXO A.1. PREPARACIÓN DEL EQUIPO

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.5.SEC-RHEL4]** Se han deshabilitado los algoritmos de cifrado inseguros. Con el endurecimiento de estos algoritmos de cifrado se evita el acceso a la información del sistema a personas o medios que no estén autorizados para realizar tales accesos.

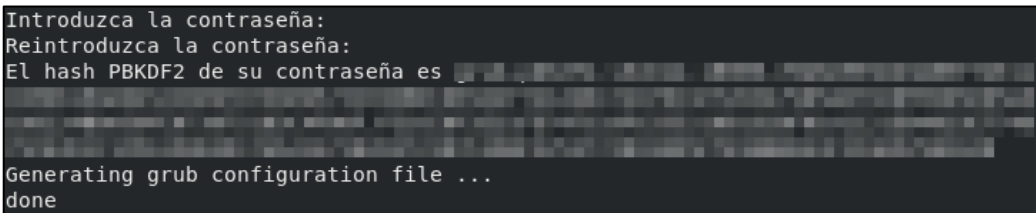
Paso	Descripción
1.	Inicie sesión en el equipo Red Hat Enterprise Linux 9 que está asegurando, utilizando una cuenta con permisos de administrador o sudoers.
2.	<p>Diríjase a la barra de tareas superior, pulse sobre “Actividades”.</p>  <p>Posteriormente en la fila de la parte inferior seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen.</p> 
3.	<p>Diríjase al directorio raíz “/”.</p> <pre>\$ cd /</pre>

Paso	Descripción
4.	<p>Cree el directorio “Scripts” en la ruta “/”.</p> <pre>\$ sudo mkdir /Scripts</pre>
5.	<p>Monte el dispositivo de CDROM.</p> <pre>\$ sudo mount /dev/cdrom /media</pre> <p>Nota: En este caso se considera que los scripts están disponibles en un disco óptico. Si el caso fuera otro, deberá adecuar la configuración a los parámetros de su organización.</p>
6.	<p>Copie en el directorio “Scripts”, los ficheros y subdirectorios asociados a esta guía.</p> <pre>\$ sudo cp -r /media/* /Scripts/</pre> <p>Nota: Los scripts asumen que su ubicación en el sistema será bajo “/Scripts”. Si los dispusiese en otra ubicación, tendrá que editar los scripts para reflejar la nueva ruta en los que se sitúan.</p>
7.	<p>Desmonte el dispositivo de CDROM.</p> <pre>\$ sudo umount /media</pre>
8.	<p>Para que el nivel de política criptográfica del sistema cumpla con los parámetros de seguridad necesarios a los niveles exigidos, ejecute el siguiente comando.</p> <pre>\$ sudo update-crypto-policies --set DEFAULT</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo update-crypto-policies --set DEFAULT [sudo] password for aCdCmN610: Setting system policy to DEFAULT Note: System-wide crypto policies are applied on application start-up. It is recommended to restart the system for the change of policies to fully take place. [aCdCmN610@RHEL9 ~]\$</pre> <p>Nota: Los niveles posibles de política criptográfica en el sistema son cuatro:</p> <ul style="list-style-type: none"> - DEFAULT: El nivel de política criptográfica predeterminado de todo el sistema ofrece configuraciones seguras para los modelos de amenazas actuales. Permite los protocolos TLS 1.2 y 1.3, así como los protocolos IKEv2 y SSH2. Las claves RSA y los parámetros Diffie-Hellman se aceptan si tienen al menos 2048 bits de longitud. - LEGACY: Esta política garantiza la máxima compatibilidad con versiones anteriores de Red Hat Enterprise Linux, es menos seguro debido a una mayor superficie de ataque. Además de los algoritmos y protocolos del nivel DEFAULT, incluye soporte para los protocolos TLS 1.0 y 1.1. Los algoritmos DSA, 3DES y RC4 están permitidos, mientras que las claves RSA y los parámetros Diffie-Hellman se aceptan si tienen al menos 1023 bits de longitud. - FUTURE: Un nivel de seguridad conservador. Este nivel no permite el uso de SHA-1 en algoritmos de firma. Las claves RSA y los parámetros Diffie-Hellman se aceptan si tienen al menos 3072 bits de longitud. - FIPS: Un nivel de política que cumple con los requisitos FIPS140-2. Esto es utilizado internamente por la herramienta de configuración del modo fips, que cambia el sistema Red Hat Enterprise Linux a modo FIPS.

ANEXO A.1.1. CONTRASEÑA DE GRUB

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.6.SEC-RHEL2]** Se restringen accesos en modo recuperación incluido el modo modificación de inicio de GRUB. Se evita que cualquier usuario pueda acceder a los ficheros de configuración de GRUB.
- b) **[A.8.SEC-RHEL7]** Está habilitado el arranque cifrado con contraseña que evite modificaciones. Se protege el inicio de GRUB.

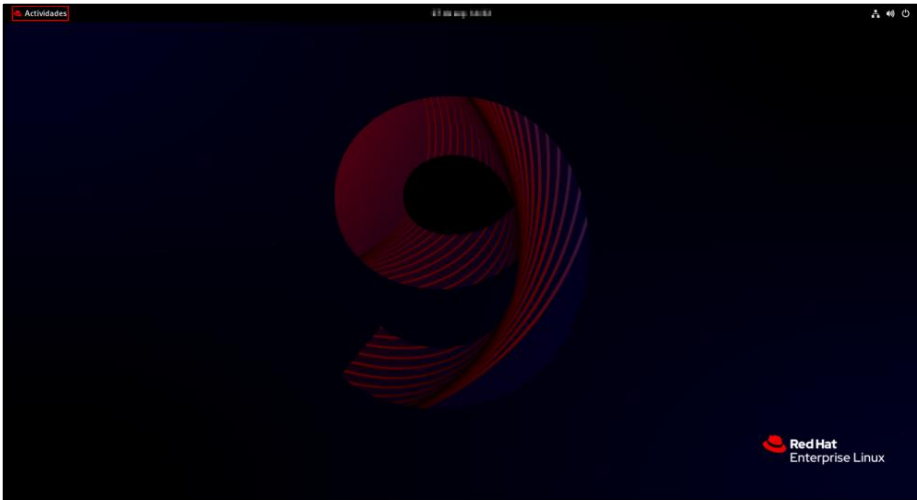

Paso	Descripción
9.	<p>Se procede a continuación a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la carpeta “/Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Acto seguido ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_01-Contraseña_grub.sh</pre> <p>Nota: Por defecto el usuario con permisos para la edición de GRUB es “root”. Deberá adaptar las configuraciones a los parámetros de su organización.</p>
10.	<p>A continuación, introduzca la contraseña deseada que cumpla con los requisitos de seguridad.</p>  <p>Nota: Si se introduce mal la contraseña y las contraseñas no coinciden, no se generará el hash, pero la configuración se exportará vacía al fichero de configuración de grub. Cuando suceda esto, repita este paso desde el inicio antes de continuar con el siguiente punto.</p>

ANEXO A.1.2. CONFIGURACIÓN DE ROOT Y COMPROBACIÓN DE USUARIOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.5.SEC-RHEL1]** Se controlan los permisos de inicio de sesión y suplantación de identidad.
- b) **[A.5.SEC-RHEL5]** Se exige el cambio de contraseña de forma recurrente evitando la suplantación de identidad de los usuarios del sistema.
- c) **[A.6.SEC-RHEL6]** Se eliminan los usuarios innecesarios del sistema.
- d) **[A.11.SEC-RHEL3]** Se dispone de una política de credenciales robusta.

Se procede a configurar las políticas de contraseña del usuario root. Además, se buscan usuarios con un “UID 0”, como cuentas sin contraseñas.

Paso	Descripción
11.	<p>Diríjase a la barra de tareas superior, pulse sobre “Actividades”.</p>  <p>Posteriormente en la fila de la parte inferior seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen.</p> 
12.	<p>Se procede a configurar la política de contraseñas del usuario “root”. Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_02-Usuarios_root_y_sin_contraseña.sh</pre> <pre>----- -- SE CONFIGURA LA CONTRASEÑA SEGURA DE ROOT -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre> <p>El script creará una política de contraseñas para el usuario “root”, y forzará el cambio de contraseña.</p> <pre>Cambiando la contraseña del usuario root. Nueva contraseña: Vuelva a escribir la nueva contraseña:</pre>

Paso	Descripción
	<p>Se mostrará los cambios de política en la contraseña de root.</p> <pre> passwd: todos los tokens de autenticación se actualizaron exitosamente. Último cambio de contraseña : mar 14, 2020 La contraseña caduca : mar 14, 2020 Contraseña inactiva : nunca La cuenta caduca : nunca Número de días mínimo entre cambio de contraseña : 2 Número de días máximo entre cambio de contraseña : 45 Número de días de aviso antes de que caduque la contraseña : 10 </pre>
13.	<p>El script realizará búsquedas de usuarios con “UID 0”, usuarios sin contraseña, y usuarios y/o grupos de sudoers sin uso de contraseñas.</p> <pre> ----- -- SE PROCEDE A BUSCAR USUARIOS CON UID 0 -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... No se detectan usuarios con UID 0. ----- -- SE PROCEDE A BUSCAR USUARIOS SIN CONTRASEÑA -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... No se detectan usuarios sin contraseña. ----- -- SE PROCEDE A BUSCAR USUARIOS/GRUPOS SUDOERS SIN CONTRASEÑA -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... No se detectan usuarios sin contraseña en sudoers. </pre> <p>Si se detecta algún usuario que no cumpla con los requisitos de contraseñas, o con “UID 0” y por ende permisos demasiado elevados y deberán ser modificados o ser eliminados.</p> <p>Nota: Si no conoce el proceso de eliminación de usuarios vaya al anexo “ANEXO A.5.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS”. Deberá adaptar las configuraciones a los parámetros de su organización.</p>

ANEXO A.2. FORTIFICACIÓN DEL KERNEL

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL6]** Se dispone de medidas anti ransomware habilitadas a través de la red. Las configuraciones aplicadas en este paso impiden la posible difusión de software dañino mediante configuraciones sobre directivas de red.
- b) **[A.8.SEC-RHEL4]** Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.

Paso	Descripción
14.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
15.	Se procede a modificar parámetros del kernel, para ello se añadirán ciertas líneas comentadas “#” al fichero “ /etc/sysctl.conf ” para facilitar la adaptación de las configuraciones a las necesidades de su organización.
16.	<p>Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_03-Parametros_del_kernel.sh</pre>
17.	<p>El script alertará de la creación de una copia de seguridad del fichero “/etc/sysctl.conf” y de la carpeta “/etc/sysctl.d” con una marca de tiempo, ya que el script añadirá una configuración que cumpla con los mínimos de seguridad.</p> <pre> --APLICANDO PARÁMETROS DEL KERNEL-- ----- EL SCRIPT GUARDARÁ UNA COPIA DE LOS ARCHIVOS ORIGINALES POR SI SE DESEARA RESTAU RAR CONFIGURACIONES ANTERIORES EN : /etc/sysctl.conf.bak 2018-09-20 11:45:44 /etc/sysctl.d 2018-09-20 11:45:44 NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE FINALICE EN CASO DE DETENCIÓN DEL SCRIPT; VUELVA A EJECUTARLO ANTES DE REINICIAR, HASTA QUE FINALICE EL PROCESO CORRECTAMENTE </pre>
18.	<p>Cuando la configuración predeterminada finalice, pulse “Enter” y se abrirá el fichero de configuración.</p> <pre> Pulse ENTER para continuar o Ctrl + C para cancelar..... >>>>>>>EL PROCESO A FINALIZADO<<<<<<< Se mostrará el fichero /etc/sysctl.conf para su revisión pulse para continuar... </pre>

Paso	Descripción
19.	<p>Se pueden observar las configuraciones de seguridad aplicadas por la ejecución del script. Habilite, deshabilite o añada configuraciones según sus necesidades.</p> <pre> net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv4.conf.default.send_redirects = 0 net.ipv4.conf.default.secure_redirects = 0 net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0 net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1 net.ipv4.icmp_ignore_bogus_error_responses = 1 net.ipv4.icmp_echo_ignore_broadcasts = 1 net.ipv4.tcp_syncookies = 1 fs.suid_dumpable = 0 net.ipv6.conf.default.accept_source_route = 0 net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_ra = 0 net.ipv6.conf.all.accept_ra = 0 net.ipv6.conf.default.accept_redirects = 0 </pre> <p>Cuando llegue al final del documento el script informará que el equipo se va a reiniciar. Guarde los documentos que tenga abiertos y pulse “Enter” para reiniciar.</p>

ANEXO A.3. CONFIGURACIÓN DE SSH

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- [A.5.SEC-RHEL6]** Se hace uso de protocolos seguros para los procesos de autenticación de red.
- [A.5.SEC-RHEL7]** Se controla la inactividad de la sesión de red.
- [A.11.SEC-RHEL2]** Se ha reforzado la seguridad del protocolo SSH. Evitando accesos no autorizados.
- [A.11.SEC-RHEL6]** Sólo se permiten algoritmos de cifrado robustos en accesos al sistema. Reforzando el cifrado de las comunicaciones.

Estas configuraciones refuerzan las medidas ante posibles intentos de suplantación de identidad.

