

MINISTERIO DE DEFENSA



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: 083-22-210-0

Fecha de Edición: agosto 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 ORACLE 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 ORACLE LINUX	20
ANEXO A.1. PREPARACIÓN DEL EQUIPO.....	21
ANEXO A.1.1. CONTRASEÑA DE GRUB	23
ANEXO A.2. FORTIFICACIÓN DEL KERNEL	24
ANEXO A.3. CONFIGURACIÓN DE SSH	25
ANEXO A.4. CONFIGURACIÓN Y PROTECCIÓN DE REGISTROS DE ACTIVIDAD	27
ANEXO A.5. CONFIGURACION DE USUARIOS Y POLITICAS DE CREDENCIALES.....	28
ANEXO A.5.1. USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS	28
ANEXO A.5.2. BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS	29
ANEXO A.5.3. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS	30
ANEXO A.5.4. CONFIGURACIÓN SEGURA DE GNOME	32
ANEXO A.6. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS	33
ANEXO A.6.1. LIMITACIÓN DE SERVICIOS, DEMONIOS Y HERRAMIENTAS	33
ANEXO A.6.2. COMPROBACIÓN DE PAQUETES INSTALADOS Y HUÉRFANOS	35
ANEXO A.7. CONFIGURACIONES ADICIONALES	36
ANEXO A.7.1. CONTRASEÑA SEGURA DE ROOT	36
ANEXO A.7.2. BUSQUEDA DE CUENTAS SIN CONTRASEÑA.....	37
ANEXO A.7.3. USUARIOS CON UID 0 QUE NO SEAN ROOT	38
ANEXO A.7.4. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS	38
ANEXO A.7.5. LIMITACIÓN DE DISPOSITIVOS EXTRAÍBLES	39
ANEXO A.7.6. PROTECCIÓN DE SERVICIOS DE RED	42
ANEXO A.7.7. CONFIGURACIÓN ADICIONAL DE SEGURIDAD – SELINUX	44
ANEXO A.7.8. INTERFAZ WEB COCKPIT	45
ANEXO A.7.9. APLICACIÓN DE ACTUALIZACIONES	49

ANEXO A.7.10.	INSTALACIÓN DE ANTIVIRUS.....	50
ANEXO A.7.11.	RESPALDO DE ARCHIVOS CON SISTEMA DE FICHEROS XFS.....	52
ANEXO A.7.12.	RESTAURACIÓN DE ARCHIVOS DE RESPALDO	54

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 (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 Oracle Linux 8.

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 Oracle Linux 8, 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 “Oracle Linux 8.5”, 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 remplazar 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.

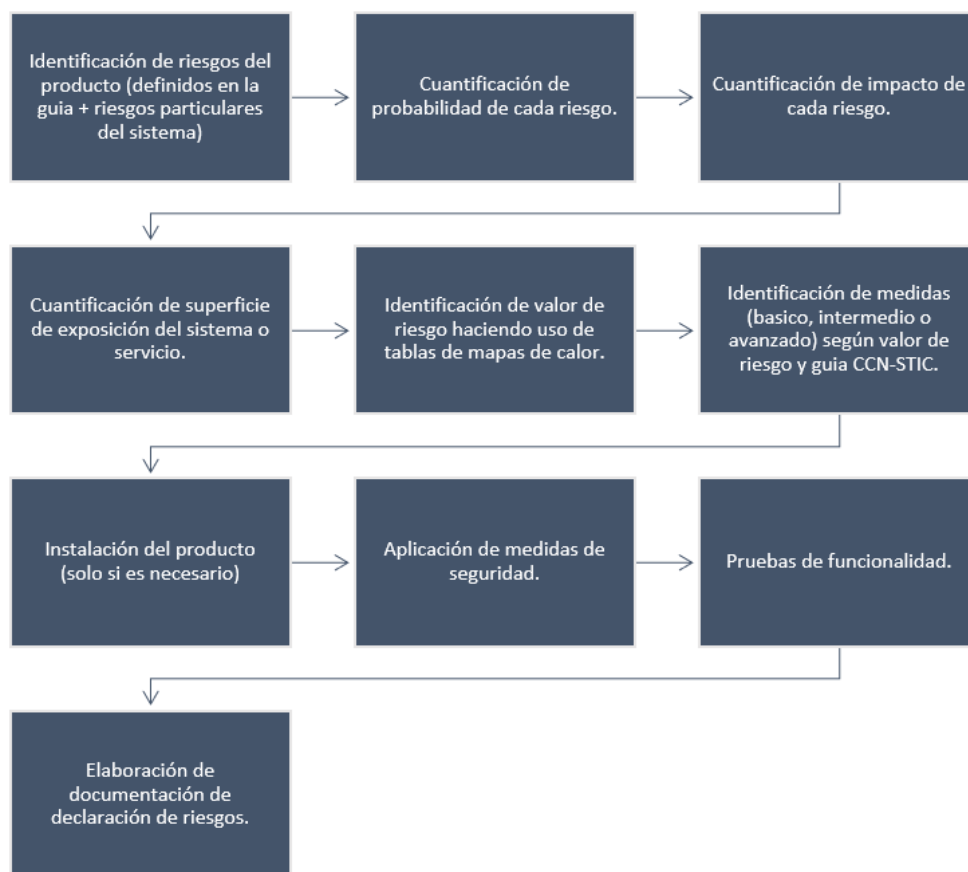
Para la identificación inicial de riesgos, se ha empleado la metodología MAGERIT y la herramienta PILAR, sobre un escenario basado en Oracle Linux 8.5.

- 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 Oracle Linux 8.5.

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 ORACLE 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 ORACLE 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 Oracle Linux 8, 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-OL1: 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 ORACLE LINUX	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log).	[A.3.SEC-OL1] Se auditan los inicios de sesión.			
	[A.3.SEC-OL2] Se controla quien puede acceder a los registros de seguridad y auditoría.			
	[A.3.SEC-OL3] Se controla el cambio de hora del sistema.			
	[A.3.SEC-OL4] Se controla quién puede generar o modificar reglas de audit.			
	[A.3.SEC-OL5] Se ha implementado la auditoría detallada basada en subcategorías.			
	[A.3.SEC-OL6] Se garantiza al menos 90 días de registros de actividad.			
	[A.3.SEC-OL7] Se auditan las modificaciones del fichero sudoers, así como los cambios en permisos, usuarios, grupos y contraseñas.			
	[A.3.SEC-OL8] Se auditan los cambios en la configuración de Cron y en tareas programadas incluyendo los de scripts de inicio.			
	[A.3.SEC-OL9] Se auditan los intentos de acceso a elementos críticos.			
	[A.3.SEC-OL10] Se audita toda operación de montaje en el sistema y modificaciones en la memoria de intercambio.			
	[A.3.SEC-OL11] Se auditan modificaciones en ficheros PAM.			
[A.4] Manipulación de los ficheros de configuración.	[A.4.SEC-OL1] Los usuarios estándar no disponen de permisos de administrador local ni se encuentran incluidos en un grupo "sudoer".			
	[A.4.SEC-OL2] El sistema tiene un antivirus y este está actualizado.			
	[A.4.SEC-OL3] Se modifican los permisos por particiones			
[A.5] Suplantación de la identidad.	[A.5.SEC-OL1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-OL2] Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.			
	[A.5.SEC-OL3] Se controla el acceso a las claves de cifrado.			
	[A.5.SEC-OL4] Se han deshabilitado los algoritmos de cifrado inseguros.			
	[A.5.SEC-OL5] Se exige el cambio de contraseña de forma recurrente.			
	[A.5.SEC-OL6] Se hace uso de protocolos seguros para los procesos de autenticación de red.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA ORACLE LINUX	ALCANCE		
		B	I	A
	[A.5.SEC-OL7] Se controla la inactividad de la sesión de red.			
	[A.5.SEC-OL8] Se controla la inactividad de consola local y remota.			
[A.6] Abuso de privilegios de acceso.	[A.6.SEC-OL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC-OL2] Se restringen accesos en modo recuperación incluido el modo modificación de inicio de grub.			
	[A.6.SEC-OL3] Se limita la shell de usuarios de servicio a "/bin/false".			
	[A.6.SEC-OL4] Se restringe el uso de sesiones con usuario "root".			
	[A.6.SEC-OL5] Se modifica la máscara global del sistema para ser más restrictiva.			
	[A.6.SEC-OL6] Se eliminan los grupos y usuarios innecesarios del sistema.			
[A.8] Difusión de software dañino.	[A.8.SEC-OL1] Se controla quién puede instalar software en el sistema.			
	[A.8.SEC-OL2] El sistema operativo está actualizado.			
	[A.8.SEC-OL3] El sistema tiene un firewall local activado.			
	[A.8.SEC-OL4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC-OL5] Se controla la ejecución de aplicaciones.			
	[A.8.SEC-OL6] Se dispone de medidas anti ransomware habilitadas.			
	[A.4.SEC-OL2] El sistema tiene un antivirus y éste está actualizado.			
	[A.8.SEC-OL7] Está habilitado el arranque cifrado con contraseña que evite modificaciones (GRUB protegido).			
	[A.5.SEC-OL1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-OL2] Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.			
	[A.6.SEC-OL6] Se eliminan los grupos y usuarios innecesarios del sistema.			
	[A.8.SEC-OL8] Se audita la descarga de archivos			
	[A.8.SEC-OL9] Están deshabilitados los compiladores del sistema			
[A.11] Acceso no autorizado.	[A.11.SEC-OL1] Se controla el inicio de sesión local en el sistema.			
	[A.11.SEC-OL2] Se ha reforzado la seguridad del protocolo SSH.			
	[A.11.SEC-OL3] Se dispone de una política de credenciales robusta.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA ORACLE LINUX	ALCANCE		
		B	I	A
	[A.11.SEC-OL4] Durante el inicio de sesión, el sistema muestra un texto en cumplimiento con las normas o directivas de la organización.			
	[A.11.SEC-OL5] Se controla el acceso al sistema a través de la red.			
	[A.11.SEC-OL6] Sólo se permiten algoritmos de cifrado robustos en accesos al sistema.			
	[A.3.SEC-OL4] Se controla quién puede generar o modificar reglas de audit.			
	[A.5.SEC-OL1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-OL2] Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.			
	[A.6.SEC-OL6] Se eliminan los grupos y usuarios innecesarios del sistema.			
	[A.11.SEC-OL7] Se limita el tiempo de inactividad del GUI.			
	[A.11.SEC-OL8] Se muestra un banner disuasorio.			
	[A.11.SEC-OL9] Se deshabilita la lista de usuarios.			
	[A.11.SEC-OL10] Se deshabilita recordar el historial de ficheros.			
	[A.11.SEC-OL11] Se deshabilita combinación de teclas para iniciar el inspector GTK			
	[A.11.SEC-OL12] Se deshabilita el auto montaje de dispositivos extraíbles en el sistema.			
[A.15] Modificación de la información.	[A.15.SEC-OL1] Se controla el uso de medios de almacenamiento extraíbles.			
	[A.5.SEC-OL6] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.6.SEC-OL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.11.SEC-OL2] Se ha reforzado la seguridad del protocolo SSH.			
	[A.11.SEC-OL6] Sólo se permiten algoritmos de cifrado robustos en accesos al sistema.			
[A.19] Revelación de información.	[A.19.SEC-OL1] Se controla el acceso al árbol de carpetas y ficheros.			
	[A.19.SEC-OL2] Se aplican medidas para la protección de las cuentas.			
	[A.19.SEC-OL3] Está habilitado un algoritmo robusto y la complejidad de contraseñas			
	[A.3.SEC-OL2] Se controla quien puede acceder a los registros de seguridad y auditoría.			
	[A.5.SEC-OL3] Se controla el acceso a las claves de cifrado.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA ORACLE LINUX	ALCANCE		
		B	I	A
	[A.5.SEC-OL6] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.6.SEC-OL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC-OL2] Se restringen accesos en modo recuperación incluido el modo modificación de inicio de grub.			
[A.22] Manipulación de programas.	[A.6.SEC-OL1] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC-OL2] Se restringen accesos en modo recuperación incluido el modo modificación de inicio de grub.			
	[A.6.SEC-OL3] Se limita la shell de usuarios de servicio a "/bin/false".			
	[A.8.SEC-OL4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC-OL6] Se dispone de medidas anti ransomware habilitadas.			
[A.23] Manipulación del hardware.	[A.23.SEC-OL1] Se controla la instalación y uso de cualquier dispositivo conectado al equipo.			
	[A.15.SEC-OL1] Se controla el uso de medios de almacenamiento extraíbles.			
	[A.23.SEC-OL2] Se restringe el montaje y desmontaje dinámico de sistemas de archivos			
[A.24] Denegación de servicio.	[A.24.SEC-OL1] Se controlan los privilegios que afectan al rendimiento del sistema.			
	[A.24.SEC-OL2] Se controla quien puede apagar el sistema.			
	[A.8.SEC-OL6] Se dispone de medidas anti ransomware habilitadas.			
	[A.3.SEC-OL3] Se controla el cambio de hora del sistema.			
	[A.3.SEC-OL4] Se controla quién puede generar o modificar reglas de audit.			
[A.25] Robo de equipos.	[A.25.SEC-OL1] El disco del sistema está cifrado.			
	[A.25.SEC-OL2] El disco de datos está cifrado.			
[A.29] Extorsión.	[A.4.SEC-OL2] El sistema tiene un antivirus y éste está actualizado.			
	[A8.SEC-OL1] Se controla quién puede instalar software en el sistema.			
	[A.8.SEC-OL2] El sistema operativo está actualizado.			
	[A.8.SEC-OL3] El sistema tiene un firewall local activado.			
	[A.8.SEC-OL4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA ORACLE LINUX	ALCANCE		
		B	I	A
	[A.8.SEC-OL5] Se controla la ejecución de aplicaciones.			
	[A.8.SEC-OL6] Se dispone de medidas anti ransomware habilitadas.			
[A.30] Ingeniería social.	[A.30.SEC-OL1] Existe una política de bloqueo de cuentas ante inicios de sesión incorrectos.			
[E.25] Pérdida de equipos.	[A.25.SEC-OL1] El disco del sistema está cifrado.			
	[A.25.SEC-OL2] El disco de datos está cifrado.			

