Cumplimiento del Esquema Nacional de Seguridad en servidores CentOS 7 con OpenSCAP

Autor: José Carlos Fandiño Calvo

Tutor: Pau Del Canto Rodrigo

Profesor: Victor García Font

Máster Universitario en Seguridad de las TIC

Seguridad Empresarial

Diciembre 2019

Créditos/Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Cumplimiento del Esquena Nacional de Seguridad en servidores CentOS 7 con OpenSCAP*
Nombre del autor:	*José Carlos Fandiño Calvo*
Nombre del colaborador/a docente:	*Pau Del Canto Rodrigo*
Nombre del PRA:	*Victor García Font*
Fecha de entrega (mm/aaaa):	*12/2019*
Titulación o programa:	*MISTIC*
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Bastionado, Configuración Segura, Política de seguridad, SCAP, XCCDF, OVAL, OpenScap, CentOS7, CCN-STIC-619, ENS*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo*

El protocolo SCAP permite la automatización de procedimientos relacionados con la seguridad (comprobación de vulnerabilidades o configuración automática de sistemas), por lo que constituye una herramienta útil para la comprobación e implementación de políticas de seguridad. El proyecto OpenSCAP proporciona diversas herramientas interoperables para trabajar con contenido SCAP.

El Centro Criptológico Nacional (CCN) es responsable de generar políticas de seguridad de la información aplicables dentro del sector público. La serie CCN-STIC contiene políticas y procedimientos relacionados con la seguridad de la información. La guía CCN-STIC-619 contiene un procedimiento manual de bastionado para clientes basados en CentOS7.

Este TFM implementa las recomendaciones contenidas la guía CCN-STIC-619 mediante contenido SCAP (reglas XCCDF y comprobaciones OVAL) lo que permite su aplicación y comprobación de forma automática. Se incluye también un conjunto de scripts de remedio, que permiten modificar automáticamente la configuración del sistema para adaptarse las reglas definidas.

La implementación realizada es verificada empleándola para comprobar una instalación por defecto de CentOS7 y ejecutando a continuación los scripts de remedio para adaptar la configuración a lo exigido en la norma.

Abstract (in English, 250 words or less):

SCAP protocol provides automation of security procedures, vulnerability assessment, automatic hardening and configuration of systems and other related security procedures. For this reason, is very appropriate to implement security policies. OpenSCAP project provides set of open and free inter-operable tools for SCAP content.

Centro Criptológico Nacional (CCN) is responsible of the Information Security policies for the government and public sector in Spain. CCN-STIC series contains a set of security policies and related procedures. CCN-STIC-619 contains official hardening instructions and security policy for client systems based on CentOS7.

This publication implements the recommendations of CCN-STIC-619 using SCAP content (XCCDF rules and OVAL checks), providing automatic capabilities to check and configure target systems. Also, a set of remediation scripts is developed, to modify the system configuration to conform with the rules when required.

The implementation is verified checking a clean install of CentOS7. Remediation scripts are applied to adapt the target system to the requirements

Palabras clave

Information Security, Secure Configuration, Hardening, SCAP, XCCDF, OVAL, OpenSCAP, CentOS7, Security Policy, CCN-STIC-619, ENS

Notaciones y Convenciones

Este apartado contiene las convenciones usadas para la tipografía a lo largo del TFM:

Texto Normal

Se utilizará esta tipografía para el texto normal del TFM.

```
Código / Scripts
Se utilizará esta tipografía para código, scripts, entrada o salida estándar de línea de comandos.
```

Índice

Índice de Figuras y tablas

1. Objeto del TFM

1.1. Introducción

El protocolo SCAP (*Security Content Automation Protocol*) constituye un conjunto de especificaciones, interoperables entre sí, cuyo desarrollo ha sido impulsado por el *National Institute of Standards and Technology* (NIST) de EEUU. SCAP permite la automatización de diversas actividades y disciplinas relacionadas con la seguridad de los sistemas de información, principalmente aquellas destinadas a detectar y solucionar vulnerabilidades en los sistemas y en su configuración.

SCAP permite la configuración automática de los sistemas, la comprobación de vulnerabilidades, la comprobación de instalación de parches de seguridad o la comprobación de controles de seguridad, garantizando la interoperabilidad entre productos y soluciones de seguridad. Define para ello un lenguaje común de expresiones estándar para describir contenido relacionado con la seguridad.

El Centro Criptológico Nacional (CCN), es responsable en nuestro país de las políticas de seguridad a implementar en los sistemas que deben cumplir los requisitos del esquema nacional de seguridad. Dentro del conjunto de guías y recomendaciones publicadas por el CCN, son habituales las guías de "securización" y/o bastionado, destinados a establecer configuraciones seguras para las plataformas y productos más comunes.

En el marco de la iniciativa anterior se sitúa la guía CCN-STIC-619, que tiene como objeto la configuración segura de la distribución CENTOS7 de Linux, en configuración de cliente independiente. Las guías del CCN siguen habitualmente la misma estructura, conteniendo una serie de recomendaciones para la configuración segura del producto, a partir de una instalación recién finalizada. La guía sigue el formato tradicional, conteniendo la descripción paso a paso para realizar de forma manual la configuración requerida. La única automatización soportada es la distribución por parte del CCN de unos scripts que deben ser ejecutados a mano, y que permiten aplicar y comprobar algunos (no todos) de los controles identificados en la guía.