Paso	Descripción
20.	Si ha cerrado la “Terminal” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “Terminal” .
21.	<p>A continuación, se procederá a configurar el servicio SSH. Para ello diríjase al directorio “Scripts”.</p> <pre>\$ cd /Scripts</pre>

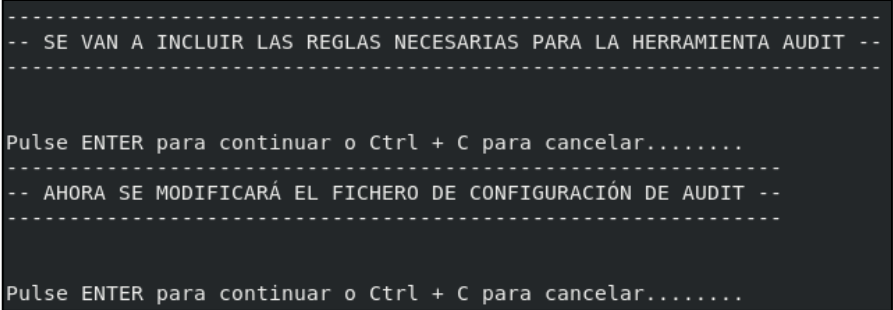
Paso	Descripción
22.	<p>Ejecute el script CCN-STIC-610A22_04-Parametros_SSH.sh.</p> <pre>\$ sudo sh CCN-STIC-610A22_04-Parametros_SSH.sh</pre> <p>Deberá elegir un puerto válido para SSH como se indica por pantalla.</p> <pre> -- MODIFICANDO CONFIGURACION SSH -- ----- ANTES DE COMENZAR SE CREARÁ UN BACKUP DEL FICHERO /etc/ssh/sshd_config CON LA SIGUIENTE NOMENCLATURA /etc/ssh/sshd_config.backup[fecha/hora] NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE EL SCRIPT FINALICE EN CASO DE DETECCIÓN DEL SCRIPT; VUELVA A EJECUTARLO ANTES DE REINICIAR HASTA QUE FINA LICE EL PROCESO CORRECTAMENTE Pulse ENTER para continuar o Ctrl + C para cancelar..... <<introduzca el puerto válido de escucha SSH que desea >> a continuación: </pre> <p>Nota: El puerto que ingrese debe tener un valor válido (superior a un valor de 1024 e inferior a 65535), y se deberá añadir la excepción oportuna en el cortafuegos del sistema (ANEXO A.7.3 PROTECCIÓN DE SERVICIOS DE RED).</p>
23.	<p>A continuación, se mostrará el estado del servicio de SSH.</p> <pre> ● sshd.service - OpenSSH server daemon Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled) Active: active (running) since 2018-04-09 20:41:22 tj; 10min ago Docs: man:sshd(8) man:sshd_config(5) Main PID: 965 (sshd) Tasks: 1 (limit: 23271) Memory: 2.9M CPU: 25ms CGroup: /system.slice/sshd.service └─965 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups" Apr 09 20:41:22 localhost systemd[1]: Starting OpenSSH server daemon... Apr 09 20:41:22 localhost sshd[965]: Server listening on 0.0.0.0 port 56437. Apr 09 20:41:22 localhost systemd[1]: Started OpenSSH server daemon. Apr 09 20:41:22 localhost sshd[965]: Server listening on :: port 56437. </pre> <p>Cierre el mensaje de estado del servicio y ejecución del script pulsando la tecla "ENTER".</p>
24.	<p>Finalmente, se mostrará la configuración de SSH.</p> <pre> Abrir [icon] sshd_config Guardar [icon] x ----- 1 # : sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp \$ 2 3 # This is the sshd server system-wide configuration file. See 4 # sshd_config(5) for more information. 5 6 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin 7 8 # The strategy used for options in the default sshd_config shipped with 9 # OpenSSH is to specify options with their default value where 10 # possible, but leave them commented. Uncommented options override the 11 # default value. 12 13 # If you want to change the port on a SELinux system, you have to tell 14 # SELinux about this change. 15 # semanage port -a -t ssh_port_t -p tcp 56437 16 # 17 Port 56437 18 #AddressFamily any 19 #ListenAddress 0.0.0.0 20 #ListenAddress :: 21 22 Protocol 2 23 24 HostKey /etc/ssh/ssh_host_rsa_key 25 HostKey /etc/ssh/ssh_host_ecdsa_key 26 HostKey /etc/ssh/ssh_host_ed25519_key 27 28 # Ciphers and keying 29 #RekeyLimit default none 30 31 # This system is following system-wide crypto policy. The changes to 32 # crypto properties (Ciphers, MACs, ...) will not have any effect here. 33 # They will be overridden by command-line options passed to the server 34 # on command line. 35 # Please, check manual pages for update-crypto-policies(8) and sshd_config(5). </pre> <p>Nota: Revise los parámetros y adecúelos a las configuraciones de su organización si fuese oportuno.</p>

ANEXO A.4. CONFIGURACIÓN Y PROTECCIÓN DE REGISTROS DE ACTIVIDAD

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.3.SEC-RHEL1]** Se auditan los inicios de sesión.
- b) **[A.3.SEC-RHEL2]** Se controla quien puede acceder a los registros de seguridad y auditoría.
- c) **[A.3.SEC-RHEL3]** Se controla el cambio de hora del sistema.
- d) **[A.3.SEC-RHEL4]** Se controla quién puede generar o modificar reglas de AUDIT.
- e) **[A.3.SEC-RHEL5]** Se ha implementado la auditoría detallada basada en subcategorías.
- f) **[A.3.SEC-RHEL6]** Se garantiza al menos 90 días de registros de actividad.
- g) **[A.8.SEC-RHEL8]** Se audita la descarga de archivos.
- h) **[A.11.SEC-RHEL1]** Se controla el inicio de sesión local en el sistema.
- i) **[A.19.SEC-RHEL1]** Se controla el acceso al árbol de carpetas y ficheros.

En este apartado se aplicarán todas las configuraciones referentes al registro de actividad y auditoría sobre usuarios y modificaciones en el sistema.

Paso	Descripción
25.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
26.	<p>Se procede a configurar la herramienta Audit, se añadirán reglas para la correcta auditoría del sistema, así como la modificación de su fichero de configuración. Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_05-Manipulacion_de_registros_de_actividad.sh</pre>  <p>El script finalizará mostrando las reglas creadas, si no fuera así, vuelva a ejecutar de nuevo el script.</p> <p>Nota: El script añade los parámetros necesarios al fichero de configuración “/etc/audit/audit.conf” para que se generen un máximo de 12 archivos de logs con una capacidad máxima por archivo de 10Mb, lo que crea un total de 120Mb. Cuando alcance el límite, los ficheros de logs rotarán gracias al parámetro “max_log_file_action = ROTATE”.</p>

ANEXO A.5. CONFIGURACION DE USUARIOS Y POLITICAS DE CREDENCIALES

ANEXO A.5.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.6.SEC-RHEL3]** Se limita la shell de usuarios de servicio a `"/bin/false"`.
- b) **[A.6.SEC-RHEL4]** Se restringe el uso de sesiones con usuario `"root"`.
- c) **[A.6.SEC-RHEL6]** Se eliminan los grupos y usuarios innecesarios del sistema.

De esta manera se evita que un atacante pueda iniciar sesión con una cuenta de servicio o una cuenta con permisos de administrador.

Paso	Descripción
27.	Si ha cerrado la "Terminal" en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre "Actividades" y seleccione el icono correspondiente a la "Terminal" .
28.	<p>Se procede a eliminar los usuarios creados por defecto en la instalación y que son innecesarios.</p> <p>Para ello diríjase a la carpeta "Scripts".</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_06-Desinstalar_usuarios_innecesarios.sh</pre> <pre> --DESINSTALANDO USUARIOS INNECESARIOS-- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre> <p>El script iniciará un proceso que deshabilitará los usuarios innecesarios, así como los grupos no necesarios, y cambiará las shells predeterminadas en caso de no estar conformes con los parámetros necesarios de seguridad. No pulse ninguna tecla ni cierre la ventana hasta que el proceso finalice. Ignore los mensajes de pantalla.</p> <pre> usermod: sin cambios Cambiando intérprete de órdenes para root. Se ha cambiado el intérprete de órdenes. Cambiando intérprete de órdenes para nobody. Se ha cambiado el intérprete de órdenes. Cambiando intérprete de órdenes para shutdown. Se ha cambiado el intérprete de órdenes. Cambiando intérprete de órdenes para halt. Se ha cambiado el intérprete de órdenes. </pre>
29.	<p>Si ha detectado que en la actualidad está habilitado un usuario que ya no tiene necesidad de acceder al sistema, puede usar el siguiente comando sin las comillas, siendo NOMBREDEUSUARIO el nombre del usuario candidato para su eliminación.</p> <pre>\$ sudo userdel -r "NOMBREDEUSUARIO"</pre> <p>De igual modo, si ha detectado un grupo que no sea de necesidad para la organización, use el siguiente comando para eliminarlo.</p> <pre>\$ sudo groupdel "NOMBREDEGRUPO"</pre>

Paso	Descripción
30.	<p>Ahora compruebe las “shells” predeterminadas de los usuarios con UID por encima del número 1000 (usuarios normales del sistema). Para ello ejecute el siguiente comando.</p> <pre>\$ sudo awk -F: '{if (\$3 >= 1000) { print \$1 ":" \$3 \$7 } }' /etc/passwd grep -v "^nobody"</pre>
31.	<p>Cuando finalice todas las tareas reinicie el sistema.</p> <pre>\$ sudo shutdown -r now</pre>

ANEXO A.5.2. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.30.SEC-RHEL1]** Existe una política de bloqueo de cuentas ante inicios de sesión incorrectos. Esta medida permite mitigar los ataques de fuerza bruta sobre el sistema.

Paso	Descripción
32.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
33.	<p>Se procederá a configurar el bloqueo de cuentas por intentos fallidos, por medio del módulo pam de seguridad “pam_faillock.so”.</p> <p>Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente script.</p> <pre>\$ sudo sh CCN-STIC-610A22_07-intentos_fallidos.sh</pre> <pre> --BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS-- ----- ANTES DE COMENZAR SE CREARÁ UN BACKUP DE LA CARPETA PAM.D EN EL DIRECTORIO /etc/pam.d_backup[fecha/hora] NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE EL SCRIPT FINALICE EN CASO DE DETECCIÓN DEL SCRIPT; VUELVA A EJECUTARLO ANTES DE REINICIAR HASTA QUE FINALICE EL PROCESO CORRECTAMENTE Pulse ENTER para continuar o Ctrl + C para cancelar..... >>>>>>>>>EL PROCESO A FINALIZADO CORRECTAMENTE<<<<<<<<<< Pulse ENTER y el sistema se reiniciará automáticamente en 1 minuto, guarde los archivos que tenga abiertos antes de continuar..... </pre> <p>El script alertará de la creación de una copia de seguridad de la configuración de los ficheros incluidos en /etc/pam.d/. El script añadirá una configuración que cumpla con los mínimos requisitos de seguridad. Al finalizar el proceso, el sistema se reiniciará para aplicar la configuración.</p>

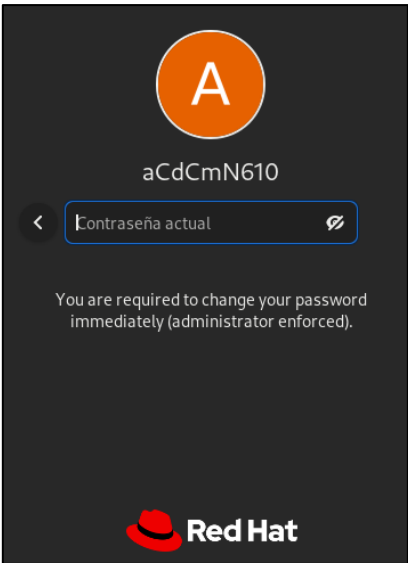
ANEXO A.5.3. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.4.SEC-RHEL1]** Los usuarios estándar no disponen de permisos de administrador local ni se encuentran incluidos en un grupo sudoer.
- b) **[A.5.SEC-RHEL1]** Se controlan los permisos de inicio de sesión y suplantación de identidad.
- c) **[A.5.SEC-RHEL2]** Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.
- d) **[A.5.SEC-RHEL3]** Se controla el acceso a las claves de cifrado.
- e) **[A.5.SEC-RHEL5]** Se exige el cambio de contraseña de forma recurrente.
- f) **[A8.SEC-RHEL1]** Se controla quién puede instalar software en el sistema.
- g) **[A.11.SEC-RHEL3]** Se dispone de una política de credenciales robusta.
- h) **[A.19.SEC-RHEL1]** Se controla el acceso al árbol de carpetas y ficheros
- i) **[A.19.SEC-RHEL2]** Se aplican medidas para la protección de las cuentas.
- j) **[A.19.SEC-RHEL3]** Está habilitado un algoritmo robusto y la complejidad de contraseñas.
- k) **[A.24.SEC-RHEL1]** Se controlan los privilegios que afectan al rendimiento del sistema.
- l) **[A.24.SEC-RHEL2]** Se controla quien puede apagar el sistema.

Todos estos riesgos se pueden mitigar aplicando una segregación de permisos y roles sobre los usuarios para una mayor seguridad. La generación de registros de auditoría sobre todos los accesos, modificaciones, descargas, errores u otros que afecten al sistema, permitirá igualmente la mitigación de estos riesgos.