ANEXO A. PASO A PASO. CONFIGURACIÓN BASE DE SEGURIDAD SOBRE ORACLE LINUX

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento de los sistemas Oracle Linux 8, 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 Oracle Linux 8 actualización 5, conectado por red a repositorios oficiales de Oracle Linux. 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-OL4]** Se han deshabilitado los algoritmos de cifrado inseguros. La deshabilitación de estos algoritmos de cifrado dificultan los ataques de fuerza bruta contra el sistema.

Paso	Descripción
1.	Inicie sesión en el equipo Oracle Linux 8 que está asegurando utilizando una cuenta con permisos de administrador o sudoers.
2.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y en la columna de la izquierda seleccione el icono correspondiente a la terminal, tal y como se muestra en la imagen.
3.	Diríjase al directorio raíz “/” . <pre>\$ cd /</pre>
4.	Cree el directorio “Scripts” en la ruta “/” . <pre>\$ sudo mkdir /Scripts</pre>
5.	Monte el dispositivo de CDROM. <pre>\$ sudo mount /dev/cdrom /media</pre> 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.
6.	Copie en el directorio “Scripts” , los ficheros y subdirectorios asociados a esta guía. <pre>\$ sudo cp -r /media/* /Scripts/</pre> Nota: Los scripts asumen que su ubicación en el sistema será bajo “/Scripts”. Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
7.	Desmonte el dispositivo de CDROM. <pre>\$ sudo umount /media</pre>

Paso	Descripción
8.	Para que el nivel de política criptográfica del sistema cumpla con los parámetros de seguridad necesarios a los niveles exigidos, ejecute el siguiente comando. <pre>\$ sudo update-crypto-policies --set DEFAULT</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo update-crypto-policies --set DEFAULT 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.</pre> Nota: Los niveles posibles de política criptográfica en el sistema son cuatro: - 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 Oracle 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 Oracle 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-OL2]** 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-OL7]** Está habilitado el arranque cifrado con contraseña que evite modificaciones. Se protege el inicio de GRUB.

Paso	Descripción
9.	Se procede a continuación a configurar una contraseña para el gestor de arranque GRUB. Para ello diríjase a la carpeta “Scripts”. <pre>\$ cd /Scripts</pre> Acto seguido ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-620_01-Contraseña_grub.sh</pre> A continuación, introduzca el nombre de usuario que tendrá acceso al modo de edición de inicio de “grub”. <pre>--APLICANDO CONTRASEÑA DE GRUB-- Pulse ENTER para continuar o Ctrl + C para cancelar.... <<Inserte usuario para la edicion de GRUB>>: aCdCmN620_grub</pre> Nota: Se usa a modo de ejemplo el usuario “aCdCmN620_grub”. Dicho usuario no es necesario que pertenezca a los usuarios del sistema. Deberá adaptar las configuraciones a los parámetros de su organización.
10.	A continuación, introduzca la contraseña deseada que cumpla con los requisitos de seguridad. <pre>Introduzca la contraseña: Reintroduzca la contraseña: El hash PBKDF2 de su contraseña es Generating grub configuration file ... done</pre> 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 vuelva a repetir este paso desde el inicio antes de continuar con el siguiente punto.

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-OL6]** 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.

Paso	Descripción
11.	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 ”.
12.	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.
13.	Para ello diríjase a la carpeta “ Scripts ”.
	<pre>\$ cd /Scripts</pre> Ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-620_02-Parametros_del_kernel.sh</pre>
14.	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.
	<pre>-- APLICANDO PARÁMETROS DEL KERNEL --</pre> <pre>EL SCRIPT GUARDARÁ UNA COPIA DE LOS ARCHIVOS ORIGINALES POR SI SE DESEARA RESTAU</pre> <pre>RAR CONFIGURACIONES ANTERIORES EN :</pre> <pre>/etc/sysctl.conf.bak</pre> <pre>/etc/sysctl.d</pre> <pre>NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE FINALICE</pre> <pre>EN CASO DE DETENCIÓN DEL SCRIPT, VUELVA A EJECUTARLO ANTES DE REINICIAR, HASTA</pre> <pre>QUE FINALICE EL PROCESO CORRECTAMENTE</pre>
15.	Cuando la configuración predeterminada finalice, pulse “ Enter ” y se abrirá el fichero de configuración.
	<pre>Pulse ENTER para continuar o Ctrl + C para cancelar....</pre> <pre>>>>>>>>EL PROCESO A FINALIZADO<<<<<<<</pre> <pre>Se mostrará el fichero /etc/sysctl.conf para su revisión pulse para continuar...</pre>
16.	Se pueden observar las configuraciones de seguridad aplicadas por la ejecución del script. Habilite, deshabilite o añada configuraciones según sus necesidades.
	<pre>net.ipv4.conf.all.send_redirects = 0</pre> <pre>net.ipv4.conf.all.accept_redirects = 0</pre> <pre>net.ipv4.conf.default.accept_redirects = 0</pre> <pre>net.ipv4.conf.default.send_redirects = 0</pre> <pre>net.ipv4.conf.default.secure_redirects = 0</pre> <pre>net.ipv4.conf.all.secure_redirects = 0</pre> <pre>net.ipv4.conf.all.accept_source_route = 0</pre> <pre>net.ipv4.conf.default.accept_source_route = 0</pre> <pre>net.ipv4.conf.all.log_martians = 1</pre> <pre>net.ipv4.conf.default.log_martians = 1</pre> <pre>net.ipv4.icmp.ignore_bogus_error_responses = 1</pre> <pre>net.ipv4.icmp_echo_ignore_broadcasts = 1</pre> <pre>net.ipv4.tcp_syncookies = 1</pre> <pre>fs.suid_dumpable = 0</pre> <pre>net.ipv6.conf.default.accept_source_route = 0</pre> <pre>net.ipv6.conf.all.accept_source_route = 0</pre> <pre>net.ipv6.conf.all.accept_redirects = 0</pre> <pre>net.ipv6.conf.default.accept_ra = 0</pre> <pre>net.ipv6.conf.all.accept_ra = 0</pre> <pre>net.ipv6.conf.default.accept_redirects = 0</pre>
	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.

ANEXO A.3. CONFIGURACIÓN DE SSH

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

- a) **[A.5.SEC-OL6]** Se hace uso de protocolos seguros para los procesos de autenticación de red.
- b) **[A.5.SEC-OL7]** Se controla la inactividad de la sesión de red.
- c) **[A.11.SEC-OL2]** Se ha reforzado la seguridad del protocolo SSH. Evitando accesos no autorizados.
- d) **[A.11.SEC-OL6]** 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
17.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
18.	A continuación, se procederá a configurar el servicio SSH. Para ello diríjase al directorio “Scripts”. <pre>\$ cd /Scripts</pre>
19.	Ejecute el script CCN-STIC-620-Parametros_SSH.sh. <pre>\$ sudo sh CCN-STIC-620_09-Parametros_SSH.sh</pre> Deberá elegir un puerto válido para SSH como se indica por pantalla. <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 DETENCIÓN 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> Nota: El puerto que ingrese debe tener un valor válido (revise el fichero /etc/services), y se deberá añadir la excepción oportuna en el cortafuegos del sistema (ANEXO A.7.6 PROTECCIÓN DE SERVICIOS DE RED).

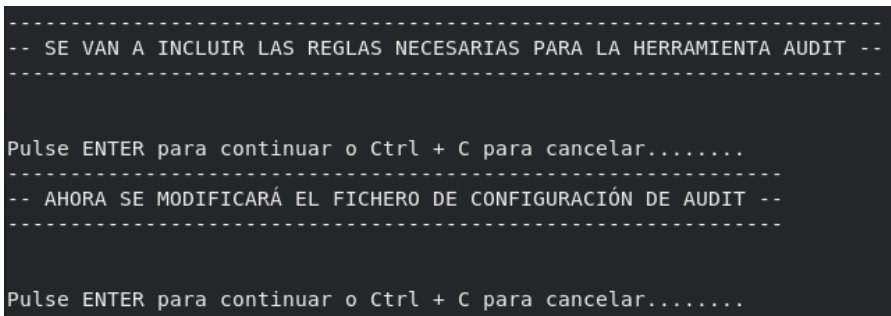
Paso	Descripción
20.	A continuación, se mostrará el estado del servicio de SSH. <pre> ssh.service - OpenSSH server daemon Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled) Active: active (running) since Thu 2018-04-09 10:41:22 CEST; 36min ago Docs: man:sshd(8) man:sshd_config(5) Process: 10062 ExecReload=/bin/kill -HUP \$MAINPID (code=exited, status=0/SUCCESS) Main PID: 7271 (sshd) Tasks: 1 (limit: 22401) Memory: 2.7M CGroup: /system.slice/ssh.service └─7271 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256- OL8 sshd[7277]: Accepted password for root from ::1 port 39884 ssh2 OL8 sshd[7277]: pam_unix(sshd:session): session opened for user root by (uid=0) OL8 systemd[1]: Reloaded OpenSSH server daemon. OL8 sshd[7271]: Received SIGHUP; restarting. OL8 systemd[1]: Reloaded OpenSSH server daemon. OL8 sshd[7271]: Server listening on 0.0.0.0 port 22. OL8 sshd[7271]: Server listening on :: port 22. OL8 systemd[1]: Reloaded OpenSSH server daemon. OL8 sshd[7271]: Received SIGHUP; restarting. OL8 systemd[1]: Reloaded OpenSSH server daemon. </pre> Cierre el mensaje de estado del servicio pulsando la tecla “q”.
21.	Finalmente, se mostrará la configuración de SSH.  Nota: Revise los parámetros y adecúelos a las configuraciones de su organización si fuese oportuno.

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-OL1] Se auditan los inicios de sesión.
- b) [A.3.SEC-OL2] Se controla quien puede acceder a los registros de seguridad y auditoría.
- c) [A.3.SEC-OL3] Se controla el cambio de hora del sistema.
- d) [A.3.SEC-OL4] Se controla quién puede generar o modificar reglas de AUDIT.
- e) [A.3.SEC-OL5] Se ha implementado la auditoría detallada basada en subcategorías.
- f) [A.3.SEC-OL6] Se garantiza al menos 90 días de registros de actividad.
- g) [A.8.SEC-OL8] Se audita la descarga de archivos.
- h) [A.11.SEC-OL1] Se controla el inicio de sesión local en el sistema.