La utilización del protocolo SCAP y de su implementación por el programa OpenSCAP, permite automatizar el proceso de comprobación y/o aplicación de controles de seguridad a una distribución, para garantizar la correcta configuración desde el punto de vista de la seguridad, por lo que la aplicabilidad de dicho protocolo para auditar/aplicar la configuración exigida por las guías STIC parece inmediata. Tras una investigación inicial, no se ha identificado, por parte del CCN ninguna publicación o distribución de contenido compatible con SCAP para la comprobación / aplicación de sus recomendaciones de seguridad.

1.2. Definición del trabajo a realizar

El TFM tiene como objetivo el desarrollo de la política de Seguridad empleando SCAP para CENTOS7 en configuración de Cliente Independiente, siguiendo las recomendaciones del Centro Criptológico Nacional incluidas en la guía CCN-STIC-619, editada en abril de 2019.

La política de Seguridad permite asegurar el cumplimiento de los requisitos del Esquema nacional de Seguridad. Para ello, se desarrollan tres perfiles, correspondientes a los niveles de Seguridad Alto, medio y bajo del ENS.

La política de seguridad se desarrolla y aplica, empleando OpenSCAP, a un sistema de referencia, para demostrar su funcionamiento. El trabajo desarrollado es novedoso porque permite, por primera vez, la comprobación automática de los requisitos de seguridad del ENS sobre una instalación de CENTOS de forma automática.

La política de seguridad desarrollada no está destinada a ser utilizada para sistemas en producción. Los mecanismos de chequeo de los controles de seguridad implantados, así como los scripts desarrollados para remediar automáticamente los controles no implementados son versiones básicas simplificadas destinadas a demostrar la funcionalidad objeto del TFM.

Finalmente, se plantean soluciones para automatizar el despliegue de la política de seguridad en entornos reales y para monitorizar, de forma continua, el cumplimiento de la política en un sistema en servicio.

1.3. Objetivos generales

Se incluye a continuación una lista de objetivos desarrollados dentro de este trabajo:

1. Estudio y comprensión de OpenSCAP, de sus componentes principales y sus capacidades
2. Estudio y comprensión de la guía CCN-STIC-619, que contiene requisitos para el bastionado de una instalación de CENTOS7
3. Desarrollo de políticas de seguridad, empleando OpenSCAP para el cumplimiento del ENS sobre CENTOS7
4. Definición y preparación de un entorno virtual que permita la verificación de la política desarrollada
5. Verificación de la política desarrollada
6. Diseño de una solución, empleando OpenSCAP para automatizar el despliegue de la política de seguridad en entornos reales
7. Demostración de una solución, empleando OpenSCAP para monitorizar de forma continua el cumplimiento de la política de seguridad en un entorno ya desplegado

1.4. Metodología y proceso de trabajo

Para la realización del trabajo se emplea una metodología basada en la descomposición en tareas y actividades previstas. Cada tarea será planificada, indicando su alcance, duración y resultados intermedios o finales previstos. El trabajo se ha estructurado en las siguientes fases:

A. Preparación del Plan de Trabajo
B. Introducción a SCAP y OpenSCAP
C. Revisión de la Guía CCN-STIC-619 para CentOS7
D. Desarrollo de la Política de Seguridad para CentOS7
E. Verificación y validación de la política desarrollada

A continuación, se indica el alcance de los trabajos a realizar dentro de cada fase:

A. Preparación del Plan de Trabajo.
- Definición del alcance del trabajo, objetivos, trabajos y actividades previstas, así como su planificación temporal

B. Introducción a SCAP y OpenSCAP
- Descripción del Protocolo SCAP. Descripción de los componentes del protocolo SCAP (XCCDF, OVAL, OCIL, CPE, CVE, CVSS, CCSS) según NIST SP 800-126
- Descripción del Proyecto OpenSCAP. Componentes y Herramientas. Descripción de las herramientas desarrolladas por el proyecto OpenSCAP (Base, Daemon, WorkBench, Timony, Anaconda Add-on) y aplicabilidad al propósito del TFM
- Políticas de Seguridad en SCAP. Concepto de política de seguridad en SCAP. Estructura y componentes de las políticas de seguridad.Aplicabilidad al propósito del TFM.

C. Guía CCN-STIC-619.
- Introducción al CCN-CERT. Introducción a las guías CCN-STIC. Resumen de las Recomendaciones de Seguridad para CentOS7 del CCN.

D. Desarrollo de la Política CCN-STIC-619 para OpenSCAP.

E. Demostración de la política desarrollada
- Entorno de demostración. Definición de un entorno destinado a comprobar el funcionamiento de la política desarrollada
- Demostración de la Política Desarrollada. Informes de resultados.

1.5. Planificación

A continuación, se indica el contenido previsto para las PEC a entregar durante la realización del TFM, así como la planificación prevista:

PEC1. Plan de Trabajo

PEC2. Entrega de la Memoria incluyendo
- Tarea A. Plan de Trabajo Revisado.
- Tarea B. SCAP y Open SCAP.
- Tarea C. Resumen de Recomendaciones CCN-STIC-619 para CENTOS7

PEC3. Actualización de la Memoria incluyendo
- Tarea D. Desarrollo Política CCN-STIC-619 para OpenSCAP

PEC4. Actualización final de la Memoria incluyendo:
- Tarea E. Definición y preparación entorno de verificación. Informe de resultados.