Paso	Descripción
34.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
35.	<p>Se van a limitar los recursos disponibles para los usuarios, en particular limitar los “volcados de núcleo (core dumps)”. Así mismo se forzará la caducidad de contraseñas para los nuevos usuarios y los ya existentes, su complejidad y los permisos en los directorios “/home” de cada usuario.</p> <p>Nota: Antes de comenzar en este paso, asegúrese de haber cerrado y guardado las aplicaciones y los documentos importantes.</p> <p>Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre>

Paso	Descripción
36.	<p>Ejecute el siguiente script.</p> <pre># sudo sh CCN-STIC-610A22_08-Limites_permisos_y_cad_contraseñas.sh</pre>  <p>Continúa la ejecución del script fortificando los permisos de los directorios “/home” de los usuarios. La realización del script finalizará con un mensaje advirtiéndole que el sistema se reiniciará en 1 minuto. Espere y cierre las aplicaciones que tenga abiertas.</p>
37.	<p>Cuando reinicie el sistema e inicie sesión, aparecerá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos.</p> 
38.	<p>Le pedirá la contraseña actual de nuevo y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.</p>

ANEXO A.5.4. CONFIGURACIÓN SEGURA DE GNOME

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

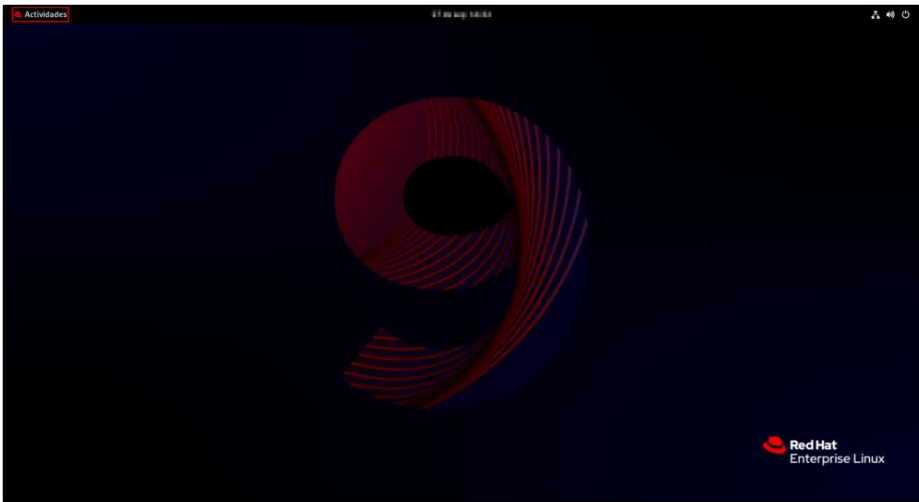
- a) **[A.11.SEC-RHEL4]** Durante el inicio de sesión, el sistema muestra un texto en cumplimiento con las normas o directivas de la organización.
- b) **[A.11.SEC-RHEL7]** Se limita el tiempo de inactividad del GUI.
- c) **[A.11.SEC-RHEL8]** Se muestra un banner disuasorio.
- d) **[A.11.SEC-RHEL9]** Se deshabilita la lista de usuarios.
- e) **[A.11.SEC-RHEL10]** Se deshabilita recordar el historial de ficheros.
- f) **[A.11.SEC-RHEL11]** Se deshabilita combinación de teclas para iniciar el inspector GTK.

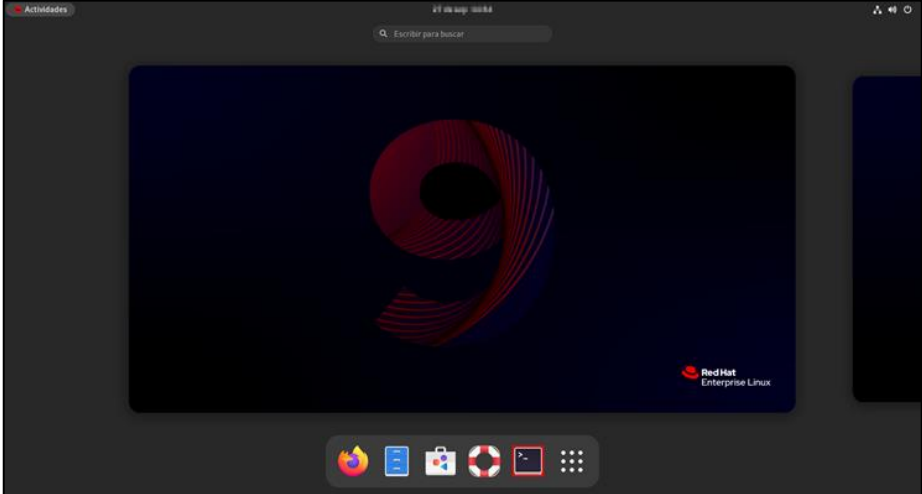
Después de securizar el kernel, proceso realizado en el **ANEXO A.1.2 CONFIGURACIÓN DE ROOT Y COMPROBACIÓN DE USUARIOS**

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- g) **[A.5.SEC-RHEL1]** Se controlan los permisos de inicio de sesión y suplantación de identidad.
- h) **[A.5.SEC-RHEL5]** Se exige el cambio de contraseña de forma recurrente evitando la suplantación de identidad de los usuarios del sistema.
- i) **[A.6.SEC-RHEL6]** Se eliminan los usuarios innecesarios del sistema.
- j) **[A.11.SEC-RHEL3]** Se dispone de una política de credenciales robusta.

Se procede a configurar las políticas de contraseña del usuario root. Además, se buscan usuarios con un “UID 0”, como cuentas sin contraseñas.

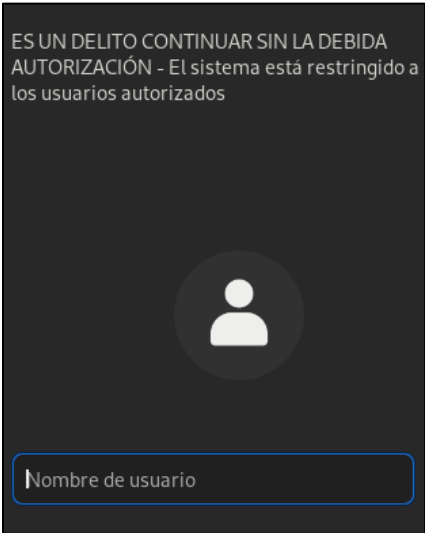
Paso	Descripción
39.	<p>Diríjase a la barra de tareas superior, pulse sobre “Actividades”.</p>  <p>Posteriormente en la fila de la parte inferior seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen.</p>

Paso	Descripción
	
40.	<p>Se procede a configurar la política de contraseñas del usuario “root”. Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_02-Usuarios_root_y_sin_contraseña.sh</pre> <pre>-- SE CONFIGURA LA CONTRASEÑA SEGURA DE ROOT --</pre> <p>Pulse ENTER para continuar o Ctrl + C para cancelar.....</p> <p>El script creará una política de contraseñas para el usuario “root”, y forzará el cambio de contraseña.</p> <pre>Cambiando la contraseña del usuario root. Nueva contraseña: Vuelva a escribir la nueva contraseña:</pre> <p>Se mostrará los cambios de política en la contraseña de root.</p> <pre>passwd: todos los tokens de autenticación se actualizaron exitosamente. Último cambio de contraseña : mar 04, 2020 La contraseña caduca : mar 04, 2020 Contraseña inactiva : nunca La cuenta caduca : nunca Número de días mínimo entre cambio de contraseña : 2 Número de días máximo entre cambio de contraseña : 45 Número de días de aviso antes de que caduque la contraseña : 10</pre>
41.	<p>El script realizará búsquedas de usuarios con “UID 0”, usuarios sin contraseña, y usuarios y/o grupos de sudoers sin uso de contraseñas.</p>

Paso	Descripción
	<pre> -- SE PROCEDE A BUSCAR USUARIOS CON UID 0 -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... No se detectan usuarios con UID 0. ----- -- SE PROCEDE A BUSCAR USUARIOS SIN CONTRASEÑA -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... No se detectan usuarios sin contraseña. ----- -- SE PROCEDE A BUSCAR USUARIOS/GRUPOS SUDOERS SIN CONTRASEÑA -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... No se detectan usuarios sin contraseña en sudoers. </pre> <p>Si se detecta algún usuario que no cumpla con los requisitos de contraseñas, o con “UID 0” y por ende permisos demasiado elevados y deberán ser modificados o ser eliminados.</p> <p>Nota: Si no conoce el proceso de eliminación de usuarios vaya al anexo “ANEXO A.5.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS”. Deberá adaptar las configuraciones a los parámetros de su organización.</p>

FORTIFICACIÓN DEL KERNEL, se deben mitigar los riesgos mediante la aplicación de configuraciones de seguridad en los parámetros de usuario a nivel de entorno gráfico, en caso de que el sistema posea dicho entorno.

Paso	Descripción
42.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.

Paso	Descripción
43.	<p>Se procede a configurar parámetros de seguridad en el escritorio Gnome. Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>\$ sudo sh CCN-STIC-610A22_09-Parametros_gnome.sh</pre> <pre>--CREANDO UN BANNER Y MODIFICANDO PARÁMETROS DE INICIO DE SESIÓN-- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre> <p>Introduzca el Banner deseado acorde con su organización.</p> <pre>--CREANDO UN BANNER Y MODIFICANDO PARÁMETROS DE INICIO DE SESIÓN-- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... <<introduzca el Banner deseado para su organización>> a continuación: ES UN DELITO CONTINUAR SIN LA DEBIDA AUTORIZACION - El sistema esta restringido a los usuarios autorizados</pre>
44.	<p>El script iniciará un proceso que modificará la pantalla de inicio de Red Hat Enterprise Linux 9.0 para que aparezca un mensaje disuasorio (banner) al inicio y solicite usuario y contraseña. Así mismo se configurará un tiempo mínimo de bloqueo según requisitos de seguridad.</p> 

ANEXO A.6. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

ANEXO A.6.1. LIMITACIÓN DE SERVICIOS, DEMONIOS Y HERRAMIENTAS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL4]** Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.
- b) **[A.8.SEC-RHEL9]** Están deshabilitados los compiladores del sistema, de esta manera se evita que un usuario no autorizado pueda desarrollar un malware usando los propios compiladores existentes.

Paso	Descripción
45.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
46.	<p>Se procede a desinstalar programas innecesarios, además se procederá a deshabilitar servicios y demonios innecesarios. Para ello diríjase a la carpeta “Scripts”.</p> <pre>\$ cd /Scripts</pre> <p>Ejecute el siguiente comando e introduzca la contraseña si se le solicita.</p> <pre>\$ sudo sh CCN-STIC-610A22_10-Elementos_innecesarios.sh</pre> <pre> ----- -- SE ELIMINARÁN PROGRAMAS Y DRIVERS INNECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre> <p>Nota: El script está configurado para una instalación de BIOS en modo “Legacy”. Para el correcto funcionamiento del sistema con una configuración de la BIOS en modo UEFI, el sistema establece una partición vfat (/boot/efi). Las particiones con sistemas de archivos que no posean listas de control de acceso como fat32 suponen un riesgo de seguridad y se deben limitar, por tanto, si su sistema no puede proporcionar configuraciones de BIOS legacy, deberá adaptar los parámetros de la guía, así como los scripts, para permitir la citada configuración, no siendo en ningún caso recomendable. El no adaptar correctamente los parámetros puede provocar fallos en el sistema, no siendo motivo de esta guía la configuración de dichos parámetros. En este punto se deshabilitan los sistemas de disco sin lista de control de acceso.</p>

Paso	Descripción
47.	<p>El proceso del script continúa con la desinstalación de paquetes de software no necesarios.</p> <pre> python3-meh-gui noarch 0.47.2-1.el8 @AppStream 24 k python3-ntplib noarch 0.3.3-10.el8 @AppStream 28 k python3-ordered-set noarch 2.0.2-4.el8 @AppStream 15 k python3-pid noarch 2.1.1-7.el8 @AppStream 33 k python3-productmd noarch 1.11-3.el8 @AppStream 241 k python3-pvquality x86_64 1.4.0-9.el8 @anaconda 21 k python3-pyatspi noarch 2.26.0-6.el8 @AppStream 380 k python3-pyparted x86_64 1:3.11.0-13.el8 @AppStream 368 k python3-pytz noarch 2017.2-9.el8 @AppStream 175 k python3-requests-file noarch 1.4.3-5.el8 @AppStream 9.4 k python3-requests-ftp noarch 0.3.1-11.el8 @AppStream 37 k python3-simpleline noarch 1.1.1-2.el8 @AppStream 402 k python3-speechd x86_64 0.8.8-6.el8 @AppStream 194 k satyr x86_64 0.26-2.el8 @AppStream 315 k speech-dispatcher-espeak-ng x86_64 0.8.8-6.el8 @AppStream 110 k tigervnc-license noarch 1.10.1-7.el8 @AppStream 18 k tigervnc-server-minimal x86_64 1.10.1-7.el8 @AppStream 2.7 M xmlrpc-c x86_64 1.51.0-5.el8 @anaconda 610 k xmlrpc-c-client x86_64 1.51.0-5.el8 @anaconda 54 k Resumen de la transacción ===== Eliminar 70 Paquetes Espacio liberado: 81 M ¿Está de acuerdo [s/N]?:</pre> <p>Nota: Deberá adaptar los parámetros a las necesidades de su organización.</p>
48.	<p>Pulse “Enter” para restringir el montaje dinámico de sistemas de archivos.</p> <pre> -- RESTRINGIR EL MONTAJE Y DESMONTAJE DINÁMICO DE SISTEMAS DE ARCHIVOS-- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre>
49.	<p>Se muestra la configuración establecida en “limites_archivos.conf”.</p>  <pre> Abrir limites_archivos.... Guardar x /etc/modprobe.d install cramfs /bin/true install freevxfs /bin/true install jffs2 /bin/true install hfs /bin/true install hfsplus /bin/true install squashfs /bin/true install udf /bin/true #Comentar en caso de instalacion EFI install fat /bin/true #Comentar en caso de instalacion EFI install vfat /bin/true install cifs /bin/true install nfs /bin/true install nfsv3 /bin/true install nfsv4 /bin/true install gfs2 /bin/true install bnep /bin/true install bluetooth /bin/true install btusb /bin/true install net-pf-31 /bin/true no Anchura del tabulador: 8 Ln 1, Col 1 INS</pre> <p>Nota: Para continuar con el proceso, deberá guardar y cerrar el documento si está conforme a los parámetros de su organización.</p>