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

Paso	Descripción
22.	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 ”.
23.	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”. <pre>\$ cd /Scripts</pre> Ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-620_03-Manipullacion_de_registros_de_actividad.sh</pre>  El script finalizará mostrando las reglas creadas. Si el sistema indicara lo contrario vuelva ejecute de nuevo el script. Nota: El script añade los parámetros necesarios al fichero de configuración “/etc/audit/audit.conf” para que se generen máximo 12 archivos de logs con una capacidad máxima por archivo de 10Mb, lo que crea un total de 120Mb. Cuando alcance el límite, los ficheros de logs rotarán gracias al parámetro “max_log_file_action = ROTATE”.

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-OL3] Se limita la shell de usuarios de servicio a `"/bin/false"`.
- b) [A.6.SEC-OL4] Se restringe el uso de sesiones con usuario `"root"`.
- c) [A.6.SEC-OL6] Se eliminan los grupos y usuarios innecesarios del sistema.
- d) [A.11.SEC-OL7] Se eliminan los 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
24.	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” .
25.	Se procede a eliminar los usuarios creados por defecto en la instalación y que son innecesarios. Para ello diríjase a la carpeta “Scripts”. <pre>\$ cd /Scripts</pre> Ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-620_04-Desinstalar_usuarios_innecesarios.sh</pre> <pre>----- --DESINSTALANDO USUARIOS INNECESARIOS-- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre> El script iniciará un proceso que deshabilitará los usuarios innecesarios, así como los grupos no necesarios, y corregirá las shells predeterminadas en caso de no ser las correctas. No pulse ninguna tecla ni cierre la ventana hasta que el proceso finalice. Ignore los mensajes de pantalla. <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>
26.	Si ha detectado que en la actualidad está habilitado un usuario que ya no tiene necesidad de acceder al sistema puede usar el siguiente comando (sin comillas), siendo NOMBREDEUSUARIO el nombre del usuario candidato para su eliminación. <pre>\$ sudo userdel -r "NOMBREDEUSUARIO"</pre> De igual modo, si ha detectado un grupo que no sea de necesidad para la organización, use el siguiente comando para eliminarlo. <pre>\$ sudo groupdel "NOMBREDEGRUPO"</pre>

Paso	Descripción
27.	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. <pre>\$ sudo awk -F: '{if (\$3 >= 1000) { print \$1 ":" \$3 \$7 } }' /etc/passwd</pre> Nota: El usuario nobody con uid:65534 y como excepción, deberá conservar su shell.
28.	Cuando finalice todas las tareas reinicie el sistema. <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-OL1]** 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
29.	Si ha cerrado la “Terminal” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “Terminal”.
30.	Se procederá a configurar el bloqueo de cuentas por intentos fallidos, por medio del módulo “pam_faillock.so”. Para ello diríjase a la carpeta “Scripts”. <pre>\$ cd /Scripts</pre> Ejecute el siguiente script. <pre>\$ sudo sh CCN-STIC-620_05-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 DETENCIÓN 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> 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.

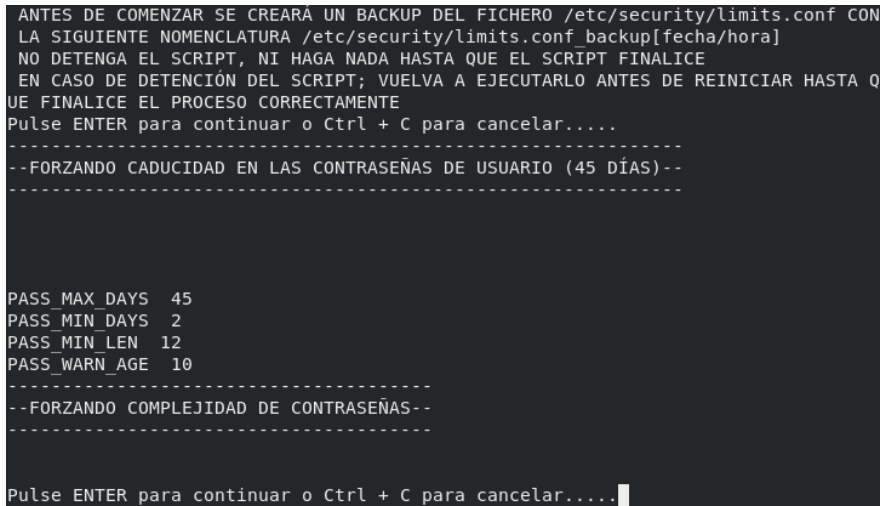
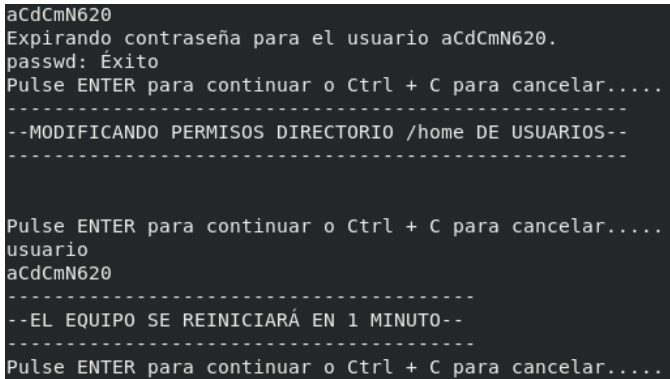
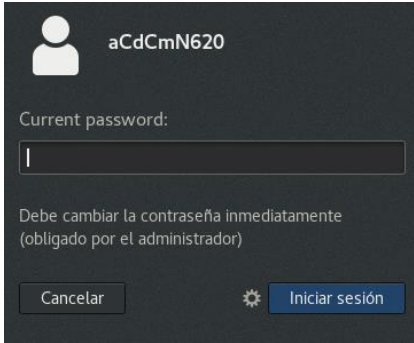
ANEXO A.5.3. LÍMITES DE RECURSOS, PERMISOS Y CADUCIDAD DE CONTRASEÑAS

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

- a) **[A.4.SEC-OL1]** Los usuarios estándar no disponen de permisos de administrador local ni se encuentran incluidos en un grupo "sudoer".
- b) **[A.5.SEC-OL1]** Se controlan los permisos de inicio de sesión y suplantación de identidad.
- c) **[A.5.SEC-OL2]** Se controlan los intentos de elevación mediante definición de usuarios y grupos sudoers.
- d) **[A.5.SEC-OL3]** Se controla el acceso a las claves de cifrado.
- e) **[A.5.SEC-OL5]** Se exige el cambio de contraseña de forma recurrente.
- f) **[A8.SEC-OL1]** Se controla quién puede instalar software en el sistema.
- g) **[A.11.SEC-OL3]** Se dispone de una política de credenciales robusta.
- h) **[A.19.SEC-OL2]** Se aplican medidas para la protección de las cuentas.
- i) **[A.19.SEC-OL3]** Está habilitado un algoritmo robusto y la complejidad de contraseñas.
- j) **[A.24.SEC-OL1]** Se controlan los privilegios que afectan al rendimiento del sistema.
- k) **[A.24.SEC-OL2]** Se controla quien puede apagar el sistema.

Todos estos riesgos se pueden aminorar 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
31.	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" .
32.	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, la complejidad y los permisos en los directorios "/home" de cada usuario. Nota: Antes de comenzar en este paso, asegúrese de haber cerrado y guardado las aplicaciones y los documentos importantes. Para ello diríjase a la carpeta "Scripts". <pre>\$ cd /Scripts</pre>

Paso	Descripción
33.	Ejecute el siguiente script. <pre># sudo sh CCN-STIC-620_06-Limites_permisos_y_cad_contraseñas.sh</pre>  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. 
34.	Cuando reinicie el sistema e inicie sesión, aparecerá un mensaje advirtiéndole del cambio de contraseña con los requisitos de complejidad exigidos. 
35.	Le pedirá la contraseña actual de nuevo y posteriormente nueva contraseña dos veces, que deberá cumplir con los requisitos exigidos.

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-OL4]** Durante el inicio de sesión, el sistema muestra un texto en cumplimiento con las normas o directivas de la organización.
- b) **[A.11.SEC-OL8]** Se limita el tiempo de inactividad del GUI.
- c) **[A.11.SEC-OL9]** Se muestra un banner disuasorio.
- d) **[A.11.SEC-OL10]** Se deshabilita la lista de usuarios.
- e) **[A.11.SEC-OL11]** Se deshabilita recordar el historial de ficheros.
- f) **[A.11.SEC-OL12]** Se deshabilita combinación de teclas para iniciar el inspector GTK.

Después de securizar el kernel, proceso realizado en el ANEXO A.2 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
36.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
37.	Se va a proceder a configurar parámetros de seguridad en el escritorio Gnome. Para ello diríjase a la carpeta “Scripts”. <pre>\$ cd /Scripts</pre> Ejecute el siguiente comando. <pre>\$ sudo sh CCN-STIC-620_07-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> Introduzca el Banner deseado acorde con su organización. <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 AUTORIZACIÓN - El sistema está restringido a los usuarios autorizados</pre>
38.	El script iniciará un proceso que modificará la pantalla de inicio de Oracle Linux 8.5 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. <pre>ES UN DELITO CONTINUAR SIN LA DEBIDA AUTORIZACIÓN - El sistema está restringido a los usuarios autorizados Nombre de usuario: </pre>

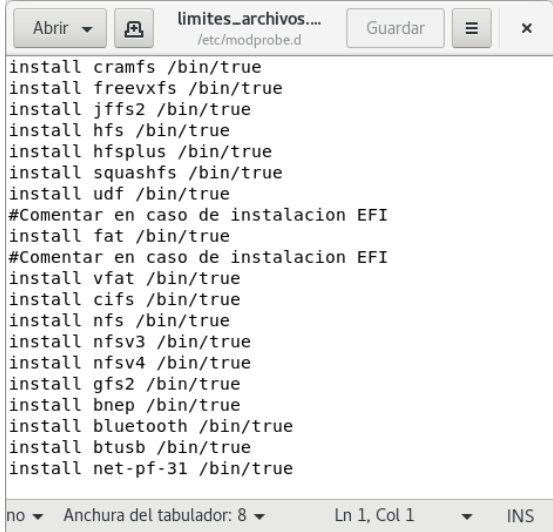
ANEXO A.6. LIMITACIÓN DE DEMONIOS, SERVICIOS Y HERRAMIENTAS INSTALADAS

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-OL4]** Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.
- b) **[A.8.SEC-OL9]** 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
39.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
40.	Se procede a desinstalar programas innecesarios, además se procederá a deshabilitar servicios y demonios innecesarios. Para ello diríjase a la carpeta “Scripts”. <pre>\$ cd /Scripts</pre> Ejecute el siguiente comando e introduzca la contraseña si se le solicita. <pre>\$ sudo sh CCN-STIC-620_10-Elementos_innecesarios.sh</pre> <pre>-- SE ELIMINARÁN PROGRAMAS Y DRIVERS INNECESARIOS --</pre> Pulse ENTER para continuar o Ctrl + C para cancelar..... 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.
41.	El proceso del script continúa con la desinstalación de paquetes de software no necesarios. <pre> noarch 0.47-2.1.el8 @AppStream 24 k noarch 0.3.3-10.el8 @AppStream 28 k noarch 2.0-2.4.el8 @AppStream 15 k noarch 2.1.1-7.el8 @AppStream 32 k noarch 1.11-3.el8 @AppStream 241 k x86_64 1.4.0-9.el8 @anaconda 21 k noarch 2.26-0-0.el8 @AppStream 308 k x86_64 1:3.11.0-13.el8 @AppStream 368 k noarch 2017.2-9.el8 @AppStream 175 k noarch 1.4-3-5.el8 @AppStream 9.4 k noarch 0.3.1-11.el8 @AppStream 37 k noarch 1.1.1-2.el8 @AppStream 402 k x86_64 0.8-0-0.el8 @AppStream 124 k x86_64 0.26-2.el8 @AppStream 315 k x86_64 0.8.0-0.el8 @AppStream 110 k noarch 1.10-1-2.el8 @AppStream 10 k x86_64 1.10-1-7.el8 @AppStream 2.7 M x86_64 1.51-0-5.el8 @anaconda 610 k 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> Nota: Deberá adaptar los parámetros a las necesidades de su organización.