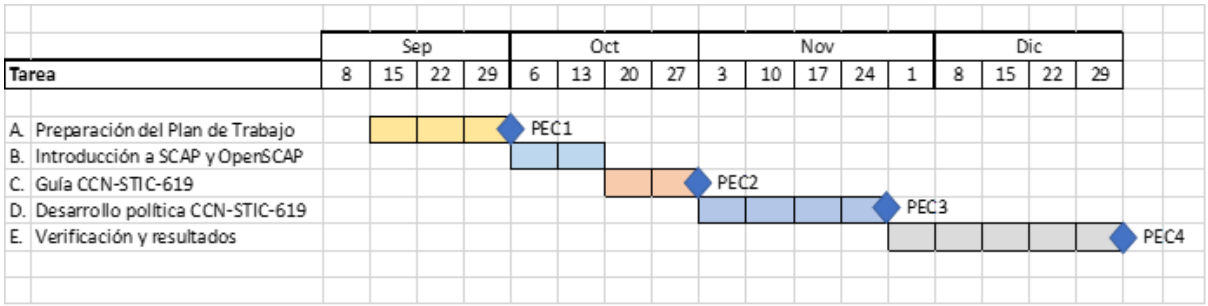

Figura 1: Planificación de trabajos

2. Introducción a SCAP y OpenSCAP

2.1. SCAP

SCAP es un conjunto de especificaciones para intercambio de información relacionada con la seguridad de los sistemas, que permite evaluar el cumplimiento de políticas de seguridad y detectar la presencia de versiones vulnerables de software y de la configuración de los sistemas (Waltermire, 2018).

SCAP proporciona formatos y nomenclaturas estándar para definir e intercambiar información entre herramientas de seguridad y también entre usuarios finales. SCAP cubre diversas áreas de la seguridad de los sistemas, como configuración automática, análisis de vulnerabilidades, comprobación de parches de seguridad o comprobación de controles de seguridad.

2.1.1.XCCDF

XCCDF es el acrónimo de “Extensible Configuration Checklist Description Format”. XCCDF proporciona un formato estándar, tipo XML, para especificar listas de comprobación e informar del resultado de las comprobaciones de seguridad realizadas sobre un sistema. Su definición formal ha sido impulsada por el NIST (Waltermire, 2012). El objetivo general es el de proporcionar a los analistas de seguridad TI una herramienta que permita crear listas de comprobación efectivas, automáticas, intercambiables y compatibles con diferentes herramientas.

Una lista de comprobación XCCDF es una colección organizada de reglas para un sistema o plataforma determinados. La capacidad de comprobación automática es necesaria para que la verificación de las reglas sea efectiva y consistente por motivos obvios. Incluso en despliegues sencillos o sistemas pequeños, la comprobación de las políticas de seguridad exigidas puede requerir la realización de gran cantidad de comprobaciones.

XCCDF facilita la creación de listas de comprobaciones de seguridad. Favorece la definición uniforme y homogénea de las comprobaciones a realizar, lo cual se traduce en una mejora de la seguridad de los sistemas y en una aplicación más homogénea y ajustada de las buenas prácticas de seguridad al uso.

XCCDF favorece y agiliza el intercambio de información entre profesionales de la seguridad, vendedores de herramientas de seguridad y auditores de seguridad, a la vez que hace posible el desarrollo de herramientas y soluciones de comprobación automática de la configuración y de los controles de seguridad requeridos para cada sistema.

XCCDF no está asociado con ningún fabricante o marca comercial. El formato es abierto y estándar, y al estar basado en XML, puede ser generado y mantenido con diversas herramientas. Puede ser extendido para incluir nueva funcionalidad, características y conjuntos de datos, sin impactar negativamente en las herramientas ya desarrolladas.

2.1.2.OVAL

OVAL es el acrónimo de "Open Vulnerability and Assessment Language". OVAL es un formato abierto, basado en XML, desarrollado de forma conjunta por la industria de seguridad, que permite el intercambio de información relacionada con el estado de la configuración de un sistema. OVAL proporciona un mecanismo estándar para realizar las comprobaciones de seguridad requeridas por XCCDF (Baker, 2011).

OVAL estandariza y facilita las tres fases del proceso de evaluación de un sistema que se indican a continuación:

1. Permite obtener y representar la configuración requerida para un sistema bajo evaluación

2. Permite analizar el sistema en evaluación para comprobar un estado determinado (p.ej. Si el sistema presenta una vulnerabilidad, si se ha aplicado un parche determinado, o si se ha configurado correctamente un servicio)

3. Permite generar de un informe detallado con el resultado del punto 2, indicando el resultado de las comprobaciones realizadas. Esto es: si el sistema es vulnerable o no conforme a una norma determinada.

En relación con SCAP, OVAL se utiliza para describir posibles vulnerabilidades de seguridad o la configuración deseada para un sistema. En este sentido, OVAL permite definir cuál debe ser la configuración segura para elementos como archivos, permisos, procesos o servicios en un sistema.

2.1.3.OCIL

OCIL es el acrónimo de "Open Ckecklist Interactive Language". OCIL define los mecanismos necesarios para definir cuestionarios, realizar preguntas al usuario del sistema y procesar e interpretar las respuestas. OCIL se utiliza, en el entorno SCAP, para gestionar aquellos casos en los que no es posible realizar una comprobación automática mediante OVAL. La definición formal del lenguaje ha sido impulsada por el NIST (Waltermire, 2011).

OCIL proporciona un procedimiento estándar, basado en XML, para estos casos que requieren intervención humana, para la evaluación no automática (manual) de la implantación un control de seguridad o de la configuración de un sistema o servicio.

Para ello, OCIL cuenta con las siguientes características principales:

- Soporte para la definición formal de preguntas (con respuestas de tipo booleano, numérico, texto o lista de opciones)
- Soporte para la definición de acciones necesarias en función de la respuesta obtenida del usuario

2.1.4.CPE

CPE es el acrónimo de “Common Platform Enumeration”. CPE es un diccionario público, definido y mantenido por el NIST (Cheikes, 2011) de sistemas TI, software y paquetes basado en un esquema estructurado de nombres. CPE es un mecanismo estándar y abierto que permite, de forma consensuada e interoperable, describir y enumerar todo tipo de activos, desde aplicaciones y sistemas operativos hasta elementos de hardware.