Paso	Descripción																																																																																																												
50.	<p>Pulse “Enter” para continuar y saldrá el mensaje “Se deshabilitarán y enmascararán demonios y procesos innecesarios”.</p> <div><pre>-- SE DESHABILITARAN Y ENMASCARARÁN DEMONIOS Y PROCESOS INNECESARIOS -- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre></div> <p>Pulse nuevamente “Enter” para continuar con la ejecución. Posteriormente se mostrarán el estado de los servicios y demonios del sistema.</p> <table><thead><tr><th>UNIT FILE</th><th>STATE</th><th>VENDOR PRESET</th></tr></thead><tbody><tr><td>proc-sys-fs-binfmt_misc.automount</td><td>static</td><td>-</td></tr><tr><td>-.mount</td><td>generated</td><td>-</td></tr><tr><td>boot.mount</td><td>generated</td><td>-</td></tr><tr><td>dev-hugepages.mount</td><td>static</td><td>-</td></tr><tr><td>dev-mqueue.mount</td><td>static</td><td>-</td></tr><tr><td>proc-sys-fs-binfmt_misc.mount</td><td>disabled</td><td>disabled</td></tr><tr><td>run-vmblock\x2dfuse.mount</td><td>enabled</td><td>disabled</td></tr><tr><td>sys-fs-fuse-connections.mount</td><td>static</td><td>-</td></tr><tr><td>sys-kernel-config.mount</td><td>static</td><td>-</td></tr><tr><td>sys-kernel-debug.mount</td><td>static</td><td>-</td></tr><tr><td>sys-kernel-tracing.mount</td><td>static</td><td>-</td></tr><tr><td>tmp.mount</td><td>disabled</td><td>disabled</td></tr><tr><td>cups.path</td><td>enabled</td><td>enabled</td></tr><tr><td>insights-client-results.path</td><td>disabled</td><td>disabled</td></tr><tr><td>ostree-finalize-staged.path</td><td>disabled</td><td>disabled</td></tr><tr><td>systemd-ask-password-console.path</td><td>static</td><td>-</td></tr><tr><td>systemd-ask-password-plymouth.path</td><td>static</td><td>-</td></tr><tr><td>systemd-ask-password-wall.path</td><td>static</td><td>-</td></tr><tr><td>session-5.scope</td><td>transient</td><td>-</td></tr><tr><td>accounts-daemon.service</td><td>enabled</td><td>enabled</td></tr><tr><td>alsa-restore.service</td><td>static</td><td>-</td></tr><tr><td>alsa-state.service</td><td>static</td><td>-</td></tr><tr><td>arp-ethers.service</td><td>disabled</td><td>disabled</td></tr><tr><td>atd.service</td><td>enabled</td><td>enabled</td></tr><tr><td>auditd.service</td><td>enabled</td><td>enabled</td></tr><tr><td>autovt@.service</td><td>masked</td><td>disabled</td></tr><tr><td>avahi-daemon.service</td><td>enabled</td><td>enabled</td></tr><tr><td>blk-availability.service</td><td>disabled</td><td>disabled</td></tr><tr><td>bluetooth.service</td><td>enabled</td><td>enabled</td></tr><tr><td>bolt.service</td><td>static</td><td>-</td></tr><tr><td>canberra-system-bootup.service</td><td>disabled</td><td>disabled</td></tr><tr><td>canberra-system-shutdown-reboot.service</td><td>disabled</td><td>disabled</td></tr><tr><td>canberra-system-shutdown.service</td><td>disabled</td><td>disabled</td></tr><tr><td>cni-dhcp.service</td><td>disabled</td><td>disabled</td></tr><tr><td>cockpit-motd.service</td><td>static</td><td>-</td></tr></tbody></table> <div>lines 1-36</div>	UNIT FILE	STATE	VENDOR PRESET	proc-sys-fs-binfmt_misc.automount	static	-	-.mount	generated	-	boot.mount	generated	-	dev-hugepages.mount	static	-	dev-mqueue.mount	static	-	proc-sys-fs-binfmt_misc.mount	disabled	disabled	run-vmblock\x2dfuse.mount	enabled	disabled	sys-fs-fuse-connections.mount	static	-	sys-kernel-config.mount	static	-	sys-kernel-debug.mount	static	-	sys-kernel-tracing.mount	static	-	tmp.mount	disabled	disabled	cups.path	enabled	enabled	insights-client-results.path	disabled	disabled	ostree-finalize-staged.path	disabled	disabled	systemd-ask-password-console.path	static	-	systemd-ask-password-plymouth.path	static	-	systemd-ask-password-wall.path	static	-	session-5.scope	transient	-	accounts-daemon.service	enabled	enabled	alsa-restore.service	static	-	alsa-state.service	static	-	arp-ethers.service	disabled	disabled	atd.service	enabled	enabled	auditd.service	enabled	enabled	autovt@.service	masked	disabled	avahi-daemon.service	enabled	enabled	blk-availability.service	disabled	disabled	bluetooth.service	enabled	enabled	bolt.service	static	-	canberra-system-bootup.service	disabled	disabled	canberra-system-shutdown-reboot.service	disabled	disabled	canberra-system-shutdown.service	disabled	disabled	cni-dhcp.service	disabled	disabled	cockpit-motd.service	static	-
UNIT FILE	STATE	VENDOR PRESET																																																																																																											
proc-sys-fs-binfmt_misc.automount	static	-																																																																																																											
-.mount	generated	-																																																																																																											
boot.mount	generated	-																																																																																																											
dev-hugepages.mount	static	-																																																																																																											
dev-mqueue.mount	static	-																																																																																																											
proc-sys-fs-binfmt_misc.mount	disabled	disabled																																																																																																											
run-vmblock\x2dfuse.mount	enabled	disabled																																																																																																											
sys-fs-fuse-connections.mount	static	-																																																																																																											
sys-kernel-config.mount	static	-																																																																																																											
sys-kernel-debug.mount	static	-																																																																																																											
sys-kernel-tracing.mount	static	-																																																																																																											
tmp.mount	disabled	disabled																																																																																																											
cups.path	enabled	enabled																																																																																																											
insights-client-results.path	disabled	disabled																																																																																																											
ostree-finalize-staged.path	disabled	disabled																																																																																																											
systemd-ask-password-console.path	static	-																																																																																																											
systemd-ask-password-plymouth.path	static	-																																																																																																											
systemd-ask-password-wall.path	static	-																																																																																																											
session-5.scope	transient	-																																																																																																											
accounts-daemon.service	enabled	enabled																																																																																																											
alsa-restore.service	static	-																																																																																																											
alsa-state.service	static	-																																																																																																											
arp-ethers.service	disabled	disabled																																																																																																											
atd.service	enabled	enabled																																																																																																											
auditd.service	enabled	enabled																																																																																																											
autovt@.service	masked	disabled																																																																																																											
avahi-daemon.service	enabled	enabled																																																																																																											
blk-availability.service	disabled	disabled																																																																																																											
bluetooth.service	enabled	enabled																																																																																																											
bolt.service	static	-																																																																																																											
canberra-system-bootup.service	disabled	disabled																																																																																																											
canberra-system-shutdown-reboot.service	disabled	disabled																																																																																																											
canberra-system-shutdown.service	disabled	disabled																																																																																																											
cni-dhcp.service	disabled	disabled																																																																																																											
cockpit-motd.service	static	-																																																																																																											
<p>Nota: Para avanzar en la pantalla de los servicios, pulse “Enter” para avanzar una línea, “Barra espaciadora” para un avance rápido y/o “q” para salir.</p>																																																																																																													
51.	<p>A continuación se bloquean los compiladores del sistema. Con dicho proceso terminará la ejecución del script.</p> <div><pre>-- SE BLOQUEARÁN LOS COMPILADORES DEL SISTEMA -- Pulse ENTER para continuar o Ctrl + C para cancelar..... -- EL EQUIPO SE REINICIARÁ EN 1 MINUTO -- Pulse ENTER para continuar o Ctrl + C para cancelar..... Shutdown scheduled for Mon Aug 14 11:00:00 CEST, use 'shutdown -c' to cancel. >>>>Guarde los documentos que tenga abiertos y espere...<<<<</pre></div>																																																																																																												

ANEXO A.6.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL4]** Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición y la difusión de software dañino mediante instalación, debido a las dependencias de paquetes no requeridos.

Paso	Descripción
52.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”. Ejecute el comando “ cd / ” y pulse la tecla “ Enter ”.
53.	<p>Se procederá a eliminar los antiguos kernel, los paquetes y repositorios huérfanos. Para ello diríjase a la carpeta “Scripts”.</p> <pre>cd /Scripts</pre> <p>Ejecute el siguiente comando.</p> <pre>sudo sh CCN-STIC-610A22_11-Paquetes_huerfanos.sh</pre> <pre>----- --ELIMINANDO PAQUETES HUÉRFANOS-- ----- Pulse ENTER para continuar o Ctrl + C para cancelar....</pre> <p>De ser detectados paquetes huérfanos o dependencias obsoletas, deberá confirmar su eliminación manualmente.</p> <p>Nota: Deberá adaptar las configuraciones a los parámetros de su organización.</p> <p>Pulse “Enter” para comenzar la ejecución del script. Se iniciará un proceso de limpieza de los paquetes “huérfanos”, para ello instalará la herramienta “yum-utils”.</p> <pre>===== Paquete Arquitectura Versión Tam. Repositorio ===== Instalando: yum-utils noarch 4.0.24-4.el9_0 45 k rhel-9-for-x86_64-baseos-rpms Resumen de la transacción ===== Instalar 1 Paquete Tamaño total de la descarga: 45 k Tamaño instalado: 23 k ¿Está de acuerdo [s/N]?: s Descargando paquetes: yum-utils-4.0.24-4.el9_0.noarch.rpm 177 kB/s 45 kB 00:00 ----- Total 173 kB/s 45 kB 00:00 Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs) 2.9 MB/s 3.6 kB 00:00 Importando llave GPG 0xFD431D51: ID usuario: "Red Hat, Inc. (release key 2) <security@redhat.com>" Huella : 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51 Desde : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release ¿Está de acuerdo [s/N]?: s</pre>

Paso	Descripción
	<p>No pulse ninguna tecla ni cierre la ventana hasta que finalice con un mensaje en pantalla de “¡Listo!”.</p> <pre> Última comprobación de caducidad de metadatos hecha hace Actualización de repositorios de Subscription Management. No hay coincidencias para el argumento: Actualización No hay coincidencias para el argumento: de No hay coincidencias para el argumento: repositorios No hay coincidencias para el argumento: Subscription No hay coincidencias para el argumento: Management. No se han seleccionado paquetes para eliminar. Dependencias resueltas. Nada por hacer. ¡Listo! </pre>

ANEXO A.7. CONFIGURACIONES ADICIONALES

El presente apartado recoge aquellas categorías de perfilado de seguridad asociadas a un riesgo concreto las cuales no pueden ser aplicadas, en su mayoría, por medio de configuraciones mediante scripts automatizados. Esto puede deberse a muchos factores, entre ellos el uso de otro software que realiza la misma función o bien debido a que se establecen las medidas que evitan el riesgo por medio otros parámetros y/o configuraciones.

Para estos casos, se desarrolla el presente anexo, en el cual se establecen comentarios sobre las categorías de perfilado de seguridad de nivel intermedio afectadas y se determina un ejemplo de configuración o validación que permita garantizar el aseguramiento de Red Hat Enterprise Linux 9.0 con la premisa de apoyar a los operadores a realizar un correcto aseguramiento.

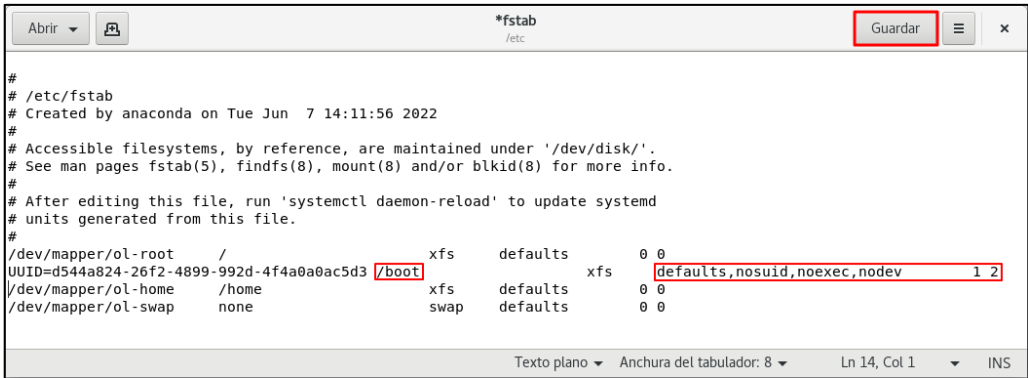
Nota: Las diferentes configuraciones ofrecidas en este anexo son una referencia de las múltiples soluciones que se pueden encontrar para cada uno de los riesgos identificados, es decir, la misma funcionalidad aquí presentada para la mitigación del riesgo puede ser aplicada mediante otros procedimientos, software, o configuraciones. No deben tomarse estas configuraciones como métodos únicos de mitigación.