Paso	Descripción																																																		
42.	Pulse “Enter” para restringir el montaje dinámico de sistemas de archivos. <pre> ----- -- RESTRINGIR EL MONTAJE Y DESMONTAJE DINÁMICO DE SISTEMAS DE ARCHIVOS-- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>																																																		
43.	Se muestra la configuración establecida en “limites_archivos.conf”.  Nota: Para continuar con el proceso, deberá guardar y cerrar el documento si está conforme a los parámetros de su organización.																																																		
44.	Pulse “Enter” para continuar y saldrá el mensaje “Se deshabilitarán y enmascararán demonios y procesos innecesarios”. <pre> ----- -- SE DESHABILITARAN Y ENMASCARARÁN DEMONIOS Y PROCESOS INNECESARIOS -- ----- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre> Pulse nuevamente “Enter” para continuar con la ejecución. Posteriormente se mostrarán el estado de los servicios y demonios del sistema. <table border="1"> <thead> <tr> <th>UNIT FILE</th> <th>STATE</th> </tr> </thead> <tbody> <tr><td>proc-sys-fs-binfmt_misc.automount</td><td>static</td></tr> <tr><td>-.mount</td><td>generated</td></tr> <tr><td>boot.mount</td><td>generated</td></tr> <tr><td>dev-hugepages.mount</td><td>static</td></tr> <tr><td>dev-mqueue.mount</td><td>static</td></tr> <tr><td>home.mount</td><td>generated</td></tr> <tr><td>proc-fs-nfsd.mount</td><td>static</td></tr> <tr><td>proc-sys-fs-binfmt_misc.mount</td><td>static</td></tr> <tr><td>run-vmblock\x2dfuse.mount</td><td>disabled</td></tr> <tr><td>sys-fs-fuse-connections.mount</td><td>static</td></tr> <tr><td>sys-kernel-config.mount</td><td>static</td></tr> <tr><td>sys-kernel-debug.mount</td><td>static</td></tr> <tr><td>tmp.mount</td><td>disabled</td></tr> <tr><td>var-lib-machines.mount</td><td>static</td></tr> <tr><td>var-lib-nfs-rpc_pipefs.mount</td><td>static</td></tr> <tr><td> cups.path</td><td>enabled</td></tr> <tr><td>ostree-finalize-staged.path</td><td>disabled</td></tr> <tr><td>systemd-ask-password-console.path</td><td>static</td></tr> <tr><td>systemd-ask-password-plymouth.path</td><td>static</td></tr> <tr><td>systemd-ask-password-wall.path</td><td>static</td></tr> <tr><td>session-2.scope</td><td>transient</td></tr> <tr><td>session-cl.scope</td><td>transient</td></tr> <tr><td>accounts-daemon.service</td><td>enabled</td></tr> <tr><td>alsa-restore.service</td><td>static</td></tr> </tbody> </table> lines 1-25 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.	UNIT FILE	STATE	proc-sys-fs-binfmt_misc.automount	static	-.mount	generated	boot.mount	generated	dev-hugepages.mount	static	dev-mqueue.mount	static	home.mount	generated	proc-fs-nfsd.mount	static	proc-sys-fs-binfmt_misc.mount	static	run-vmblock\x2dfuse.mount	disabled	sys-fs-fuse-connections.mount	static	sys-kernel-config.mount	static	sys-kernel-debug.mount	static	tmp.mount	disabled	var-lib-machines.mount	static	var-lib-nfs-rpc_pipefs.mount	static	cups.path	enabled	ostree-finalize-staged.path	disabled	systemd-ask-password-console.path	static	systemd-ask-password-plymouth.path	static	systemd-ask-password-wall.path	static	session-2.scope	transient	session-cl.scope	transient	accounts-daemon.service	enabled	alsa-restore.service	static
UNIT FILE	STATE																																																		
proc-sys-fs-binfmt_misc.automount	static																																																		
-.mount	generated																																																		
boot.mount	generated																																																		
dev-hugepages.mount	static																																																		
dev-mqueue.mount	static																																																		
home.mount	generated																																																		
proc-fs-nfsd.mount	static																																																		
proc-sys-fs-binfmt_misc.mount	static																																																		
run-vmblock\x2dfuse.mount	disabled																																																		
sys-fs-fuse-connections.mount	static																																																		
sys-kernel-config.mount	static																																																		
sys-kernel-debug.mount	static																																																		
tmp.mount	disabled																																																		
var-lib-machines.mount	static																																																		
var-lib-nfs-rpc_pipefs.mount	static																																																		
cups.path	enabled																																																		
ostree-finalize-staged.path	disabled																																																		
systemd-ask-password-console.path	static																																																		
systemd-ask-password-plymouth.path	static																																																		
systemd-ask-password-wall.path	static																																																		
session-2.scope	transient																																																		
session-cl.scope	transient																																																		
accounts-daemon.service	enabled																																																		
alsa-restore.service	static																																																		

Paso	Descripción
45.	A continuación se bloquean los compiladores del sistema. Con dicho proceso terminará la ejecución del script. <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 2022-02-01 11:00:00 CEST, use 'shutdown -c' to cancel. >>>Guarde los documentos que tenga abiertos y espere...<<<< </pre>

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-OL4]** Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición y la difusión de software dañino mediante la instalación, debido a las dependencias, de paquetes asociados a estos servicios no requeridos.

Paso	Descripción																																								
46.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”. Ejecute el comando “ cd / ” y pulse la tecla “ Enter ”.																																								
47.	Se procederá a eliminar los antiguos kernel, los paquetes y repositorios huérfanos. Para ello dirijase a la carpeta “Scripts”. cd /Scripts Ejecute el siguiente comando. sudo sh CCN-STIC-620_11-Paquetes_huerfanos.sh <pre>----- --ELIMINANDO PAQUETES HUÉRFANOS-- ----- Pulse ENTER para continuar o Ctrl + C para cancelar.....</pre> De ser detectados paquetes huérfanos o dependencias obsoletas, deberá confirmar su eliminación manualmente. Nota: Deberá adaptar las configuraciones a los parámetros de su organización. <table><thead><tr><th>Paquete</th><th>Arq.</th><th>Versión</th><th>Repositorio</th><th>Tam.</th></tr></thead><tbody><tr><td colspan="5">Eliminando:</td></tr><tr><td>NetworkManager-initscripts-updown</td><td>noarch</td><td>1:1.36.0-4.0.1.el8</td><td>@ol8_baseos_latest</td><td>2.1 k</td></tr><tr><td>grub2-tools-efi</td><td>x86_64</td><td>1:2.02-123.0.3.el8</td><td>@ol8_baseos_latest</td><td>2.0 M</td></tr><tr><td>libibmad</td><td>x86_64</td><td>37.2-1.el8</td><td>@ol8_baseos_latest</td><td>41 k</td></tr><tr><td>python3-configobj</td><td>noarch</td><td>5.0.6-11.el8</td><td>@anaconda</td><td>342 k</td></tr><tr><td>radvd</td><td>x86_64</td><td>2.17-15.el8</td><td>@AppStream</td><td>188 k</td></tr><tr><td>rdma-core</td><td>x86_64</td><td>37.2-1.el8</td><td>@ol8_baseos_latest</td><td>103 k</td></tr></tbody></table> Resumen de la transacción Eliminar 6 Paquetes Espacio liberado: 2.7 M ¿Está de acuerdo [s/N]?: Pulse “Enter” para comenzar la ejecución del script. El script iniciará un proceso de desinstalación de dichos paquetes, para ello instalará la herramienta “yum-utils”. No pulse ninguna tecla ni cierre la ventana hasta que finalice con un mensaje en pantalla de “¡Listo!”.	Paquete	Arq.	Versión	Repositorio	Tam.	Eliminando:					NetworkManager-initscripts-updown	noarch	1:1.36.0-4.0.1.el8	@ol8_baseos_latest	2.1 k	grub2-tools-efi	x86_64	1:2.02-123.0.3.el8	@ol8_baseos_latest	2.0 M	libibmad	x86_64	37.2-1.el8	@ol8_baseos_latest	41 k	python3-configobj	noarch	5.0.6-11.el8	@anaconda	342 k	radvd	x86_64	2.17-15.el8	@AppStream	188 k	rdma-core	x86_64	37.2-1.el8	@ol8_baseos_latest	103 k
Paquete	Arq.	Versión	Repositorio	Tam.																																					
Eliminando:																																									
NetworkManager-initscripts-updown	noarch	1:1.36.0-4.0.1.el8	@ol8_baseos_latest	2.1 k																																					
grub2-tools-efi	x86_64	1:2.02-123.0.3.el8	@ol8_baseos_latest	2.0 M																																					
libibmad	x86_64	37.2-1.el8	@ol8_baseos_latest	41 k																																					
python3-configobj	noarch	5.0.6-11.el8	@anaconda	342 k																																					
radvd	x86_64	2.17-15.el8	@AppStream	188 k																																					
rdma-core	x86_64	37.2-1.el8	@ol8_baseos_latest	103 k																																					

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 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.

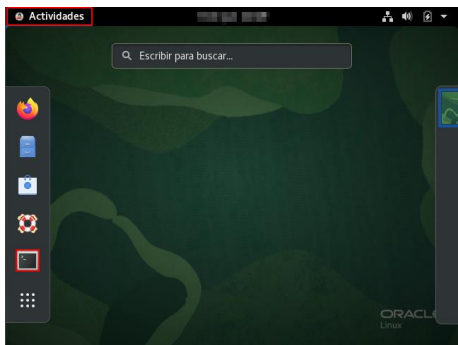
Para estos casos, se desarrolla el presente anexo, en el cual se establecen comentarios sobre las categorías de perfilado de seguridad de nivel intermedio afectadas y se determina un ejemplo de configuración o validación que permita garantizar el aseguramiento de Oracle Linux 8.5 con la premisa de apoyar 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. CONTRASEÑA SEGURA DE ROOT

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

- a) **[A.5.SEC-OL5]** Se exige el cambio de contraseña de forma recurrente evitando la suplantación de identidad de los usuarios del sistema.

Paso	Descripción
48.	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” . 
49.	Ejecute el siguiente comando. <pre>\$ sudo passwd root</pre>
50.	Se pedirán las credenciales del usuario para continuar la operación y una vez identificado que se tienen permisos se mostrará en pantalla el siguiente comentario “Cambiando la contraseña del usuario root” . Se pedirá la nueva contraseña y la confirmación de esta. <pre>Cambiando la contraseña del usuario root. Nueva contraseña: Vuelva a escribir la nueva contraseña: passwd: todos los tokens de autenticación se actualizaron exitosamente.</pre>

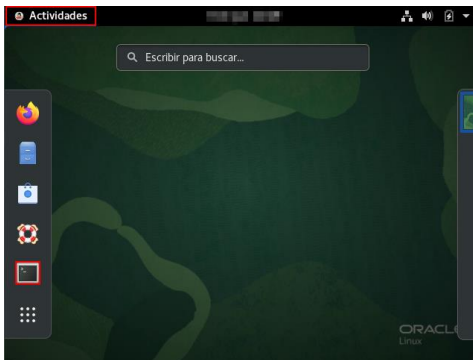
Paso	Descripción
51.	Cuando el proceso haya terminado se mostrará el siguiente mensaje. “passwd: todos los tokens de autenticación se actualizaron exitosamente.” Si no muestra ese mensaje, vuelva al paso 49 y repita la operación.
52.	Una vez actualizada la contraseña deberá adaptar la caducidad de la cuenta a los parámetros de seguridad requeridos, para ello ejecute el siguiente comando: <pre>\$ sudo /usr/bin/chage -m 2 -M 45 -W 10 root</pre>

ANEXO A.7.2. BUSQUEDA DE CUENTAS SIN CONTRASEÑA

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

- a) **[A.11.SEC-OL7]** Se eliminan los usuarios innecesarios del sistema.

De esta manera se mitiga la suplantación de identidad e intentos de acceso al sistema a través de cuentas por defecto del sistema.

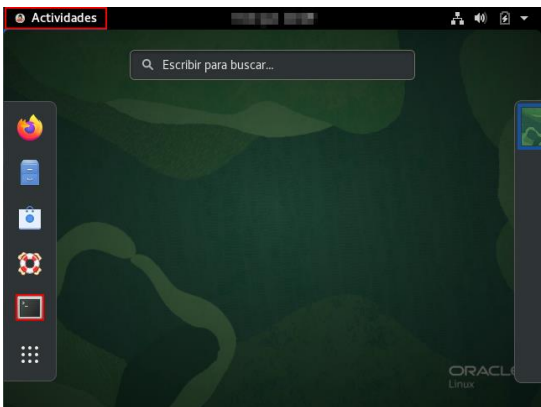
Paso	Descripción
53.	Si ha cerrado la “Terminal” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a la “Terminal” . 
54.	Ejecute los siguientes comandos. <pre>\$ sudo cat /etc/shadow cut -d":" -f2 grep ":\$" cut -d":" -f1 \$ sudo cat /etc/sudoers grep "NOPASSWD"</pre>
55.	Los comandos no deberán devolver ningún resultado por pantalla, si por el contrario sale algún resultado, significaría que esos usuarios no tienen contraseña configurada y deben ser eliminados. Nota: Si no conoce el proceso de eliminación de usuarios vaya al anexo “ANEXO A.5.1 USUARIOS INNECESARIOS Y SHELLS PREDETERMINADAS” .