CPE permite identificar de manera única cada activo, dentro de una categoría o clase y permite la integración de las herramientas de monitorización de activos con las herramientas de comprobación automática de seguridad. Para ello, se usa en conjunción con OVAL y XCCDF para identificar el activo sobre el que se desea verificar un control de seguridad determinado.

2.1.5.CVE

CVE es el acrónimo de “Common Vulnerabilities and Exposures”. CVE es una lista de vulnerabilidades conocidas, incluyendo un identificador único, una descripción y una referencia pública a dicha vulnerabilidad, publicada en el sitio web cve.mitre.org.

CVE permite identificar de manera única una vulnerabilidad. Por ello, puede ser utilizado en diferentes contextos, como son la gestión de parches de seguridad, la detección de vulnerabilidades o la detección de intrusiones.

SCAP permite el uso de identificadores oficiales CVE cuyo estado sea “candidate” o “entry”.

2.1.6.CVSS

CVSS es el acrónimo de “Common Vulnerability Scoring System”. CVSS es un estándar abierto para evaluar vulnerabilidades de seguridad definido en por la organización FIRST (FIRST.org, 2019). CVSS permite asignar una puntuación numérica (de 0 a 10, siendo el 10 más severo) a una vulnerabilidad, facilitando así a los responsables de seguridad priorizar la mitigación, respuesta o el uso de recursos.

CVSS define tres indicadores diferentes para la severidad denominados base (base score), temporal (temporal score) y de entorno (environmental score). SCAP permite el uso de todas las puntuaciones CVSS de una vulnerabilidad (base, temporal y de entorno).

2.2. OpenSCAP

OpenSCAP es un conjunto de aplicaciones basadas en el protocolo SCAP que permiten a los administradores de sistemas y a los auditores de seguridad la evaluación, comprobación y aplicación automática o manual de controles de seguridad. OpenSCAP está disponible en internet y puede descargarse en la dirección www.openscap.org (OpenScap, 2019)

Se incluye a continuación una breve descripción de las principales herramientas proporcionadas por OpenSCAP.

2.2.1. OpenSCAP Base

OpenSCAP proporciona una librería (OpenSCAP Library) y una utilidad para línea de comandos (`oscap`) que permiten procesar contenido de acuerdo con el estándar SCAP. La librería permite el desarrollo de aplicaciones (o la integración con otras aplicaciones existentes) mientras que la herramienta de línea de comandos permite la comprobación automática de la configuración y las vulnerabilidades sobre un sistema determinado.

Ambas herramientas soportan actualmente (Diciembre 2019) la versión 1.2 de SCAP. Son también compatibles hacia atrás con las versiones 1.1 y 1.0. de SCAP.

Se indican a continuación las características principales de cada uno de los productos incluidos en OpenSCAP base:

- Librería OpenSCAP: librería utilizada para los productos SCAP Workbench, SCAP Timony y OpenSCAP daemon.
- Herramienta `oscap`: Soporta listas de comprobación mediante protocolos XCCDF/OVAL y genera los resultados correspondientes tras realizar la comprobación del sistema.

Por último, se incluye una captura de pantalla, con información de configuración típicamente mostrada por la herramienta `oscap`:

```
keko@Lenovo:~$ oscap --version
OpenSCAP command line tool (oscap) 1.2.9
Copyright 2009--2016 Red Hat Inc., Durham, North Carolina.

==== Supported specifications ====
XCCDF Version: 1.2
OVAL Version: 5.11.1
CPE Version: 2.3
CVSS Version: 2.0
CVE Version: 2.0
Asset Identification Version: 1.1
Asset Reporting Format Version: 1.1
```

2.2.2.OpenSCAP-daemon

OpenSCAP-daemon es un servicio que realiza evaluaciones periódicas siguiendo una planificación determinada empleando la herramienta `oscap`. Permite escanear sistemas completos en modo local o remoto, máquinas virtuales y contenedores. La comprobación puede realizarse una única vez o de manera periódica. El servicio ofrece interfaces de control vía línea de comandos y mediante Dbus.

2.2.3.SCAP Workbench

SCAP Workbench es una interfaz gráfica de usuario que permite realizar las tareas más habituales de comprobación de la configuración y vulnerabilidades, en modo local o sobre un sistema remoto, empleando un perfil determinado. Incluye capacidades para generar informes, en diferentes formatos, así como la posibilidad de personalizar/modificar el perfil XCCDF con una interfaz amigable y de almacenar dichos cambios.

A continuación, se muestra una captura de pantalla, con la aplicación configurada para comprobar un perfil PCI-DSS v3.2.1 sobre RHEL7/CentOS7.