ANEXO A.7.1. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.4.SEC-RHEL3]** Se modifican los permisos por particiones para evitar, por seguridad, que se puedan modificar y realizar acciones sobre ellas.

Paso	Descripción
54.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
55.	<p>Ejecute el siguiente comando e introduzca la contraseña si se le solicita.</p> <pre>\$ sudo gedit /etc/fstab</pre>

Paso	Descripción
56.	<p>Edite el fichero de configuración con el editor de textos, modificando los permisos de la partición “/boot” para que el resultado sea similar al de la imagen (defaults,nosuid,noexec,nodev 1 2).</p>  <p>Guarde la configuración del fichero pulsando en “Guardar”.</p> <p>Nota: Para instalaciones con una configuración de BIOS en modo “UEFI”, deberá aplicar las mismas configuraciones de seguridad a la partición “/boot/efi”.</p>
57.	<p>Para una correcta aplicación de los valores establecidos en el sistema de ficheros de Red Hat Enterprise Linux, es necesario reiniciar el equipo, asegúrese de guardar todos los documentos y ficheros en uso. Si ha cerrado la “Terminal” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “Terminal”. Ejecute el siguiente comando.</p> <pre>\$ sudo shutdown -r now</pre> <p>Nota: Debe tener en consideración, que para realizar actualizaciones del kernel es posible que deba restablecer los valores de la partición “/boot” a defaults y posteriormente cuando la actualización finalice, revertirlos a los establecidos por esta guía.</p>

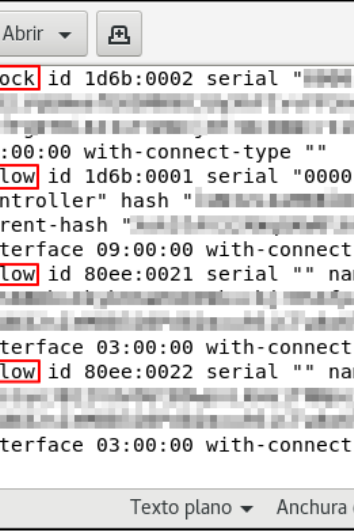
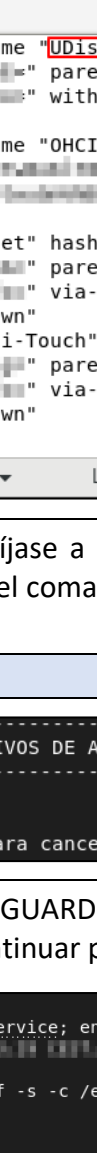
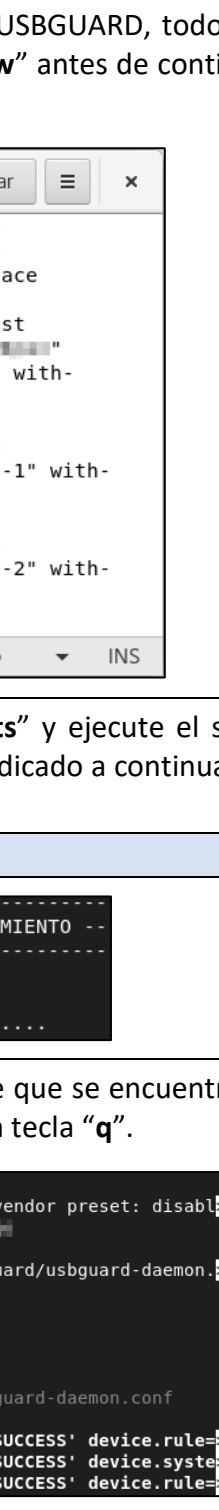
ANEXO A.7.2. LIMITACIÓN DE DISPOSITIVOS EXTRAÍBLES

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- [A.3.SEC-RHEL10]** Se audita toda operación de montaje en el sistema y modificaciones en la memoria de intercambio. Se proporciona trazabilidad para actuación en el caso de incidente por software malicioso.
- [A.11.SEC-RHEL12]** Se deshabilita el auto montaje de dispositivos extraíbles en el sistema.
- [A.15.SEC-RHEL1]** Se controla el uso de medios de almacenamiento extraíbles.
- [A.23.SEC-RHEL1]** Se controla la instalación y uso de cualquier dispositivo conectado al equipo.
- [A.23.SEC-RHEL2]** Se restringe el montaje y desmontaje dinámico de sistemas de archivos.

Se debe mantener un control sobre todas las unidades extraíbles, solo se deben conectar unidades extraíbles autorizadas por la organización.

Paso	Descripción
58.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
59.	Se va a proceder al bloqueo de los dispositivos USB en el sistema. Para tal tarea se utilizará la herramienta “ USBGuard ”. Si no se ha instalado la herramienta ejecute el siguiente comando. <pre>sudo dnf install usbguard</pre>
60.	Se va a proceder configurar la herramienta “ USBGuard ”. El fichero de reglas que gestiona los accesos al sistema de los dispositivos USB (/etc/usbguard/rules.conf) se encuentra con permisos de lectura y escritura solo para el usuario “ root ”. Para ello ingrese con la cuenta de root e introduzca la contraseña cuando así se le solicita. <pre>\$ sudo su</pre>
61.	Inserte todos los dispositivos extraíbles permitidos en el sistema para que se registren en el momento de la generación de políticas. <p>Nota: Todo dispositivo que no se encuentre insertado en este punto, no se registrará y, por tanto, dejará de ser funcional hasta que se generen políticas nuevamente con el nuevo dispositivo, dispositivos tales como un ratón, teclado o medio de almacenamiento, por ejemplo.</p>
62.	Ahora ejecute los siguientes comandos. <pre># usbguard generate-policy > /etc/usbguard/rules.conf</pre> <p>Compruebe que se han generado las políticas de acceso de los dispositivos USB.</p> <pre># cat /etc/usbguard/rules.conf more</pre> <p>Nota: Deberá de corroborar los dispositivos “USB” de su equipo, con los mostrados en el archivo de configuración mostrados. De detectar alguna discrepancia en el fichero “/etc/usbguard/rules.conf”, repita este punto o adapte los parámetros de configuración con los de su organización.</p>
63.	Salga de la sesión de usuario root escribiendo el siguiente comando. <pre># exit</pre>
64.	Ahora se procederá a bloquear todos los dispositivos del sistema y posteriormente habilitar los que sean necesarios. Para ello ejecute el siguiente comando. <pre>\$ sudo sed -i -e 's/allow/block/g' -e 's/allow/block/g' /etc/usbguard/rules.conf</pre>
65.	Se deberán habilitar en este momento los USB necesarios y autorizados para el sistema (teclado, ratón, etc.). Para ello deberá editar el fichero “ /etc/usbguard/rules.conf ” por medio del siguiente comando. <pre>\$ sudo gedit /etc/usbguard/rules.conf</pre>

Paso	Descripción
66.	<p>A partir de la ejecución del script, todo dispositivo que no se encuentre registrado en el fichero de reglas como “allow” o configurado como “block”, se le denegará su acceso. En el ejemplo de la imagen se han permitido todos los dispositivos a excepción del dispositivo USB “UDisk”.</p> <p>Se deberá tener en consideración que, si se han introducido en el sistema los USB autorizados en el momento de la generación de las reglas de USBGUARD, todos los dispositivos deberán estar configurados con el parámetro “allow” antes de continuar con el siguiente paso.</p> 
67.	<p>Posteriormente si se encuentra en otra ruta, diríjase a “Scripts” y ejecute el script “CCN-STIC-610A22-Limitacion_usb.sh” mediante el comando indicado a continuación y pulse “Enter” para continuar.</p> <pre>\$ sudo CCN-STIC-610A22_Limitacion_usb.sh</pre> 
68.	<p>El script le mostrará el estado del servicio de USBGUARD. Fíjese que se encuentra en estado “active (running)” en color verde. Para continuar pulse la tecla “q”.</p> 

El script le informará de su finalización con el mensaje **“>>>>El SCRIPT ha finalizado<<<<”**.

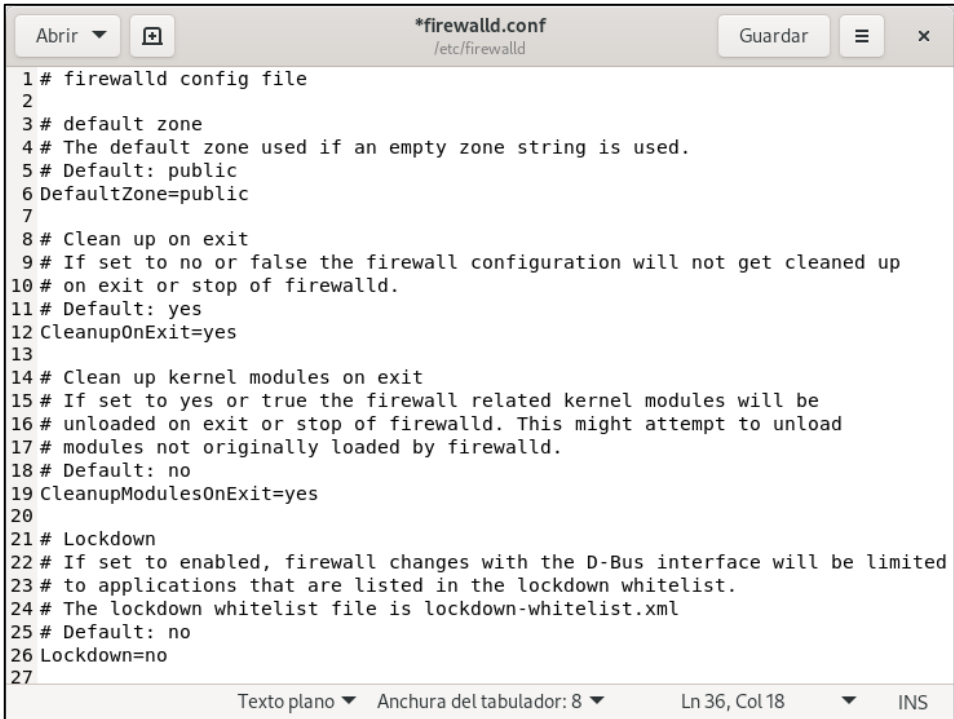
ANEXO A.7.3. PROTECCIÓN DE SERVICIOS DE RED

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL3]** El sistema tiene un firewall local activado.
- b) **[A.11.SEC-RHEL5]** Se controla el acceso al sistema a través de la red.

Se deben aplicar medidas de seguridad para evitar ataques de denegación de servicio a través de protocolos de red, la posible difusión de software malintencionado y establecer niveles de confianza entre las redes o interfaces usadas para las conexiones.

Paso	Descripción
69.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios del ENS en un perfilado intermedio.
70.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “ sudoers ”.
71.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
72.	Se procede a configurar el Firewall de Red Hat 9.0. Para ello es importante que antes de crear las reglas y elegir la zona que más se adecue a su organización se active el servicio de FirewallD. Ejecute el siguiente comando. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">\$ sudo systemctl start firewalld.service && sudo systemctl enable firewalld.service</div> Compruebe su estado con siguiente comando. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">\$ sudo firewall-cmd --state</div>
73.	Para visualizar la zona actual en la cual se encuentra el equipo se usará el siguiente comando. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">\$ sudo firewall-cmd --get-default-zone</div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">[aCdCmN610@RHEL9 ~]\$ sudo firewall-cmd --get-default-zone public</div>
74.	Para conocer qué reglas están asociadas a dicha zona se puede ejecutar el siguiente comando. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">\$ sudo firewall-cmd --list-all</div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">[aCdCmN610@RHEL9 ~]\$ sudo firewall-cmd --list-all public (active) target: default icmp-block-inversion: no interfaces: ens160 sources: services: cockpit dhcpv6-client ssh ports: protocols: forward: yes masquerade: no forward-ports: source-ports: icmp-blocks: rich rules:</div>

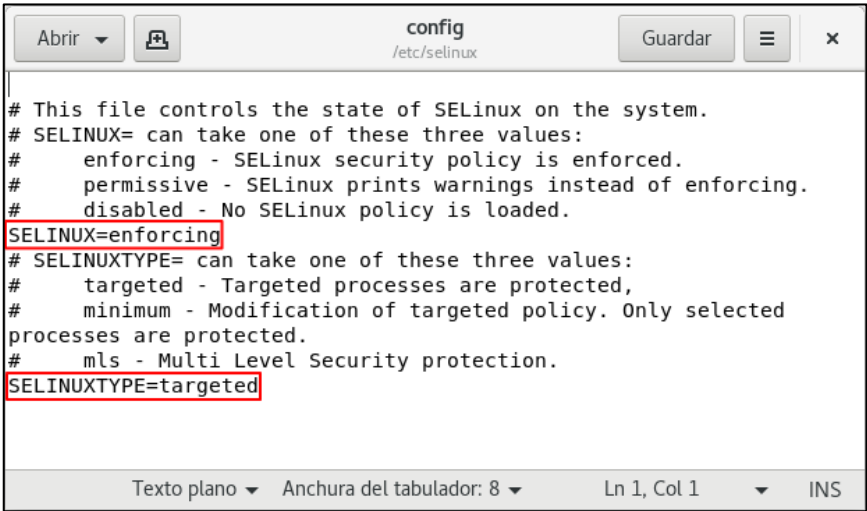
Paso	Descripción
75.	<p>Para comprobar los puertos abiertos en una zona del firewall se usa el siguiente comando, por ejemplo, para ver los puertos abiertos en la zona “internal”.</p> <pre>\$ sudo firewall-cmd --list-ports --zone=internal</pre>
76.	<p>Se recomienda crear una zona propia de la que se tenga control total y pueda cubrir las necesidades de su organización.</p> <p>Para ello ejecute el siguiente comando siendo “NUEVAZONA” el nombre de la zona que se elegirá.</p> <pre>\$ sudo firewall-cmd --new-zone=[NUEVAZONA] --permanent --add-service=[SERVICIO]</pre> <p>Por ejemplo, se añade una zona y se permite un servicio.</p> <pre>\$ sudo firewall-cmd --new-zone=NUEVAZONA --permanent --add-service=ssh</pre>
77.	<p>Para que la zona se refleje reinicie el Firewall con el siguiente comando.</p> <pre>\$ sudo firewall-cmd --reload</pre> <p>Compruebe que está agregada correctamente.</p> <pre>\$ sudo firewall-cmd --permanent --get-zones</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo firewall-cmd --permanent --get-zones block dmz drop external home internal nm-shared public trusted work</pre>
78.	<p>Por último, si quisiera realizar configuraciones adicionales o modificar la zona por defecto, modifique los parámetros necesarios en el fichero de configuración de firewalld (/etc/firewalld/firewalld.conf). Para editar el fichero ejecute el siguiente comando.</p> <pre>\$ sudo gedit /etc/firewalld/firewalld.conf</pre> 

ANEXO A.7.4. CONFIGURACIÓN DE SEGURIDAD – SELINUX

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.6.SEC-RHEL1]** Se refuerza la seguridad de los objetos sensibles del sistema.
- b) **[A.8.SEC-RHEL6]** Se dispone de medidas anti ransomware habilitadas.