ANEXO A.7.3. USUARIOS CON UID 0 QUE NO SEAN ROOT

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

- a) **[A.5.SEC-OL1]** Se controlan los permisos de inicio de sesión.

Se debe mantener un control sobre los cambios que realizan las cuentas con permisos de administrador sobre el sistema.

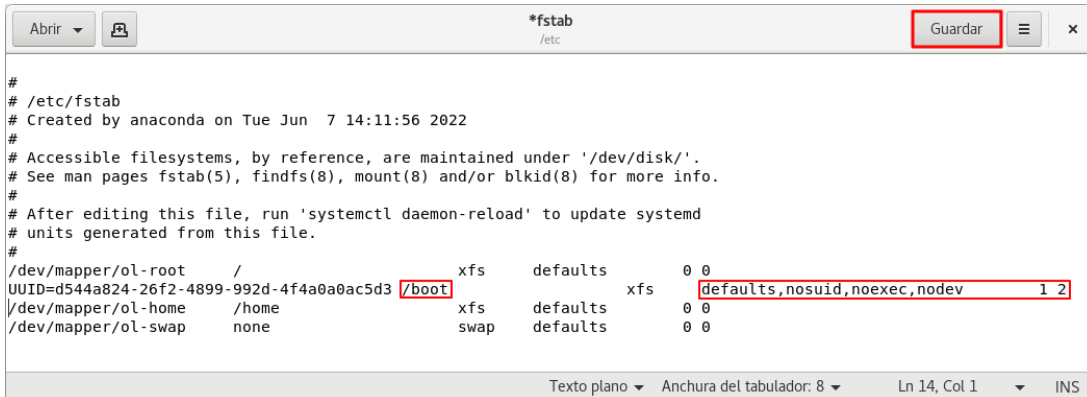
Paso	Descripción
56.	Si ha cerrado la “ Terminal ” en algún paso anterior, diríjase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
	
57.	Ejecute el siguiente comando.
	<pre>\$ sudo cat /etc/passwd cut -d":" -f1,3 grep -w 0 cut -d":" -f1</pre>
58.	El comando deberá devolver “ root ” como resultado por pantalla, si por el contrario sale algún resultado que no sea root, significará que los usuarios mostrados tienen “ UID ” 0 y por ende permisos demasiado elevados y deberán ser modificados o ser eliminados.
	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.

ANEXO A.7.4. 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-OL3]** Se modifican los permisos por particiones para evitar, por seguridad, que se puedan modificar y realizar acciones sobre ellas.

Paso	Descripción
59.	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 ”.
60.	Ejecute el siguiente comando e introduzca la contraseña si se le solicita.
	<pre>\$ sudo gnome-text-editor /etc/fstab</pre>

Paso	Descripción
61.	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).  Guarde la configuración del fichero pulsando en “Guardar”. Nota: Para instalaciones con una configuración de BIOS en modo “UEFI”, deberá aplicar las mismas configuraciones de seguridad a la partición “/boot/efi”.
62.	Para una correcta aplicación de los valores establecidos en el sistema de ficheros de Oracle 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. <pre>\$ sudo shutdown -r now</pre> Nota: Debe tener en consideración, que para realizar actualizaciones del kernel es posible que deba restablecer los valores de la partición “/boot” a defaults y posteriormente cuando la actualización finalice, revertirlos a los establecidos por esta guía.

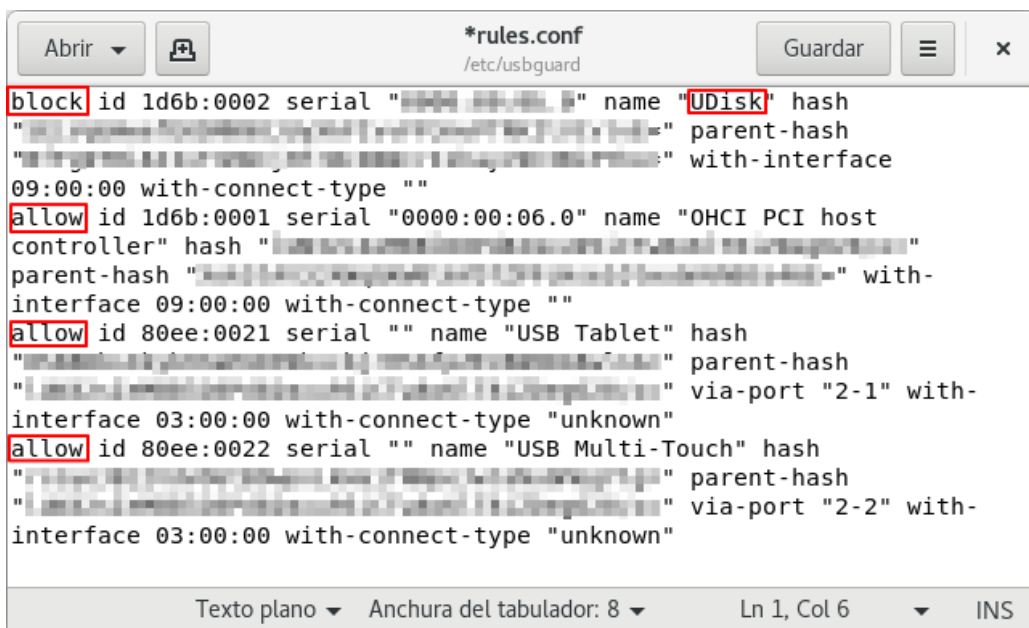
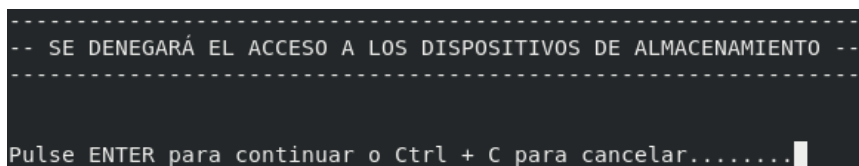
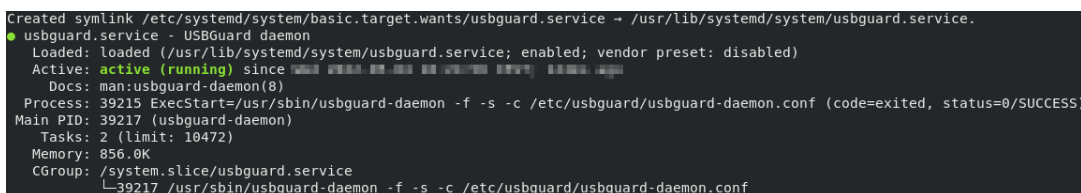
ANEXO A.7.5. LIMITACIÓN DE DISPOSITIVOS EXTRAÍBLES

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

- [A.3.SEC-OL10]** 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-OL13]** Se deshabilita el automontaje de dispositivos extraíbles en el sistema.
- [A.15.SEC-OL1]** Se controla el uso de medios de almacenamiento extraíbles.
- [A.23.SEC-OL1]** Se controla la instalación y uso de cualquier dispositivo conectado al equipo.
- [A.23.SEC-OL2]** 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
63.	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 ”.
64.	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 yum install usbguard</pre>
65.	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>
66.	Inserte todos los dispositivos extraíbles permitidos en el sistema para que se registren en el momento de la generación de políticas. 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.
67.	Ahora ejecute los siguientes comandos. <pre># usbguard generate-policy > /etc/usbguard/rules.conf</pre> Compruebe que se han generado las políticas de acceso de los dispositivos usb. <pre># cat /etc/usbguard/rules.conf more</pre> Nota: Si el fichero “/etc/usbguard/rules.conf”, se encontrase vacío. Repita este punto.
68.	Salga del usuario root escribiendo el siguiente comando. <pre># exit</pre>
69.	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>
70.	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 gnome-text-editor /etc/usbguard/rules.conf</pre>

Paso	Descripción
71.	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 del paso anterior se han permitido todos los dispositivos a excepción del dispositivo USB “UDisk” para posteriormente mostrar un ejemplo de denegación de acceso al mismo. 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.  <pre> *rules.conf /etc/usbguard block id 1d6b:0002 serial "0000:00:00.0" name "UDisk" hash "0000:00:00.0" parent-hash "0000:00:00.0" with-interface 09:00:00 with-connect-type "" allow id 1d6b:0001 serial "0000:00:06.0" name "OHCI PCI host controller" hash "0000:00:06.0" parent-hash "0000:00:06.0" with-interface 09:00:00 with-connect-type "" allow id 80ee:0021 serial "" name "USB Tablet" hash "0000:00:00.0" parent-hash "0000:00:00.0" via-port "2-1" with- interface 03:00:00 with-connect-type "unknown" allow id 80ee:0022 serial "" name "USB Multi-Touch" hash "0000:00:00.0" parent-hash "0000:00:00.0" via-port "2-2" with- interface 03:00:00 with-connect-type "unknown" </pre>
72.	Posteriormente si se encuentra en otra ruta, diríjase a “Scripts” y ejecute el script “CCN-STIC-620-Limitacion_usb.sh” mediante el comando indicado a continuación y pulse “Enter” para continuar. <pre>\$ sudo CCN-STIC-620_08-Limitacion_usb.sh</pre>  <pre> -- SE DENEGARÁ EL ACCESO A LOS DISPOSITIVOS DE ALMACENAMIENTO -- Pulse ENTER para continuar o Ctrl + C para cancelar..... </pre>
73.	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”.  <pre> Created symlink /etc/systemd/system/basic.target.wants/usbguard.service → /usr/lib/systemd/system/usbguard.service. ● usbguard.service - USBGuard daemon Loaded: loaded (/usr/lib/systemd/system/usbguard.service; enabled; vendor preset: disabled) Active: active (running) since 2020-08-08 10:00:00 UTC; 10min ago Docs: man:usbguard-daemon(8) Process: 39215 ExecStart=/usr/sbin/usbguard-daemon -f -s -c /etc/usbguard/usbguard-daemon.conf (code=exited, status=0/SUCCESS) Main PID: 39217 (usbguard-daemon) Tasks: 2 (limit: 10472) Memory: 856.0K CGroup: /system.slice/usbguard.service └─39217 /usr/sbin/usbguard-daemon -f -s -c /etc/usbguard/usbguard-daemon.conf </pre> El script le informará de su finalización con el mensaje “>>>>El SCRIPT ha finalizado<<<<”.