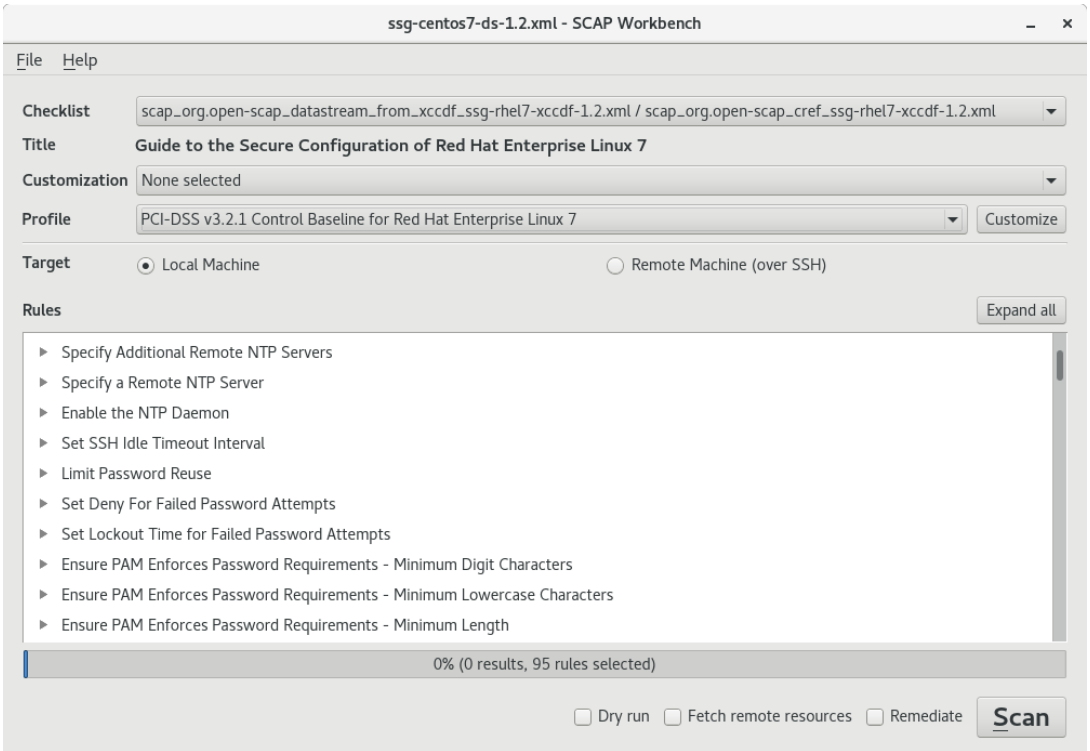

Figura 2: Ventana principal de SCAP Workbench

2.2.4.SCAP Timony

SCAP Timony es una herramienta que permite almacenar y consultar los resultados de las comprobaciones de seguridad realizadas mediante OpenSCAP. Se trata de un servidor de base de datos y almacenamiento construido sobre la librería OpenSCAP Library y que permite el despliegue integrado con otras herramientas compatibles con el modelo Ruby on RAILS.

Timony permite monitorizar el cumplimiento de las políticas de seguridad para todos los sistemas e infraestructuras de una organización.

2.2.5.OSCAP Anaconda Add-On

Anaconda es un instalador de Linux libre y de código abierto, usado principalmente en las distribuciones Red Hat, CentOS y Fedora. El add-on desarrollado por OpenSCAP para Anaconda permite aplicar el perfil de seguridad deseado (empleando XCCDF) durante el proceso de instalación del sistema operativo, de forma que se garantiza que la configuración es segura desde el primer arranque del sistema.

El add-on soporta dos modos de funcionamiento: atendido y desatendido, según se describe a continuación:

- En modo atendido, el usuario puede seleccionar el perfil de seguridad deseado durante el proceso de instalación del sistema operativo, a partir de una lista pre-configurada o bien descargarlo desde una url
- En modo desatendido, el plugin se configura automáticamente con el perfil deseado.

2.3. Políticas de seguridad con SCAP

SCAP emplea una combinación de SCCDF y OVAL/OCIL para la comprobación de requisitos de seguridad. Por un lado, el contenido XCCDF representa una colección estructurada de reglas de comprobación para un sistema determinado. El contenido XCCDF está compuesto por una o más reglas. Cada regla define una o varias comprobaciones de seguridad que deberán realizarse sobre el sistema, pero no define cómo debe realizarse la comprobación. En su lugar, apunta a otro contenido (habitualmente una definición en formato OVAL cuando la comprobación puede realizarse de forma automática) que indica cómo debe realizarse dicha la comprobación.

A continuación, se desarrolla una regla de ejemplo que comprueba que el sistema no permita configurar una cuenta de usuario con la contraseña en blanco. Para ello, se presentan y analizan los contenidos XCCDF y OVAL necesarios para la implementación de dicha regla.

2.3.1. Estructura de una regla XCCDF

A continuación, a modo de ejemplo, se describe en detalle la información contenida en una regla sencilla, que garantiza que no sea posible configurar una cuenta de usuario con la contraseña en blanco (rule_no_empty_passwords):

```
<Rule id="rule_no_empty_passwords" selected="false" severity="high">

<title>Prevent Login to Accounts With Empty Password</title>

<description>
If an account is configured for password authentication but does not have an assigned
password, it may be possible to log into the account without  authentication. Remove
any instances of the nullok option in /etc/pam.d/system-auth to prevent logins with
empty passwords.
</description>

<reference href="https://www.stigqter.com/SV-86561r3_rule.html"></reference>

<rationale>
If an account has an empty password, anyone could log in and run commands with the
privileges of that account. Accounts with empty passwords should never be used in
operational environments.
</rationale>

<fix id="no_empty_passwords" system="urn:xccdf:fix:script:sh">
        sed --follow-symlinks -i 's/\&lt;nullok\&gt;//g' /etc/pam.d/system-auth
        sed --follow-symlinks -i 's/\&lt;nullok\&gt;//g' /etc/pam.d/password-auth
</fix>

<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
<check-content-ref
        href="ssg-rhel7-oval.xml"
        name="oval:ssg-no_empty_passwords:def:1" />
</check>

<check system="http://scap.nist.gov/schema/ocil/2" >
<check-content-ref
        href="ssg-rhel7-ocil.xml"
        name="ocil:ssg no_empty_passwords_ocil:questionnaire:1" />
</check>
</Rule>
```