Los riesgos mencionados con anterioridad se pueden mitigar mediante el uso de SELinux, módulo de seguridad propio del kernel de Linux.

Paso	Descripción
79.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
80.	<p>Se va a proceder a activar SELinux y configurarlo para que registre los eventos del sistema y aplique las políticas de seguridad. Edite el fichero de configuración “/etc/selinux/config” y modifique los siguientes parámetros: SELINUX=Enforcing, SELINUXTYPE=targeted.</p> <pre>\$ sudo gedit /etc/selinux/config</pre>  <p>Nota: Se comentan a continuación algunos parámetros del fichero de configuración:</p> <ul style="list-style-type: none"> - SELINUX=enforcing: La opción SELINUX pone el modo en el que inicia SELinux. SELinux tiene tres modos: obligatorio (enforcing), permisivo (permissive) y deshabilitado (disabled). Cuando se usa modo obligatorio, la política de SELinux es aplicada y SELinux deniega el acceso basándose en las reglas de políticas de SELinux. Los mensajes de denegación se guardan. Cuando se usa modo permisivo, la política de SELinux no es obediente. Los mensajes son guardados. SELinux no deniega el acceso, pero se guardan las denegaciones de acciones que hubieran sido denegadas si SELinux estuviera en modo obediente. Cuando se usa el modo deshabilitado, SELinux está deshabilitado (el módulo de SELinux no se registra con el kernel de Linux). - SELINUXTYPE=targeted: La opción SELINUXTYPE selecciona la política a usar por SELinux. La política Destinada es la predeterminada. Cambie esta opción si quiere usar la política MLS. Para usar la política MLS, instale el paquete selinux-policy-mls; configure SELINUXTYPE=mls en /etc/selinux/config; y reinicie su sistema.

Paso	Descripción
81.	<p>Para comprobar el estado de SELinux ejecute los siguientes comandos.</p> <pre>\$ sudo getenforce</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo getenforce Enforcing</pre> <pre>\$ sudo sestatus</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo sestatus SELinux status: enabled SELinuxfs mount: /sys/fs/selinux SELinux root directory: /etc/selinux Loaded policy name: targeted Current mode: enforcing Mode from config file: enforcing Policy MLS status: enabled Policy deny_unknown status: allowed Memory protection checking: actual (secure) Max kernel policy version: 33</pre> <p>Compruebe que SELinux se encuentre configurado como “enforcing”, “enabled” y “targeted”. En caso contrario repita los pasos anteriores.</p>

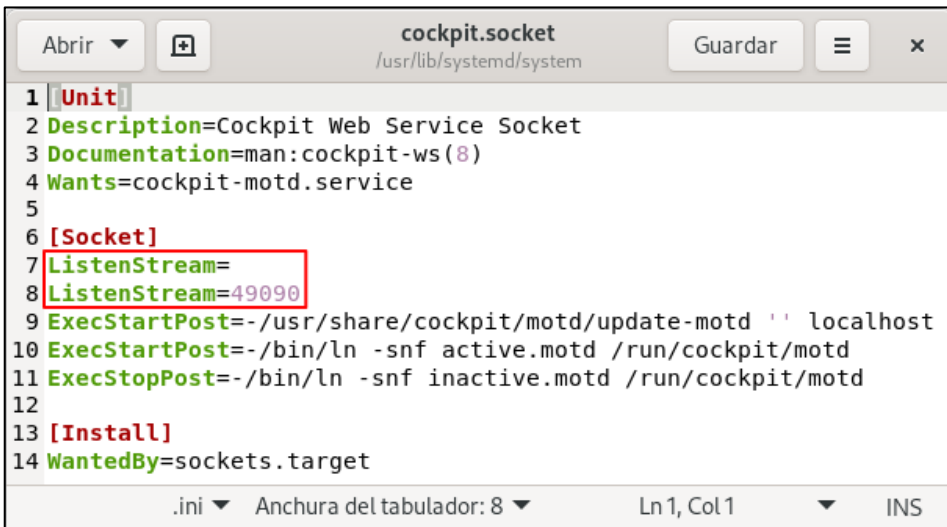
ANEXO A.7.5. INTERFAZ WEB COCKPIT

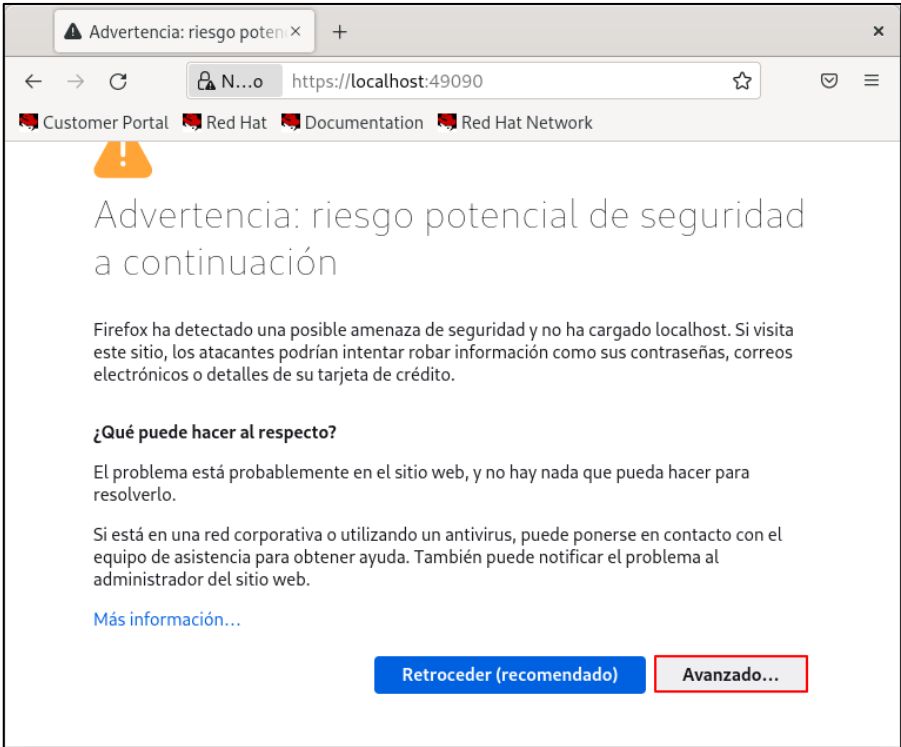
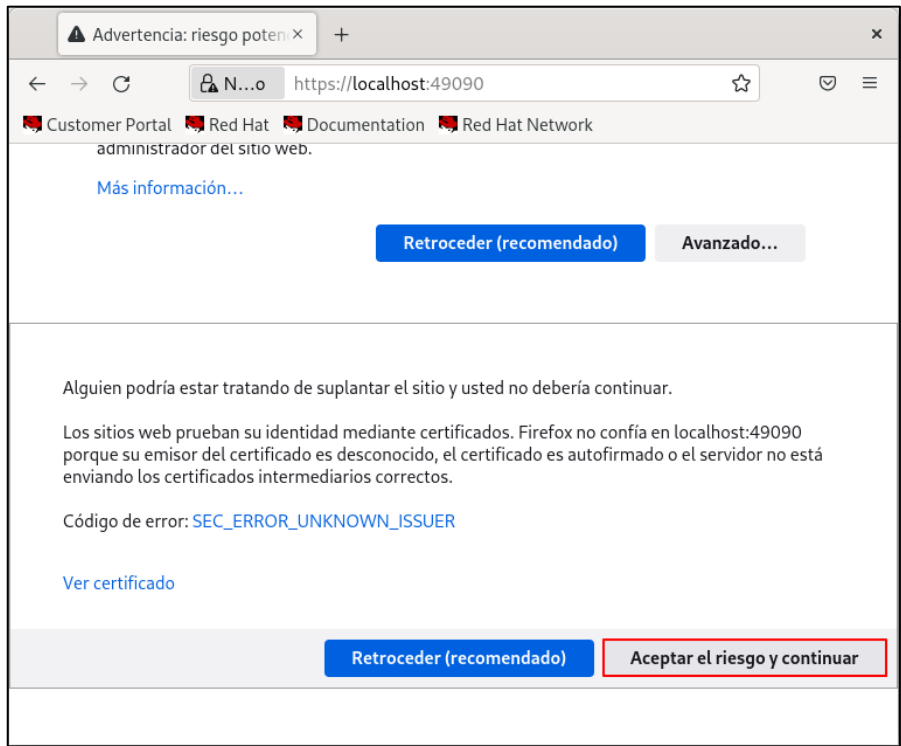
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.11.SEC-RHEL6]** Sólo se permiten algoritmos de cifrado robustos en accesos al sistema.

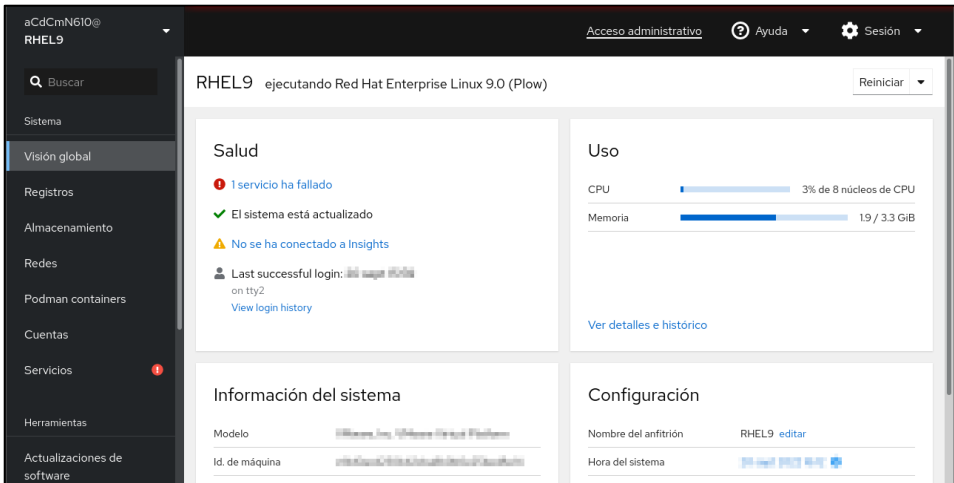
Se deben configurar algoritmos robustos y evitar el uso de puertos conocidos o por defecto para el uso de las comunicaciones, y así mitigar la interceptación de la información.