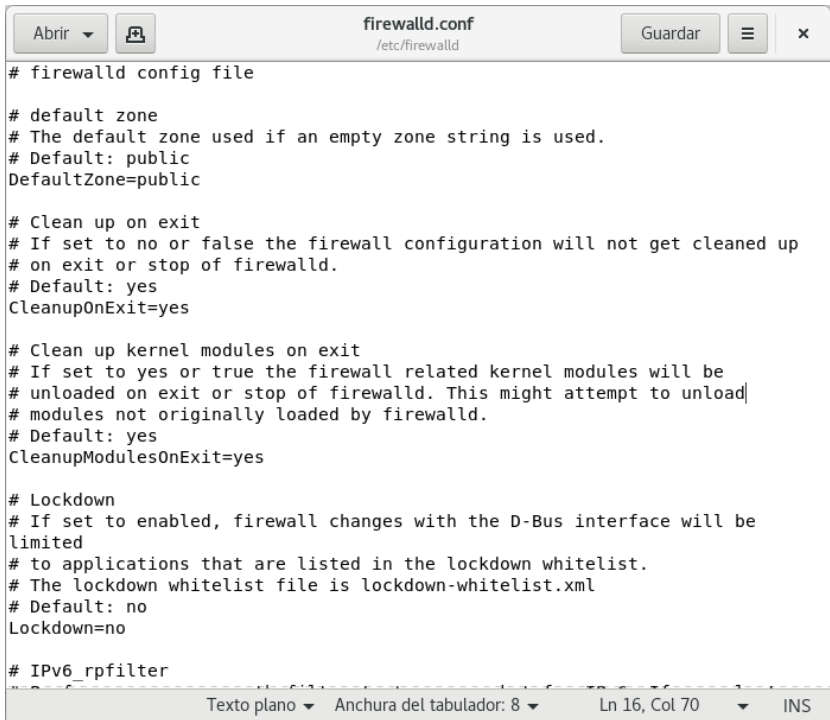
ANEXO A.7.6. PROTECCIÓN DE SERVICIOS DE RED

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

- a) **[A.8.SEC-OL3]** El sistema tiene un firewall local activado.
- b) **[A.11.SEC-OL5]** 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
74.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios del ENS en un perfilado intermedio.
75.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “ sudoers ”.
76.	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 ”.
77.	Se procede a configurar el Firewall de Oracle Linux. 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 Firewall. Ejecute el siguiente comando. \$ sudo systemctl start firewalld.service Compruebe su estado con siguiente comando. \$ sudo firewall-cmd --state
78.	Para visualizar la zona actual en la cual se encuentra el equipo se usará el siguiente comando. \$ sudo firewall-cmd --get-default-zone <pre>[aCdCmN620@OL8 ~]\$ sudo firewall-cmd --get-default-zone public</pre>
79.	Para conocer qué reglas están asociadas a dicha zona se puede ejecutar el siguiente comando. \$ sudo firewall-cmd --list-all <pre>[aCdCmN620@OL8 ~]\$ sudo firewall-cmd --list-all public (active) target: default icmp-block-inversion: no interfaces: enp0s3 sources: services: cockpit dhcpv6-client ssh ports: protocols: forward: no masquerade: no forward-ports: source-ports: icmp-blocks: rich rules:</pre>
80.	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 ”. \$ sudo firewall-cmd --list-ports --zone=internal

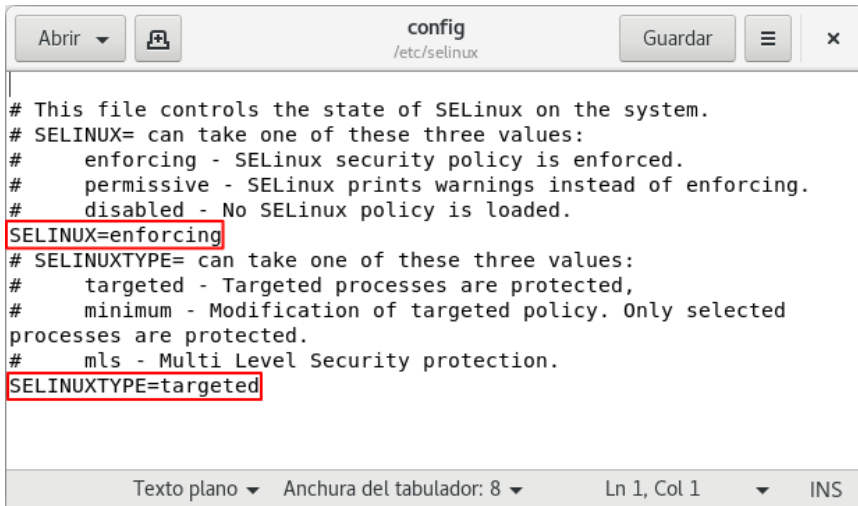
Paso	Descripción
81.	Se recomienda crear una zona propia de la que se tenga control total y pueda cubrir las necesidades de su organización. Para ello ejecute el siguiente comando siendo “NUEVAZONA” el nombre de la zona que se elegirá. <pre>\$ sudo firewall-cmd --new-zone=[NUEVAZONA] --permanent --add- \$ service=[SERVICIO]</pre> Por ejemplo, se añade una zona y se permite un servicio. <pre>\$ sudo firewall-cmd --new-zone=NUEVAZONA --permanent --add-service=ssh</pre>
82.	Para que la zona se refleje reinicie el Firewall con el siguiente comando. <pre>\$ sudo firewall-cmd --reload</pre> Compruebe que está agregada correctamente. <pre>\$ sudo firewall-cmd --permanent --get-zones</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo firewall-cmd --permanent --get-zones block dmz drop external home internal libvirt nm-shared public trusted work</pre>
83.	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. <pre>\$ sudo gnome-text-editor /etc/firewalld/firewalld.conf</pre>  <pre># firewalld config file # default zone # The default zone used if an empty zone string is used. # Default: public DefaultZone=public # Clean up on exit # If set to no or false the firewall configuration will not get cleaned up # on exit or stop of firewalld. # Default: yes CleanupOnExit=yes # Clean up kernel modules on exit # If set to yes or true the firewall related kernel modules will be # unloaded on exit or stop of firewalld. This might attempt to unload # modules not originally loaded by firewalld. # Default: yes CleanupModulesOnExit=yes # Lockdown # If set to enabled, firewall changes with the D-Bus interface will be # limited # to applications that are listed in the lockdown whitelist. # The lockdown whitelist file is lockdown-whitelist.xml # Default: no Lockdown=no # IPv6 rpfilter</pre>

ANEXO A.7.7. CONFIGURACIÓN ADICIONAL DE SEGURIDAD – SELINUX

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

- a) **[A.6.SEC-OL1]** Se refuerza la seguridad de los objetos sensibles del sistema.
- b) **[A.8.SEC-OL6]** 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
84.	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 ”.
85.	Se va a proceder a activar SELinux y configurarlo para que registre los eventos del sistema. Edite el fichero de configuración “/etc/selinux/config” y modifique los siguientes parámetros: SELINUX=Enforcing, SELINUXTYPE=targeted. <pre>\$ sudo gnome-text-editor /etc/selinux/config</pre>  Nota: Se comentan a continuación algunos parámetros del fichero de configuración: - SELINUX=enforcing: La opción SELINUX pone el modo en el que inicia SELinux. SELinux tiene tres modos: obligatorio (enforcing), permisivo (permissive) y deshabilitado (disabled). Cuando se usa modo obligatorio, la política de SELinux es aplicada y SELinux deniega el acceso basándose en las reglas de políticas de SELinux. Los mensajes de denegación se guardan. Cuando se usa modo permisivo, la política de SELinux no es obediente. Los mensajes son guardados. SELinux no deniega el acceso, pero se guardan las denegaciones de acciones que hubieran sido denegadas si SELinux estuviera en modo obediente. Cuando se usa el modo deshabilitado, SELinux está deshabilitado (el módulo de SELinux no se registra con el kernel de Linux). - SELINUXTYPE=targeted: La opción SELINUXTYPE selecciona la política a usar por SELinux. La política Destinada es la predeterminada. Cambie esta opción si quiere usar la política MLS. Para usar la política MLS, instale el paquete selinux-policy-mls; configure SELINUXTYPE=mls en /etc/selinux/config; y reinicie su sistema.

Paso	Descripción
86.	Para comprobar el estado de SELinux ejecute los siguientes comandos. <pre>\$ sudo getenforce</pre> <pre>\$ sudo sestatus</pre> <pre>[aCdCmN620@OL8 ~]\$ 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: 31</pre> Compruebe que SELinux se encuentre configurado como “enforcing”, “enabled” y “targeted”. En caso contrario repita los pasos anteriores.

ANEXO A.7.8. INTERFAZ WEB COCKPIT

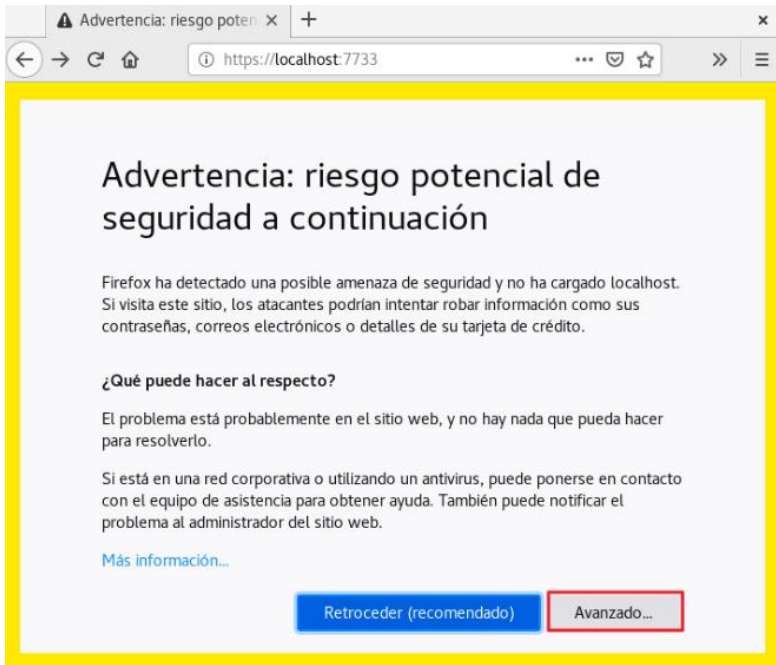
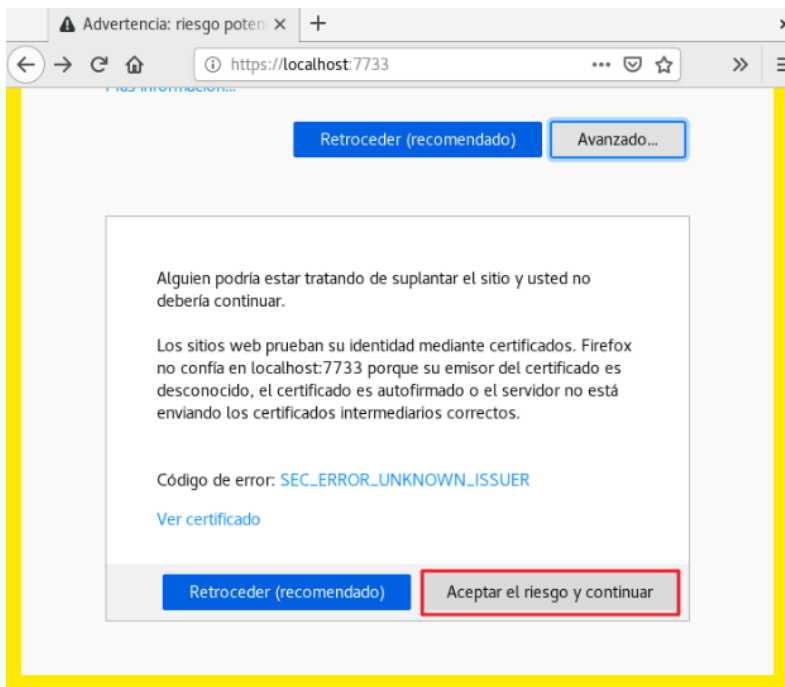
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