Figura 3: Ejemplo de regla XCCDF en formato XML

La tabla que se muestra a continuación explica la definición de cada uno de los campos y valores utilizados en el ejemplo:

Campo	Valor	Comentario
Rule ID	rule_no_empty_passwords	Identificador de la regla
Rule Severity	high	Indica la severidad en caso de incumplimiento de la regla
Title	Prevent Login to accounts with empy passwords	Título de la regla
Description	If an account is configured for password authentication but does not have an assigned password, it may be possible to log into	Descripción de la regla

	the account without authentication. Remove any instances of the “nullok” option in /etc/pam.d/system-auth to prevent logins with empty passwords.	
References	SV-86561r3	Referencia a listas de comprobación u otros documentos normativos que contienen requisitos relacionados con esta regla. En este caso, la regla SV-86561r3 de la recomendación DISA STIG para RHEL7
Rationale	If an account has an empty password, anyone could log in and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.	Justificación de la regla
Fix		Solución. Se trata de un script que modifica el estado del sistema para implementar el control de seguridad requerido
Fix ID	no_empty_passwords	Identificador de la solución propuesta
Fix Value	sed --follow-symlinks -i 's/\<nullok\>//g' /etc/pam.d/system-auth sed --follow-symlinks -i 's/\<nullok\>//g' /etc/pam.d/password-auth	En este caso la solución consiste en un pequeño script que elimina el valor “<nullok> de los siguientes archivos: /etc/pam.d/system-auth /etc/pam.d/password-auth
Check		Comprobación para evaluar el cumplimiento de la regla
Check System	http://oval.mitre.org/XMLSchema/oval-definitions-5	URI para el sistema de comprobación de la regla
Check-content-ref	href="ssg-rhel7-oval.xml" name="oval:ssg-no_empty_passwords:def:1"	Referencia a Código OVAL para la comprobación de la regla
Check		Comprobación para evaluar el cumplimiento de la regla
Check System	http://scap.nist.gov/schema/ocil/2	URI para el sistema de comprobación de la regla
Check-content-ref	href="ssg-rhel7-ocil.xml" name="ocil:ssg-no_empty_password:quest:1"	Referencia a Código OCIL para la comprobación de la regla

Tabla 1: Campos para definición de una regla empleando XCCDF

2.3.2.Estructura de una comprobación OVAL

Continuando con el ejemplo, se describe en detalle la información contenida en una comprobación OVAL, que determina si es posible configurar una cuenta de usuario con la contraseña en blanco.

```
<definition class="compliance" id="oval:ssg-no_empty_passwords:def:1" version="1">

<metadata>
        <title>No nullok Option in /etc/pam.d/system-auth</title>
        <affected family="unix"><platform>CentOS 7</platform></affected>
        <description>
                The file /etc/pam.d/system-auth should not contain the nullok option
        </description>
        <reference ref_id="no_empty_passwords" source="ssg" />
        </metadata>

<criteria>
        <criterion
                comment="make sure the nullok option is not used in /etc/pam.d/system-auth"
                test_ref="oval:ssg-test_no_empty_passwords:tst:1" />
        </criteria>

</definition>
```

Figura 4: Ejemplo de comprobación OVAL en formato XML

La tabla que se muestra a continuación explica la definición de cada uno de los campos y valores utilizados en el ejemplo:

Campo	Valor	Comentario
Definition ID	oval:ssg-no_empty_passwords:def:1	Identificador comprobación
Definition Class	compliance	Indica que la comprobación define la conformidad con una política de seguridad
Definition Version	1	Versión de la definición
Metadata		
Title	No nullok Option in /etc/pam.d/system-auth	Título de la definición
Affected Platform	unix: CentOS 7	Sistema operativo o aplicación para la que la definición es aplicable
References	ref_id="no_empty_passwords" source="ssg"	Referencia a listas de comprobación u otros documentos relacionados con la definición
Description	The file /etc/pam.d/system-auth should not contain the nullok option	Descripción detallada de la definición
Criteria		
Definition Reference	oval:ssg-test_no_empty_passwords:tst:1	Identificador del test OVAL a realizar (criterion), para verificar la regla
Definition Comment	Make sure the nullok option is not used in /etc/pam.d/system-auth	Comentario

Tabla 2: Campos para definición de una comprobación empleando OVAL

La comprobación a realizar se identifica como `oval:ssg-test_no_empty_passwords:tst:1`. Continuando con el ejemplo, veamos cómo se realiza su definición mediante contenido OVAL:

```
<test
        check="all"
        check_existence="none_exist"
        comment="make sure nullok is not used in /etc/pam.d/system-auth"
        id="oval:ssg-test_no_empty_passwords:tst:1"
        version="1">

        <object object_ref="oval:ssg-object_no_empty_passwords:obj:1" />

        </test>

<object
        id="oval:ssg-object_no_empty_passwords:obj:1"
        version="1">

        <filepath>/etc/pam.d/system-auth</ns7:filepath>
        <pattern operation="pattern match">^[^#]*\bnullok\b.*$</pattern>
        <instance datatype="int">1</instance>

        </object>
```

Figura 5: Definición de comprobación OVAL en formato XML

Como se puede ver en la figura, la comprobación consiste en verificar que ninguna línea (‘none exist’) del archivo /etc/pam.d/system-auth contiene la cadena ‘nullok’. La comprobación se realiza empleando una comparación mediante una expresión regular.

3. Guía CCN-STIC-619

3.1. CCN y Guías CCN-STIC

El Centro Criptológico Nacional (CCN) es el organismo responsable, dentro del estado español, de la seguridad de la información del sector público, así como de determinadas empresas y organizaciones de interés estratégico, según se indica en el RD 421/2004 (BOE num. 68 de 19 de Marzo de 2004).