Paso	Descripción
82.	Se procede a configurar el entorno web de administración cockpit de forma segura. Diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y en la columna de la izquierda seleccione el icono correspondiente a la terminal.
83.	<p>Ejecute el siguiente comando para habilitar la funcionalidad cockpit.</p> <pre>\$ sudo systemctl enable --now cockpit.socket</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo systemctl enable --now cockpit.socket Created symlink /etc/systemd/system/sockets.target.wants/cockpit.socket → /usr/lib/systemd/system/cockpit.socket.</pre>
84.	<p>Compruebe el puerto de escucha de cockpit por medio del siguiente comando.</p> <pre>\$ grep -i listen /usr/lib/systemd/system/cockpit.socket</pre> <pre>[aCdCmN610@RHEL9 ~]\$ grep -i listen /usr/lib/systemd/system/cockpit.socket ListenStream=9090</pre>

Paso	Descripción
85.	<p>Para modificar el puerto de escucha al que más convenga para su organización, ejecute el siguiente comando y edite el fichero “cockpit.socket”. Modifique el campo “ListenStream” por el valor correspondiente al nuevo puerto de escucha dejando el mismo parámetro justo encima sin valor, tal y como se muestra en la siguiente imagen. Cierre y guarde el fichero cuando finalice.</p> <pre>\$ sudo gedit /usr/lib/systemd/system/cockpit.socket</pre>  <pre> 1 [Unit] 2 Description=Cockpit Web Service Socket 3 Documentation=man:cockpit-ws(8) 4 Wants=cockpit-motd.service 5 6 [Socket] 7 ListenStream= 8 ListenStream=49090 9 ExecStartPost=-/usr/share/cockpit/motd/update-motd ' ' localhost 10 ExecStartPost=-/bin/ln -snf active.motd /run/cockpit/motd 11 ExecStopPost=-/bin/ln -snf inactive.motd /run/cockpit/motd 12 13 [Install] 14 WantedBy=sockets.target </pre>
86.	<p>Ejecute los siguientes comandos para que SELinux y firewalld permitan el uso del puerto elegido por la organización para el uso de la interfaz web.</p> <pre>\$ sudo semanage port -a -t websm_port_t -p tcp [PUERTO ELEGIDO]</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo semanage port -a -t websm_port_t -p tcp 49090</pre> <pre>\$ sudo firewall-cmd --permanent --zone=[ZONA HABILITADA] --add-port=[PUERTO ELEGIDO]/[PROTOCOLO]</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo firewall-cmd --permanent --zone=public --add-port=49090/tcp success</pre>
87.	<p>Deberá reiniciar el demonio y comprobar de nuevo el puerto de escucha. Para ello ejecute los siguientes comandos. Introduzca la contraseña si se le solicita.</p> <pre>\$ sudo systemctl daemon-reload & sudo systemctl restart cockpit.service</pre> <pre>\$ sudo systemctl enable --now cockpit.socket</pre> <pre>\$ grep -i listen /usr/lib/systemd/system/cockpit.socket</pre> <pre>[aCdCmN610@RHEL9 ~]\$ grep -i listen /usr/lib/systemd/system/cockpit.socket ListenStream= ListenStream=49090</pre>

Paso	Descripción
88.	<p>Diríjase a la siguiente URL https://localhost:[PUERTO Elegido]. Allí se le advertirá del riesgo potencial de seguridad puesto que el certificado es autogenerado por el sistema. Pulse sobre el botón “Avanzado...” para continuar y desplácese a la parte inferior de la página.</p> 
89.	<p>Pulse sobre el botón “Aceptar el riesgo y continuar”.</p> 

Paso	Descripción
90.	<p>Se mostrará el interfaz de inicio de cockpit, donde deberá introducir las credenciales de su usuario y pulsar en el botón “Iniciar sesión”.</p>
91.	<p>No deberá almacenar contraseñas en el navegador para realizar el inicio de sesión en cockpit.</p>

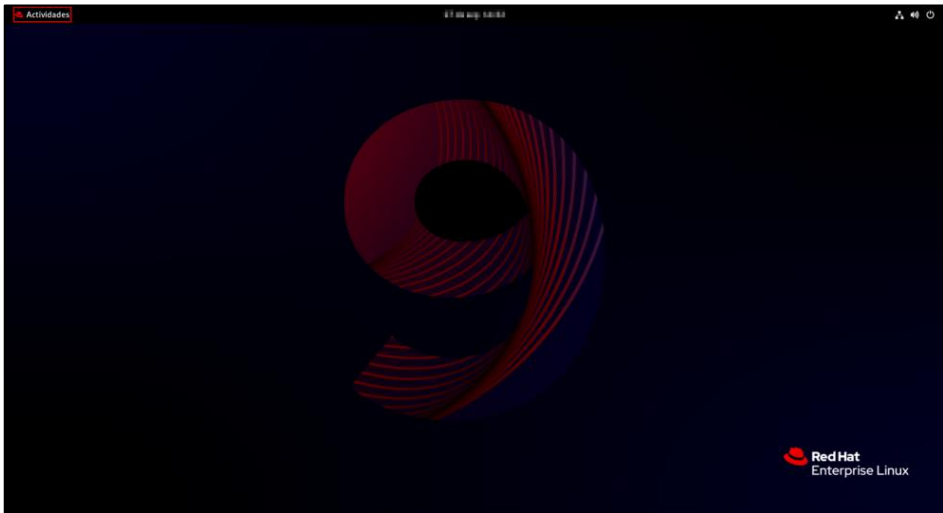
Paso	Descripción
92.	<p>Se mostrará el panel de cockpit para la administración y monitorización del sistema.</p> 

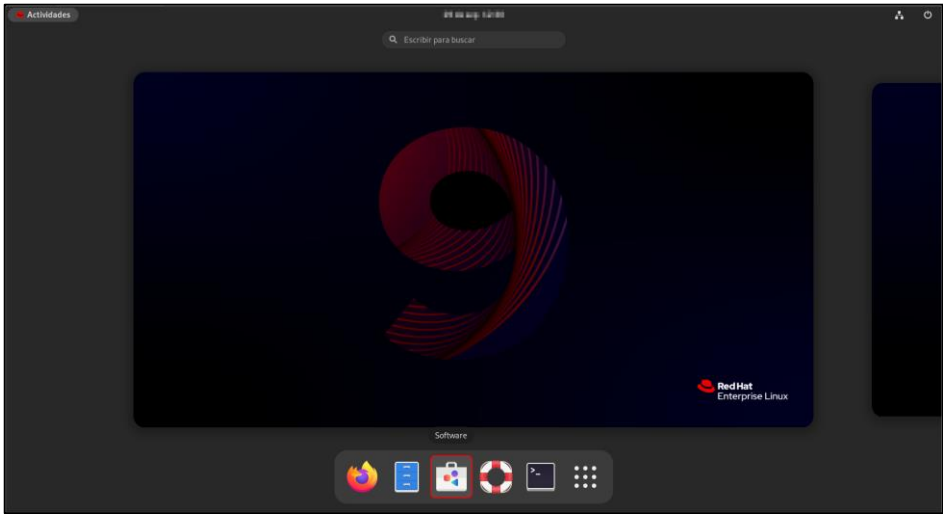
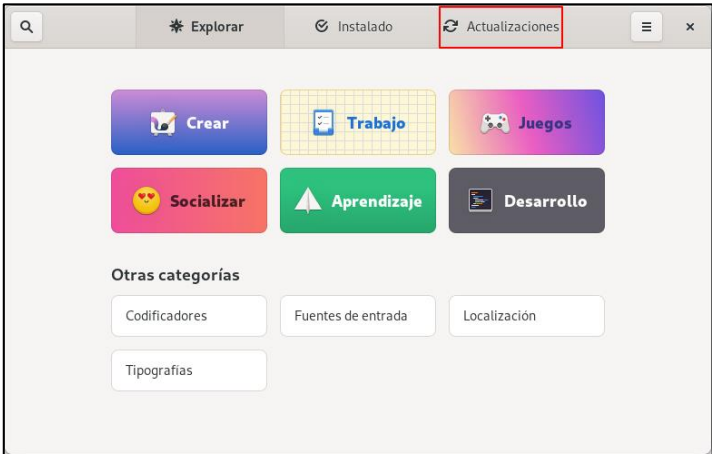
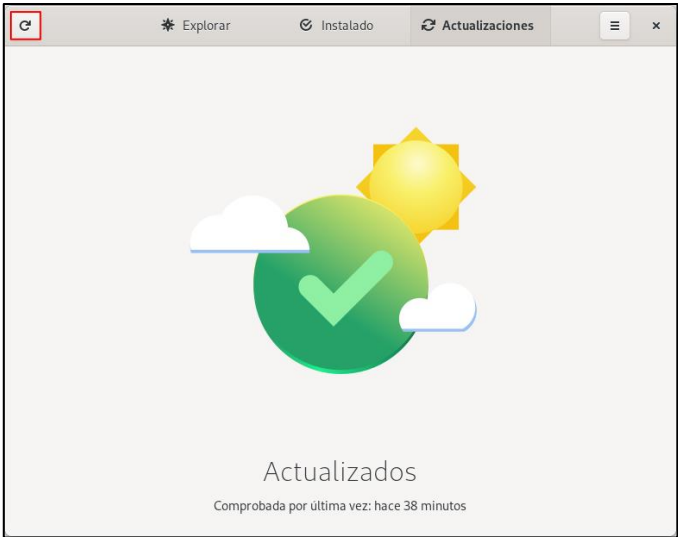
ANEXO A.7.6. APLICACIÓN DE ACTUALIZACIONES

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL2]** El sistema operativo está actualizado.

Se debe disponer un sistema operativo actualizado que disponga de todos los parches y actualizaciones ofreciendo así una mayor seguridad.

Paso	Descripción
93.	<p>Diríjase a la barra de tareas superior, pulse sobre “Actividades”.</p> 

Paso	Descripción
	<p>Posteriormente seleccione el icono correspondiente a “Software”.</p> 
94.	<p>Una vez iniciada la aplicación, pulse sobre la pestaña “Actualizaciones”.</p> 
95.	<p>Pulse sobre el botón de la flecha de recargar. Comprobará si hay más actualizaciones, cuando finalice, si existen actualizaciones, pulse en el botón “Descargar...”.</p> 

ANEXO A.7.7. INSTALACIÓN DE ANTIVIRUS

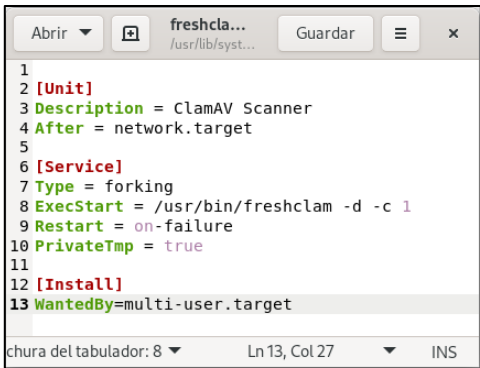
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.4.SEC-RHEL2]** El sistema tiene un antivirus y éste está actualizado.

El sistema debe disponer de un antivirus para poder alertar en caso de la existencia de software o archivos maliciosos.

Nota: En el ejemplo mostrado a continuación se ha procedido a la instalación de ClamAV como una de las posibles soluciones disponibles para la mitigación de este riesgo. Cada organización deberá valorar la solución a implementar.

Paso	Descripción
96.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
97.	<p>A continuación, con el siguiente comando se descargará el antivirus, en este caso ClamAV.</p> <pre>\$ sudo dnf install clamav clamav-data clamav-devel clamav-filesystem clamav-update clamd</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo dnf install clamav clamav-data clamav-devel clamav-filesystem clamav-update clamd Actualización de repositorios de Subscription Management. Última comprobación de caducidad de metadatos hecha hace 10 minutos. Dependencias resueltas. ===== Paquete Arq. Versión Repositorio Tam. ===== Instalando: clamav x86_64 0.103.7-1.el9 epel 2.3 M clamav-data noarch 0.103.7-1.el9 epel 218 M clamav-devel x86_64 0.103.7-1.el9 epel 26 k clamav-filesystem noarch 0.103.7-1.el9 epel 19 k clamav-update x86_64 0.103.7-1.el9 epel 94 k clamd x86_64 0.103.7-1.el9 epel 96 k Instalando dependencias: clamav-lib x86_64 0.103.7-1.el9 epel 821 k libprelude x86_64 5.2.0-9.el9 epel 330 k openssl-devel x86_64 1:3.0.1-41.el9_0 rhel-9-for-x86_64-appstream-rpms 4.1 M Resumen de la transacción ===== Instalar 9 Paquetes Tamaño total de la descarga: 226 M Tamaño instalado: 404 M ¿Está de acuerdo [s/N]?:</pre>
98.	<p>Se continúa configurando SELinux para ClamAV.</p> <pre>\$ sudo setsebool -P antivirus_can_scan_system 1 \$ sudo setsebool -P clamd_use_jit 1</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo setsebool -P antivirus_can_scan_system 1 [aCdCmN610@RHEL9 ~]\$ sudo setsebool -P clamd_use_jit 1</pre>

Paso	Descripción
99.	<p>Se buscan actualizaciones del propio antivirus con el siguiente comando.</p> <pre>\$ sudo freshclam</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo freshclam ClamAV update process started at Mon Aug 14 12:54:12 2023 daily database available for update (local version: 26673, remote version: 26674) Current database is 1 version behind. Downloading database patch # 26674... Time: 0.3s, ETA: 0.0s [=====] 12.94KiB/12.94KiB Testing database: '/var/lib/clamav/tmp.1de37f0883/clamav-5e13a4b99abccba785f959c4a 2c34c92.tmp-daily.cld' ... Database test passed. daily.cld updated (version: 26674, sigs: 2005852, f-level: 90, builder: raynman) main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr) bytecode.cvd database is up-to-date (version: 333, sigs: 92, f-level: 63, builder: awillia2)</pre>
100.	<p>Se finaliza con la configuración del demonio de ejecución de ClamAV.</p> <pre>\$ sudo sed -i 's/#LocalSocket \/run/LocalSocket \run/g' /etc/clamd.d/scan.conf</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo sed -i 's/#LocalSocket \run/LocalSocket \run/g' /etc/clamd.d/scan.conf</pre>
101.	<p>Se crea un nuevo fichero en el que se introducirá la nueva configuración.</p> <pre>\$ sudo gedit /usr/lib/systemd/system/freshclam.service</pre>  <pre>1 [Unit] 2 3 Description = ClamAV Scanner 4 After = network.target 5 6 [Service] 7 Type = forking 8 ExecStart = /usr/bin/freshclam -d -c 1 9 Restart = on-failure 10 PrivateTmp = true 11 12 [Install] 13 WantedBy=multi-user.target</pre>
102.	<p>Por último, se habilitan y ejecutan los servicios del antivirus.</p> <pre>\$ sudo systemctl start clamd@scan \$ sudo systemctl start freshclam</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo systemctl start clamd@scan [aCdCmN610@RHEL9 ~]\$ sudo systemctl start freshclam</pre> <pre>\$ sudo systemctl enable clamd@scan \$ sudo systemctl enable freshclam</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo systemctl enable clamd@scan Created symlink /etc/systemd/system/multi-user.target.wants/clamd@scan.service → /usr/lib/systemd/system/clamd@.service. [aCdCmN610@RHEL9 ~]\$ sudo systemctl enable freshclam Created symlink /etc/systemd/system/multi-user.target.wants/freshclam.service → /usr/lib/systemd/system/freshclam.service.</pre>