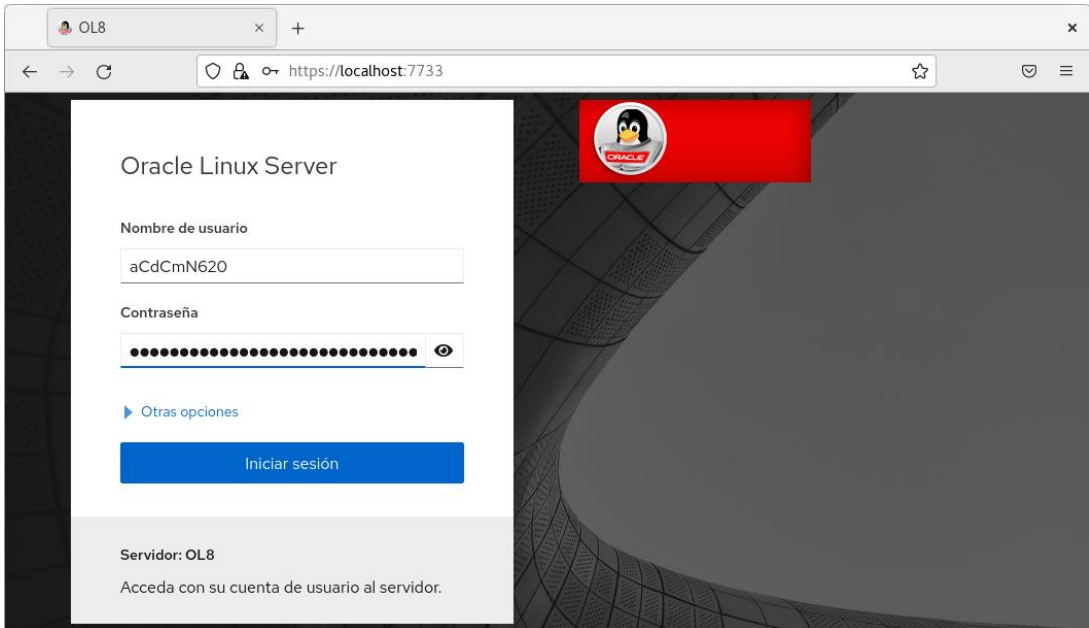
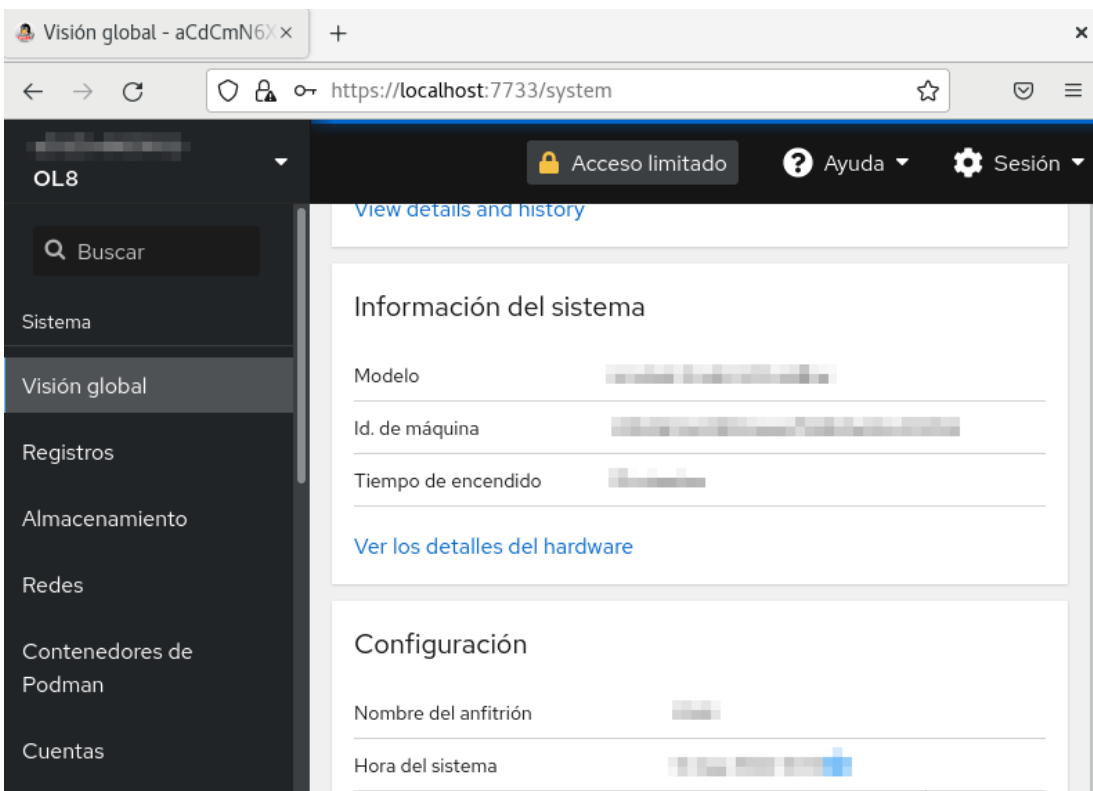
- a) [A.11.SEC-OL6] Sólo se permiten algoritmos de cifrado robustos en accesos al sistema.

Se deben configurar unos algoritmos robustos y puertos seguros para las comunicaciones a través de la red para mitigar ataques tipo Man in the middle.

Paso	Descripción
87.	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.
88.	Ejecute el siguiente comando para habilitar la funcionalidad cockpit. <pre>\$ sudo systemctl enable --now cockpit.socket</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo systemctl enable --now cockpit.socket Created symlink /etc/systemd/system/sockets.target.wants/cockpit.socket → /usr/lib/systemd/system/cockpit.socket.</pre>
89.	Compruebe el puerto de escucha de cockpit por medio del siguiente comando. <pre>\$ grep -i listen /usr/lib/systemd/system/cockpit.socket</pre> <pre>[aCdCmN620@OL8 ~]\$ grep -i listen /usr/lib/systemd/system/cockpit.socket ListenStream=9090</pre>

Paso	Descripción
90.	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. <pre>\$ sudo gnome-text-editor /usr/lib/systemd/system/cockpit.socket</pre> 
91.	Ejecute los siguientes comandos para que SELinux y firewalld permitan el uso de ese puerto para el interfaz web. <pre>\$ sudo semanage port -a -t websm_port_t -p tcp [PUERTO ELEGIDO]</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo semanage port -a -t websm_port_t -p tcp 7733</pre> <pre>\$ sudo firewall-cmd --permanent --zone=[ZONA HABILITADA] --add-port=[PUERTO ELEGIDO]/[PROTOCOLO]</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo firewall-cmd --permanent --zone=ZONAHABILITADA --add-port=7733/tcp success</pre>
92.	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. <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>[aCdCmN620@OL8 ~]\$ grep -i listen /usr/lib/systemd/system/cockpit.socket</pre> <pre>ListenStream=</pre> <pre>ListenStream=7733</pre>

Paso	Descripción
93.	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 operativo y no uno correctamente firmado por una entidad certificadora. Pulse sobre el botón “Avanzado...” para continuar. 
94.	Pulse sobre el botón “Aceptar el riesgo y continuar”. 

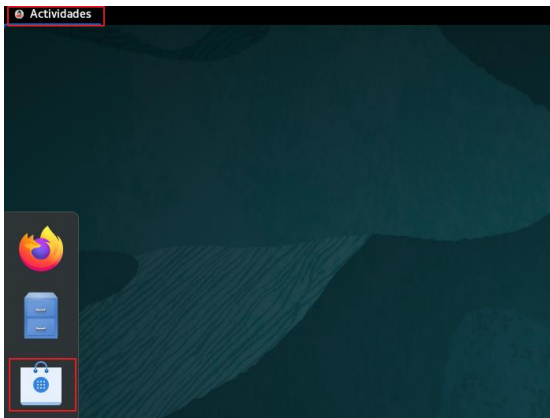
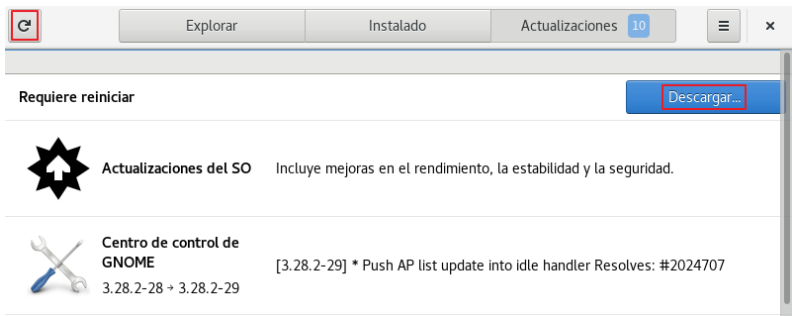
Paso	Descripción
95.	Se mostrará el interfaz de inicio de cockpit, donde deberá introducir las credenciales de su usuario y pulsar en el botón “Iniciar sesión”. 
96.	Se mostrará el panel de cockpit para la administración y monitorización del sistema. 

ANEXO A.7.9. APLICACIÓN DE ACTUALIZACIONES

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

a) **[A.8.SEC-OL2]** 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
97.	Diríjase a la barra de tareas superior, pulse sobre “Actividades” y seleccione el icono correspondiente a “Software”. 
98.	Una vez iniciada la aplicación, pulse sobre la pestaña “Actualizaciones”. 
99.	Pulse sobre el botón de la flecha de recargar. Comprobará si hay más actualizaciones, cuando finalice, si existen actualizaciones, pulse en el botón “Descargar...”. 

ANEXO A.7.10. INSTALACIÓN DE ANTIVIRUS

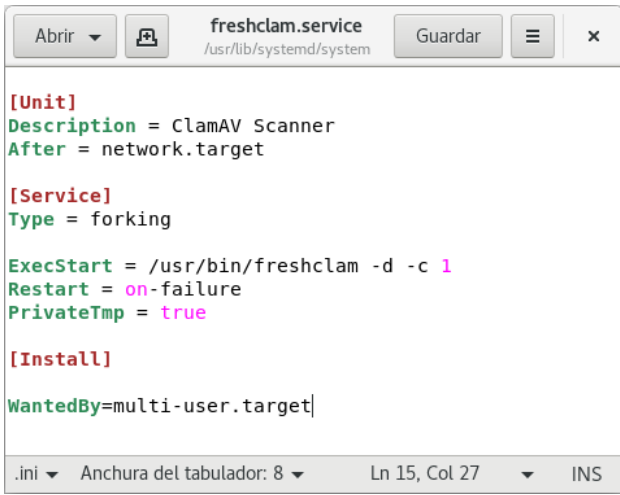
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