En este contexto, el CCN es responsable de la serie normativa CCN-STIC, que contiene normas, instrucciones, guías y recomendaciones para la seguridad de las tecnologías de la información y las comunicaciones. La serie CCN-STIC promueve la difusión de los principios básicos de seguridad, de requisitos mínimos de seguridad y de las medidas de protección necesarias para garantizar la seguridad de la información en los sistemas.

La serie CCN-STIC, se estructura de acuerdo con el siguiente esquema:

Serie	Objeto
000	Políticas
100	Procedimientos
200	Normas
300	Instrucciones Técnicas
400	Guías Generales
500	Guías de entornos windows
600	Guías de otros entornos
800	Guía del ENS
900	Informes Técnicos

Tabla 3: Series de la normativa CCN-STIC

La guía número 619 del Centro Criptológico Nacional (CCN-STIC-619, 2019) pertenece a la serie 600 de guías para entornos diferentes de Windows y contiene un conjunto de recomendaciones para la configuración segura del sistema operativo CentOS, como cliente independiente y de acuerdo con los requisitos del esquema nacional de seguridad.

3.2. Recomendaciones de seguridad para CentOS 7

En este apartado se incluye un resumen de las recomendaciones de seguridad contenidas en la guía CCN-STIC-619. Este TFM tiene por objeto la implementación de dichas recomendaciones mediante protocolo SCAP para facilitar su comprobación automática.

La tabla que se muestra a continuación contiene una lista controles de seguridad extraídos del contenido de la guía, agrupados por categorías. Se asigna una categoría y un identificador a cada regla de seguridad para luego poder ser referenciados durante su implementación.

Categoría	Control	
SI: Protección del sistema		
	SI.1	Particiones y sistemas de archivos
	SI.2	Configuración segura de arranque
	SI.3	Configuración segura de particiones
	SI.4	Configuración segura de red
	SI.5	Configuración segura del kernel
	SI.6	Configuración de TCP wrappers
	SI.7	Seguridad de las contraseñas
US: Recursos de usuario		
	US.1	Configuración de volcados de memoria
	US.2	Limitación de recursos de usuario
	US.3	Bloqueo de atajos críticos
	US.4	Establecimiento de cuotas de disco
AS: Acceso al Sistema		
	AS.1	Configuración de banners
	AS.2	Configuración de SSH
	AS.3	Configuración de Autenticación
	AS.4	Configuración de intentos de acceso
EN: Elementos no necesarios		
	EN.1	Eliminación de servicios no necesarios
	EN.2	Eliminación de paquetes no necesarios
	EN.3	Eliminación de usuarios no necesarios
PE: Configuración de permisos y entornos		
	PE.1	Configuración de entornos de usuario
	PE.2	Configuración de directorios de usuario
	PE.3	Configuración de permisos de usuario
	PE.4	Configuración de automatización de tareas

Tabla 4: Controles de seguridad extraídos de CCN-STIC-619

Los apartados siguientes recogen la definición detallada de cada uno de los controles anteriores.

3.2.1. SI1. Particiones y sistemas de archivos

Se recomienda utilizar XFS como sistema de archivos, opcionalmente cifrado. El sistema estará configurado con los siguientes puntos de montaje en particiones de disco diferentes:

- /
- /boot
- /boot/efi
- /var
- /tmp
- /var/log
- /home
- /var/log/audit
- /var/www
- swap

3.2.2. SI2. Configuración segura de arranque

Se recomiendan los siguientes controles sobre el gestor de arranque:

- Bloquear el acceso a la línea de comandos del Grub.
- Bloquear la posibilidad de edición de las entradas del Grub.
- Bloquear la posibilidad de ejecución de todas las entradas del Grub.

3.2.3. SI3. Configuración segura de particiones

Se recomiendan las siguientes opciones de montaje de las particiones:

Partición	**Opciones de montaje**
/boot	noauto, noexec, nodev, nosuid, ro
/boot/efi	umask=0077, shortname=winnt <dump> 0 <pass> 0.
/usr	nodev, ro
/opt	nodev, ro
/var/log	nodev, noexec, nosuid, rw
/var/log/audit	nodev, noexec, nosuid, rw
/var/www	nodev, noexec, nosuid, rw
/home	nodev, noexec, nosuid, rw
/tmp	nodev, noexec, nosuid, rw
/media	nodev, noexec, nosuid, rw

/swap	defaults, <dump> 0 <pass> 0
/	rw

Tabla 5: Opciones de montaje recomendadas por CCN-STIC-619 para CentOS7

3.2.4. SI.4 Configuración segura de red

Se recomienda utilizar direccionamiento IP estático, en lugar de DHCP/BOOTP

3.2.5. SI.5 Configuración segura del kernel

Se recomienda la siguiente configuración segura para el kernel del sistema operativo:

- Deshabilitar respuesta a peticiones ICMP (p.ej. *ping*)
- Deshabilitar enrutado de paquetes entre interfaces
- Deshabilitar la modificación de tablas de enrutamiento
- Deshabilitar el *source routing*
- Habilitar los logs para paquetes anormales o excepcionales
- Deshabilitar la respuesta a peticiones *broadcast*
- Deshabilitar el tratamiento de mensajes de error mal formados
- Habilitar la Protección contra ante ataques *tcp syn*
- Habilitar *reverse path filtering*
- Deshabilitar vulnerabilidad de marca de tiempo en TCP
- Deshabilitar la capacidad ipv6
- Deshabilitar la generación de *core dumps* de programas con SUID
- Configurar Tamaño máximo de las colas de espera de TCP

3.2.6. SI.6 Configuración segura de tcp wrappers

Se recomienda la siguiente configuración:

- /etc/hosts.allow contendrá los equipos a los que se permite el acceso
- /etc/host.deny contendrá “ALL:ALL”

3.2.7. SI.7 Seguridad de las contraseñas

Se recomiendan las siguientes características para la seguridad de las contraseñas:

- Longitud mínima: 8 caracteres
- Incluir Mayúsculas y minúsculas
- Incluir signos de puntuación y números
- Evitar palabras o frases comunes que puedan figurar en cualquier diccionario

3.2.8. SI.8 Configuración para auditoría

Se recomienda establecer un mecanismo de rotado de registros. Se generarán 12 registros con un tamaño máximo de 10Mb cada uno.