Paso	Descripción
103.	<p>Se comprueba que los servicios se estén ejecutando correctamente.</p> <pre>\$ sudo systemctl status clamd@scan</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo systemctl status clamd@scan ● clamd@scan.service - clamd scanner (scan) daemon Loaded: loaded (/usr/lib/systemd/system/clamd@.service; enabled; vendor pre Active: active (running) since 2023-08-11 11:11:11 CEST; 45s ago Docs: man:clamd(8) man:clamd.conf(5) https://www.clamav.net/documents/ Main PID: 1108 (clamd) Tasks: 2 (limit: 21568) Memory: 1.5G CPU: 30.014s CGroup: /system.slice/system-clamd.slice/clamd@scan.service └─1108 /usr/sbin/clamd -c /etc/clamd.d/scan.conf</pre> <pre>\$ sudo systemctl status freshclam</pre> <pre>[aCdCmN610@RHEL9 ~]\$ sudo systemctl status freshclam ● freshclam.service - ClamAV Scanner Loaded: loaded (/usr/lib/systemd/system/freshclam.service; enabled; vendor Active: active (running) since 2023-08-11 11:11:11 CEST; 1min 55s ago Main PID: 1115 (freshclam) Tasks: 1 (limit: 21568) Memory: 4.9M CPU: 328ms CGroup: /system.slice/freshclam.service └─1115 /usr/bin/freshclam -d -c 1</pre>

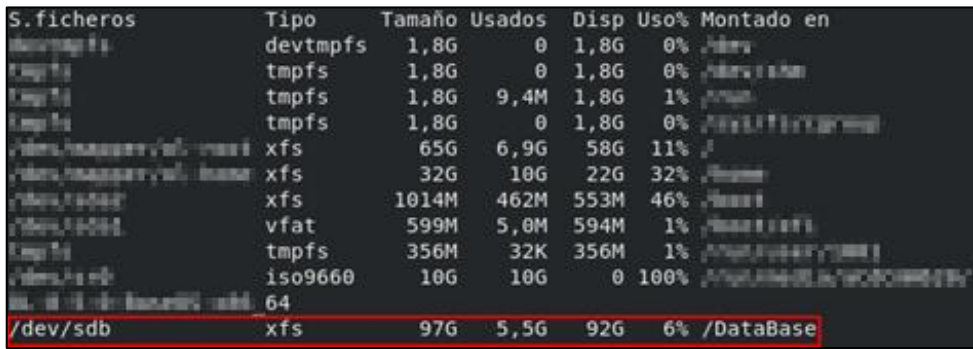
ANEXO A.7.8. RESPALDO DE ARCHIVOS CON SISTEMA DE FICHEROS XFS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL6]** Se dispone de medidas anti ransomware habilitadas.

Este riesgo se puede mitigar realizando copias de seguridad sobre los archivos del sistema permitiendo, de este modo, una restauración de la información en caso de incidente disruptivo.

Paso	Descripción
104.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.

Paso	Descripción
105.	<p>Se procede a realizar, a modo de ejemplo, un respaldo de archivos utilizando las herramientas del sistema de ficheros “XFS”. Dicho sistema de ficheros es utilizado por defecto en las instalaciones de los sistemas Red Hat Enterprise Linux. Para tal cometido ejecute el siguiente comando para localizar la unidad a la cual se va a realizar el respaldo.</p> <pre>\$ df -hT</pre>  <p>Nota: La organización deberá realizar un respaldo de los archivos necesarios para la correcta recuperación de la funcionalidad del servidor, en caso de ser necesario.</p>
106.	<p>Para realizar un respaldo de ficheros, como el proceso se puede demorar, y para respetar la integridad del sistema a respaldar, se va a proceder a “congelar” el uso del sistema de ficheros XFS, el cual se va a respaldar.</p> <pre>\$ sudo xfs_freeze -f /DataBase</pre> <p>Nota: Los ficheros a los que se les aplica “xfs_freeze”, se encuentran en un modo de consulta (read-only), quedando pospuestas todas las modificaciones y entradas de datos hasta que se revierta el estado de “congelado”, momento en el que se aplicarán los cambios. Para realizar los archivos de respaldo, las unidades se deben encontrar o desmontadas o “congeladas”.</p>
107.	<p>Se procede a realizar el respaldo inicial del sistema de archivos seleccionado, a un fichero. Para tal proceso se utiliza la herramienta “xfsdump”. Inserte el siguiente comando en la terminal.</p> <pre>\$ sudo xfsdump -l [NIVEL_DE_RESPALDO] -f [UBICACIÓN_FICHERO_RESPALDO] [SISTEMA_A_RESPALDAR]</pre> <p>Nota: Los respaldos creados por la herramienta xfsdump son iniciales, otorgándole el valor de “0” a la opción “-l” o incrementales, dando valores del 1 al 9. Deberá adaptar las configuraciones a los parámetros de su organización.</p>

Paso	Descripción
108.	<p>A continuación, la salida del comando pedirá insertar el nombre de una etiqueta a la sesión de volcado y otro para los medios de la unidad.</p> <pre> xfsdump: using file dump (drive_simple) strategy xfsdump: version 3.1.8 (dump format 3.0) - type ^C for status and control ===== dump label dialog ===== please enter label for this dump session (timeout in 300 sec) -> Backup_Base_de_datos session label entered: "Backup_Base_de_datos" ----- end dialog ----- xfsdump: level 0 dump of localhost.localdomain:/DataBase xfsdump: dump date: 16 Dec 2016 16:27:43 xfsdump: session id: 401a5407-a048-45ae-97e4-9157a9284719 xfsdump: session label: "Backup_Base_de_datos" xfsdump: ino map phase 1: constructing initial dump list xfsdump: ino map phase 2: skipping (no pruning necessary) xfsdump: ino map phase 3: skipping (only one dump stream) xfsdump: ino map construction complete xfsdump: estimated dump size: 5133849216 bytes ===== media label dialog ===== please enter label for media in drive 0 (timeout in 300 sec) -> /DataBase media label entered: "/DataBase" ----- end dialog ----- </pre>
109.	<p>El comando concluirá mostrando los datos del proceso.</p> <pre> xfsdump: creating dump session media file 0 (media 0, file 0) xfsdump: dumping ino map xfsdump: dumping directories xfsdump: dumping non-directory files xfsdump: ending media file xfsdump: media file size 5135102576 bytes xfsdump: dump size (non-dir files) : 5134993064 bytes xfsdump: dump complete: 90 seconds elapsed xfsdump: Dump Summary: xfsdump: stream 0 OK (success) xfsdump: Dump Status: SUCCESS </pre>
110.	<p>Revierta al estado original del medio al que realizó el respaldo, con la siguiente sentencia.</p> <pre>\$ sudo xfs_freeze -u /DataBase</pre>

ANEXO A.7.9. RESTAURACIÓN DE ARCHIVOS DE RESPALDO

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.8.SEC-RHEL6]** Se dispone de medidas anti ransomware habilitadas.

Los incidentes que afecten a la disponibilidad del sistema pueden ser mitigados mediante la restauración satisfactoria de las copias de seguridad generadas previas al incidente, que permitan restablecer dicha disponibilidad del sistema.

Paso	Descripción																																																																																											
111.	Se procede a restaurar un archivo de respaldo creado con la herramienta “ xfsdump ”. Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.																																																																																											
112.	<div>Compruebe que el medio en el que va a realizar la restauración de los archivos de respaldo posee un sistema de ficheros “XFS”.</div> <div><pre>\$ df -hT</pre><table><thead><tr><th>S.ficheros</th><th>Tipo</th><th>Tamaño</th><th>Usados</th><th>Disp</th><th>Uso%</th><th>Montado en</th></tr></thead><tbody><tr><td>/dev/mapper/rl-root</td><td>devtmpfs</td><td>1,8G</td><td>0</td><td>1,8G</td><td>0%</td><td>/dev</td></tr><tr><td>/dev/fda</td><td>tmpfs</td><td>1,8G</td><td>0</td><td>1,8G</td><td>0%</td><td>/dev/fda</td></tr><tr><td>/dev/fda</td><td>tmpfs</td><td>1,8G</td><td>9,4M</td><td>1,8G</td><td>1%</td><td>/tmp</td></tr><tr><td>/dev/fda</td><td>tmpfs</td><td>1,8G</td><td>0</td><td>1,8G</td><td>0%</td><td>/dev/fda</td></tr><tr><td>/dev/mapper/rl-root</td><td>xfs</td><td>65G</td><td>6,9G</td><td>58G</td><td>11%</td><td>/</td></tr><tr><td>/dev/mapper/rl-home</td><td>xfs</td><td>32G</td><td>10G</td><td>22G</td><td>32%</td><td>/home</td></tr><tr><td>/dev/sda2</td><td>xfs</td><td>1014M</td><td>462M</td><td>553M</td><td>46%</td><td>/DataBase</td></tr><tr><td>/dev/sda1</td><td>vfat</td><td>599M</td><td>5,0M</td><td>594M</td><td>1%</td><td>/boot/efi</td></tr><tr><td>/dev/fda</td><td>tmpfs</td><td>356M</td><td>32K</td><td>356M</td><td>1%</td><td>/tmp</td></tr><tr><td>/dev/sda3</td><td>iso9660</td><td>10G</td><td>10G</td><td>0</td><td>100%</td><td>/mnt/iso</td></tr><tr><td>/dev/sda4</td><td>64</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>/dev/sdb</td><td>xfs</td><td>97G</td><td>5,5G</td><td>92G</td><td>6%</td><td>/DataBase</td></tr></tbody></table></div>	S.ficheros	Tipo	Tamaño	Usados	Disp	Uso%	Montado en	/dev/mapper/rl-root	devtmpfs	1,8G	0	1,8G	0%	/dev	/dev/fda	tmpfs	1,8G	0	1,8G	0%	/dev/fda	/dev/fda	tmpfs	1,8G	9,4M	1,8G	1%	/tmp	/dev/fda	tmpfs	1,8G	0	1,8G	0%	/dev/fda	/dev/mapper/rl-root	xfs	65G	6,9G	58G	11%	/	/dev/mapper/rl-home	xfs	32G	10G	22G	32%	/home	/dev/sda2	xfs	1014M	462M	553M	46%	/DataBase	/dev/sda1	vfat	599M	5,0M	594M	1%	/boot/efi	/dev/fda	tmpfs	356M	32K	356M	1%	/tmp	/dev/sda3	iso9660	10G	10G	0	100%	/mnt/iso	/dev/sda4	64						/dev/sdb	xfs	97G	5,5G	92G	6%	/DataBase
S.ficheros	Tipo	Tamaño	Usados	Disp	Uso%	Montado en																																																																																						
/dev/mapper/rl-root	devtmpfs	1,8G	0	1,8G	0%	/dev																																																																																						
/dev/fda	tmpfs	1,8G	0	1,8G	0%	/dev/fda																																																																																						
/dev/fda	tmpfs	1,8G	9,4M	1,8G	1%	/tmp																																																																																						
/dev/fda	tmpfs	1,8G	0	1,8G	0%	/dev/fda																																																																																						
/dev/mapper/rl-root	xfs	65G	6,9G	58G	11%	/																																																																																						
/dev/mapper/rl-home	xfs	32G	10G	22G	32%	/home																																																																																						
/dev/sda2	xfs	1014M	462M	553M	46%	/DataBase																																																																																						
/dev/sda1	vfat	599M	5,0M	594M	1%	/boot/efi																																																																																						
/dev/fda	tmpfs	356M	32K	356M	1%	/tmp																																																																																						
/dev/sda3	iso9660	10G	10G	0	100%	/mnt/iso																																																																																						
/dev/sda4	64																																																																																											
/dev/sdb	xfs	97G	5,5G	92G	6%	/DataBase																																																																																						
113.	<div>Se procede a restaurar el respaldo inicial del sistema de archivos. Para tal tarea se utiliza la herramienta “xfsrestore”. Inserte el siguiente comando en la terminal.</div> <div><pre>\$ sudo xfsrestore --f [UBICACIÓN_FICHERO_RESPALDO] [DESTINO_RESTAURACIÓN]</pre><pre>xfsrestore: using file dump (drive_simple) strategy xfsrestore: version 3.1.8 (dump format 3.0) - type ^C for status and control xfsrestore: searching media for dump xfsrestore: examining media file 0 xfsrestore: dump description: xfsrestore: hostname: localhost.localdomain xfsrestore: mount point: /DataBase xfsrestore: volume: /dev/sdb xfsrestore: session time: Mon Jan 11 10:11:07 2020 xfsrestore: level: 0 xfsrestore: session label: "Backup_Base_de_datos" xfsrestore: media label: "/DataBase" xfsrestore: file system id: e3fd7e5d-d520-4b55-ba14-463b003ffff3 xfsrestore: session id: 401a5407-a048-45ae-97e4-9157a9284719 xfsrestore: media id: a412f519-fa53-4bff-a4bd-12271471c428 xfsrestore: using online session inventory xfsrestore: searching media for directory dump xfsrestore: reading directories xfsrestore: 1 directories and 1 entries processed xfsrestore: directory post-processing xfsrestore: restoring non-directory files xfsrestore: restore complete: 11 seconds elapsed xfsrestore: Restore Summary: xfsrestore: stream 0 /home/usuario/respaldo_db OK (success) xfsrestore: Restore Status: SUCCESS</pre></div>																																																																																											