- a) **[A.4.SEC-OL2]** 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																																																																																																														
100.	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 ”.																																																																																																														
101.	A continuación, con el siguiente comando se descargará el antivirus, en este caso ClamAV. <pre>\$ sudo dnf install clamav clamav-data clamav-devel clamav-filessystem clamav-update clamd</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo dnf install clamav clamav-data clamav-devel clamav-filessystem clamav-update clamd</pre><pre>Oracle Linux 8 EPEL Packages for Development (x86_64) 9.3 MB/s 31 MB 00:03</pre><pre>Oracle Linux 8 EPEL Modular Packages for Development (x86_64) 1.4 MB/s 248 kB 00:00</pre><pre>Dependencias resueltas.</pre><table><thead><tr><th>Paquete</th><th>Arquitectura</th><th>Versión</th><th>Repositorio</th><th>Tam.</th></tr></thead><tbody><tr><td colspan="5">Instalando:</td></tr><tr><td>clamav</td><td>x86_64</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>2.7 M</td></tr><tr><td>clamav-data</td><td>noarch</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>219 M</td></tr><tr><td>clamav-devel</td><td>x86_64</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>54 k</td></tr><tr><td>clamav-filessystem</td><td>noarch</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>47 k</td></tr><tr><td>clamav-update</td><td>x86_64</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>131 k</td></tr><tr><td>clamd</td><td>x86_64</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>126 k</td></tr><tr><td colspan="5">Instalando dependencias:</td></tr><tr><td>clamav-lib</td><td>x86_64</td><td>0.103.6-1.el8</td><td>ol8_developer_EPEL</td><td>863 k</td></tr><tr><td>keyutils-libs-devel</td><td>x86_64</td><td>1.5.10-9.el8</td><td>ol8_baseos_latest</td><td>48 k</td></tr><tr><td>krb5-devel</td><td>x86_64</td><td>1.18.2-14.0.1.el8</td><td>ol8_baseos_latest</td><td>560 k</td></tr><tr><td>libcom_err-devel</td><td>x86_64</td><td>1.45.6-4.el8</td><td>ol8_baseos_latest</td><td>38 k</td></tr><tr><td>libkadm5</td><td>x86_64</td><td>1.18.2-14.0.1.el8</td><td>ol8_baseos_latest</td><td>187 k</td></tr><tr><td>libprelude</td><td>x86_64</td><td>5.2.0-1.el8</td><td>ol8_developer_EPEL</td><td>327 k</td></tr><tr><td>libselinux-devel</td><td>x86_64</td><td>2.9-5.el8</td><td>ol8_baseos_latest</td><td>200 k</td></tr><tr><td>libsepol-devel</td><td>x86_64</td><td>2.9-3.el8</td><td>ol8_baseos_latest</td><td>87 k</td></tr><tr><td>libverto-devel</td><td>x86_64</td><td>0.3.0-5.el8</td><td>ol8_baseos_latest</td><td>18 k</td></tr><tr><td>openssl-devel</td><td>x86_64</td><td>1:1.1.1k-6.el8_5</td><td>ol8_baseos_latest</td><td>2.3 M</td></tr><tr><td>pcr2-devel</td><td>x86_64</td><td>10.32-2.el8</td><td>ol8_baseos_latest</td><td>605 k</td></tr><tr><td>pcr2-utf16</td><td>x86_64</td><td>10.32-2.el8</td><td>ol8_baseos_latest</td><td>229 k</td></tr><tr><td>pcr2-utf32</td><td>x86_64</td><td>10.32-2.el8</td><td>ol8_baseos_latest</td><td>220 k</td></tr></tbody></table><pre>Resumen de la transacción</pre><pre>=====</pre><pre>Instalar 19 Paquetes</pre>	Paquete	Arquitectura	Versión	Repositorio	Tam.	Instalando:					clamav	x86_64	0.103.6-1.el8	ol8_developer_EPEL	2.7 M	clamav-data	noarch	0.103.6-1.el8	ol8_developer_EPEL	219 M	clamav-devel	x86_64	0.103.6-1.el8	ol8_developer_EPEL	54 k	clamav-filessystem	noarch	0.103.6-1.el8	ol8_developer_EPEL	47 k	clamav-update	x86_64	0.103.6-1.el8	ol8_developer_EPEL	131 k	clamd	x86_64	0.103.6-1.el8	ol8_developer_EPEL	126 k	Instalando dependencias:					clamav-lib	x86_64	0.103.6-1.el8	ol8_developer_EPEL	863 k	keyutils-libs-devel	x86_64	1.5.10-9.el8	ol8_baseos_latest	48 k	krb5-devel	x86_64	1.18.2-14.0.1.el8	ol8_baseos_latest	560 k	libcom_err-devel	x86_64	1.45.6-4.el8	ol8_baseos_latest	38 k	libkadm5	x86_64	1.18.2-14.0.1.el8	ol8_baseos_latest	187 k	libprelude	x86_64	5.2.0-1.el8	ol8_developer_EPEL	327 k	libselinux-devel	x86_64	2.9-5.el8	ol8_baseos_latest	200 k	libsepol-devel	x86_64	2.9-3.el8	ol8_baseos_latest	87 k	libverto-devel	x86_64	0.3.0-5.el8	ol8_baseos_latest	18 k	openssl-devel	x86_64	1:1.1.1k-6.el8_5	ol8_baseos_latest	2.3 M	pcr2-devel	x86_64	10.32-2.el8	ol8_baseos_latest	605 k	pcr2-utf16	x86_64	10.32-2.el8	ol8_baseos_latest	229 k	pcr2-utf32	x86_64	10.32-2.el8	ol8_baseos_latest	220 k
Paquete	Arquitectura	Versión	Repositorio	Tam.																																																																																																											
Instalando:																																																																																																															
clamav	x86_64	0.103.6-1.el8	ol8_developer_EPEL	2.7 M																																																																																																											
clamav-data	noarch	0.103.6-1.el8	ol8_developer_EPEL	219 M																																																																																																											
clamav-devel	x86_64	0.103.6-1.el8	ol8_developer_EPEL	54 k																																																																																																											
clamav-filessystem	noarch	0.103.6-1.el8	ol8_developer_EPEL	47 k																																																																																																											
clamav-update	x86_64	0.103.6-1.el8	ol8_developer_EPEL	131 k																																																																																																											
clamd	x86_64	0.103.6-1.el8	ol8_developer_EPEL	126 k																																																																																																											
Instalando dependencias:																																																																																																															
clamav-lib	x86_64	0.103.6-1.el8	ol8_developer_EPEL	863 k																																																																																																											
keyutils-libs-devel	x86_64	1.5.10-9.el8	ol8_baseos_latest	48 k																																																																																																											
krb5-devel	x86_64	1.18.2-14.0.1.el8	ol8_baseos_latest	560 k																																																																																																											
libcom_err-devel	x86_64	1.45.6-4.el8	ol8_baseos_latest	38 k																																																																																																											
libkadm5	x86_64	1.18.2-14.0.1.el8	ol8_baseos_latest	187 k																																																																																																											
libprelude	x86_64	5.2.0-1.el8	ol8_developer_EPEL	327 k																																																																																																											
libselinux-devel	x86_64	2.9-5.el8	ol8_baseos_latest	200 k																																																																																																											
libsepol-devel	x86_64	2.9-3.el8	ol8_baseos_latest	87 k																																																																																																											
libverto-devel	x86_64	0.3.0-5.el8	ol8_baseos_latest	18 k																																																																																																											
openssl-devel	x86_64	1:1.1.1k-6.el8_5	ol8_baseos_latest	2.3 M																																																																																																											
pcr2-devel	x86_64	10.32-2.el8	ol8_baseos_latest	605 k																																																																																																											
pcr2-utf16	x86_64	10.32-2.el8	ol8_baseos_latest	229 k																																																																																																											
pcr2-utf32	x86_64	10.32-2.el8	ol8_baseos_latest	220 k																																																																																																											
102.	Se continúa configurando SELinux para CLamAV. <pre>\$ sudo setsebool -P antivirus_can_scan_system 1</pre><pre>\$ sudo setsebool -P clamd_use_jit 1</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo setsebool -P antivirus_can_scan_system 1</pre><pre>[aCdCmN620@OL8 ~]\$ sudo setsebool -P clamd_use_jit 1</pre>																																																																																																														

Paso	Descripción
103.	Se buscan actualizaciones del propio antivirus con el siguiente comando. <pre>\$ sudo freshclam</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo freshclam ClamAV update process started at Fri Jun 10 10:46:29 2022 daily database available for update (local version: 26532, remote version: 26567) Current database is 35 versions behind. Downloading database patch # 26533... Time: 1.6s, ETA: 0.0s [=====>] 13.41KiB/13.41KiB Downloading database patch # 26534... Time: 0.1s, ETA: 0.0s [=====>] 16.52KiB/16.52KiB Downloading database patch # 26535...</pre>
104.	Se finaliza con la configuración del demonio de ejecución de ClamAV. <pre>\$ sudo sed -i 's/#LocalSocket \\/run/LocalSocket \\/run/g' /etc/clamd.d/scan.conf</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo sed -i 's/#LocalSocket \\/run/LocalSocket \\/run/g' /etc/clamd.d/scan.conf</pre>
105.	Se crea un nuevo fichero en el que se introducirá la nueva configuración. <pre>\$ sudo gnome-text-editor /usr/lib/systemd/system/freshclam.service</pre>  <pre>[Unit] Description = ClamAV Scanner After = network.target [Service] Type = forking ExecStart = /usr/bin/freshclam -d -c 1 Restart = on-failure PrivateTmp = true [Install] WantedBy=multi-user.target</pre>
106.	Por último, se habilitan y ejecutan los servicios del antivirus. <pre>\$ sudo systemctl start clamd@scan \$ sudo systemctl start freshclam</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo systemctl start clamd@scan [aCdCmN620@OL8 ~]\$ sudo systemctl start freshclam</pre> <pre>\$ sudo systemctl enable clamd@scan \$ sudo systemctl enable freshclam</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo systemctl enable clamd@scan Created symlink /etc/systemd/system/multi-user.target.wants/clamd@scan.service. → /usr/lib/systemd/system/clamd@.service. [aCdCmN620@OL8 ~]\$ sudo systemctl enable freshclam Created symlink /etc/systemd/system/multi-user.target.wants/freshclam.service → /usr/lib/systemd/system/freshclam.service.</pre>

Paso	Descripción
107.	Se comprueba que los servicios se estén ejecutando correctamente. <pre>\$ sudo systemctl status clamd@scan</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo systemctl status clamd@scan ● clamd@scan.service - clamd scanner (scan) daemon Loaded: loaded (/usr/lib/systemd/system/clamd@.service; enabled; vendor Active: active (running) since Fri 2022-08-11 11:11:11 CEST; 8min ago Docs: man:clamd(8) man:clamd.conf(5) https://www.clamav.net/documents/</pre> <pre>\$ sudo systemctl status freshclam</pre> <pre>[aCdCmN620@OL8 ~]\$ sudo systemctl status freshclam ● freshclam.service - ClamAV Scanner Loaded: loaded (/usr/lib/systemd/system/freshclam.service; enabled; vendor Active: active (running) since Fri 2022-08-11 11:11:11 CEST; 2min 55s ago</pre>

ANEXO A.7.11. 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-OL6]** 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
108.	Si ha cerrado la “ Terminal ” en algún paso anterior, dirijase a la barra de tareas superior, pulse sobre “ Actividades ” y seleccione el icono correspondiente a la “ Terminal ”.
109.	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 Oracle Linux. Para tal cometido ejecute el siguiente comando para localizar la unidad a la cual se va realizar el respaldo. <pre>\$ df -hT</pre> <pre>[aCdCmN620@OL8 Backup]\$ df -hT S.ficheros Tipo Tamaño Usados Disp Uso% Montado en devtmpfs devtmpfs 1,8G 0 1,8G 0% /dev tmpfs tmpfs 1,8G 0 1,8G 0% /dev/shm tmpfs tmpfs 1,8G 9,4M 1,8G 1% /run tmpfs tmpfs 1,8G 0 1,8G 0% /sys/fs/cgroup /dev/mapper/ol-root xfs 65G 6,9G 58G 11% / /dev/mapper/ol-home xfs 32G 10G 22G 32% /home /dev/sda2 xfs 1014M 462M 553M 46% /boot /dev/sda1 vfat 599M 5,0M 594M 1% /boot/efi tmpfs tmpfs 356M 32K 356M 1% /run/user/1001 /dev/sr0 iso9660 10G 10G 0 100% /run/media/aCdCmN620/ OL-8-5-0-BaseOS-x86_64 /dev/sdb xfs 97G 5,5G 92G 6% /DataBase</pre> 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.

Paso	Descripción
110.	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. <pre>\$ sudo xfs_freeze -f /DataBase</pre> 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”. Para realizar los archivos de respaldo, las unidades se deben encontrar o desmontadas o “congeladas”. Para más información de XFS, consulte el siguiente enlace: https://docs.oracle.com/cd/E37670_01/E37355/html/ol_xfs.html.
111.	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. <pre>\$ sudo xfsdump -l [NIVEL_DE_RESPALDO] -f [UBICACIÓN_FICHERO_RESPALDO] [SISTEMA_A_RESPALDAR]</pre> <pre>[aCdCmN620@localhost ~]\$ sudo xfsdump -l 0 -f /home/aCdCmN620/Backup/respaldo db /DataBase</pre> 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.
112.	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. <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 Feb 2020 16:07:43 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>

Paso	Descripción
113.	El comando concluirá mostrando los datos del proceso. <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 /home/aCdCmN620/Backup/respaldo_db OK (success) xfsdump: Dump Status: SUCCESS </pre>
114.	Revierta al estado original del medio al que realizó el respaldo, con la siguiente sentencia. <pre>\$ sudo xfs_freeze -u /DataBase</pre>

ANEXO A.7.12. 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-OL6]** Se dispone de medidas anti ransomware habilitadas.

Este riesgo se puede mitigar mediante la restauración satisfactoria de las copias de seguridad generadas previas al incidente que permitan restablecer la disponibilidad del sistema.

Paso	Descripción
115.	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”.
116.	Compruebe que el medio en el que va a realizar la restauración de los archivos de respaldo posee un sistema de ficheros “XFS”. <pre>\$ df -hT</pre> <pre> [aCdCmN620@OL8 Backup]\$ df -hT S.ficheros Tipo Tamaño Usados Disp Uso% Montado en devtmpfs devtmpfs 1,8G 0 1,8G 0% /dev tmpfs tmpfs 1,8G 0 1,8G 0% /dev/shm tmpfs tmpfs 1,8G 9,4M 1,8G 1% /run tmpfs tmpfs 1,8G 0 1,8G 0% /sys/fs/cgroup /dev/mapper/ol-root xfs 65G 6,9G 58G 11% / /dev/mapper/ol-home xfs 32G 10G 22G 32% /home /dev/sda2 xfs 1014M 462M 553M 46% /boot /dev/sda1 vfat 599M 5,0M 594M 1% /boot/efi tmpfs tmpfs 356M 32K 356M 1% /run/user/1001 /dev/sr0 iso9660 10G 10G 0 100% /run/media/aCdCmN620/ OL-8-5-0-BaseOS-x86_64 /dev/sdb xfs 97G 5,5G 92G 6% /DataBase </pre>

Paso	Descripción
117.	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. <pre>\$ sudo xfsrestore --f [UBICACIÓN_FICHERO_RESPALDO] [DESTINO_RESTAURACIÓN]</pre> <pre>[aCdCmN620@0L8 Backup]\$ sudo xfsrestore -f /home/aCdCmN620/Backup/respaldo_db /DataBase/ [sudo] password for aCdCmN620: 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 14 16:14:16 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/aCdCmN620/Backup/respaldo_db OK (success) xfsrestore: Restore Status: SUCCESS</pre>