3.2.9. US.1 Configuración de volcados de memoria

Se recomienda deshabilitar los volcados de memoria (*core dump*) en caso de error de un programa en ejecución.

3.2.10. US.2 Limitación de recursos de usuario

Se recomienda limitar la cantidad de procesos, memoria y conexiones permitidas por usuario, modificando el archivo /etc/security/limits.conf.

Se recomienda limitar el número máximo de hilos concurrentes en el sistema, modificando el archivo /etc/sysctl.conf.

3.2.11. US.3 Bloqueo de atajos críticos

Se recomienda deshabilitar la combinación de teclas Ctrl-Alt-Supr.

3.2.12. US.4 Establecimiento de cuotas

Se recomienda el establecimiento de cuotas de disco a la partición /home.

3.2.13. AS.1 Configuración de avisos

Se recomienda configurar los avisos (*banners*) de acceso al sistema para que muestren un aviso legal previniendo de las consecuencias del acceso no autorizado.

3.2.14. AS.2 Configuración de SSH

Se recomienda la siguiente configuración para el servicio SSH

- Se forzará el uso de la versión 2 del protocolo.
- Se denegará el uso de aplicaciones gráficas de modo remoto por medio de X11
- Se configurarán los usuarios no administradores como acceso denegado.
- Se limitará el tiempo total para hacer login en 120 segundos.
- Se establecerá el tiempo mínimo de inactividad antes de la desconexión.
- Se deshabilitará la emulación de rsh.
- Se deshabilitará la autenticación basada en host de SSH
- Se denegarán los inicios de sesión root por medio de SSH
- Se denegarán los accesos por medio de usuarios sin contraseña.
- Se configurará correctamente un banner que disuada a los posibles atacantes.
- Se garantizará que los usuarios no puedan usar variables de entorno al demonio SSH.
- Se configurará el uso únicamente del protocolo SSH con los algoritmos de cifrado permitidos.

3.2.15. AS.3 Configuración de autenticación

Se recomienda la siguiente configuración para el módulo pam_faillock.so:

- Se contabilizarán los intentos fallidos de acceso o cambio de privilegios mediante su.
- Se recordarán las 7 últimas contraseñas de cada usuario para evitar su repetición.
- Se limitará el acceso de usuarios wheel a cuentas administrativas

3.2.16. AS.4 Configuración de intentos de acceso

Se recomienda la siguiente configuración:

- Número máximo de intentos de acceso fallidos: 3 intentos.
- Se bloquearán aquellas cuentas que superen 5 intentos fallidos.
- Se fijará un máximo de 5 intentos de acceso fallidos para *root* antes de bloquear la cuenta
- El tiempo máximo permitido para acceder al sistema: 60 segundos.
- Evitar que el sistema indique cuando el usuario es desconocido para el mismo.
- El tiempo de retardo tras un intento fallido: 10 segundos.
- Se registrarán los intentos fallidos de acceso al sistema.

3.2.17. EL.1 Desactivación de servicios no necesarios

Se recomienda desactivar los servicios que no sean necesarios.

En nuestro caso, se considerará que los siguientes servicios del sistema deben ser desactivados:

- cups

3.2.18. EL.2 Eliminación de paquetes no necesarios

Se recomienda la eliminación de paquetes huérfanos y de paquetes no necesarios.

En nuestro caso, se considerará que los siguientes paquetes instalados con el sistema no son necesarios, por lo que deberán ser desinstalados:

- gnome-weather
- gnome-contacts

3.2.19. EL.3 Eliminación de usuarios no necesarios

Se recomienda la eliminación de los usuarios creados automáticamente durante la instalación del sistema que no sean necesarios.

En nuestro caso, se considerará que los siguientes usuarios de la instalación por defecto no son necesarios:

- ftp
- games

3.2.20. PE.1 Configuración de entornos de usuario

Se recomienda la siguiente configuración para el fichero /etc/profile:

- PATH no debe incluir el directorio actual (.)
- Tiempo máximo de inactividad (TMOUT): 600
- Tamaño máximo del historial de comandos (HISTSIZE): 1000

Se recomienda la siguiente configuración para el fichero /etc/bashrc:

- Mascara de usuario por defecto (umask): 027

3.2.21. PE.2 Configuración de directorios de usuario

Se recomienda que los directorios /home de los usuarios no permitan a otros usuarios acceder ni modificar su contenido (modo de acceso 0700)

3.2.22. PE.3 Configuración de permisos de usuario

Se comprobarán los permisos de los archivos /etc/passwd, /etc/group y /etc/shadow. El propietario de los tres debe ser root, con grupo root; los permisos de los dos primeros deben permitir la lectura por parte de todos los usuarios del sistema y la modificación únicamente por root (0644), mientras que el fichero de contraseñas shadow únicamente debe ser leído por root.

Se comprobarán todos aquellos directorios en los que los usuarios del sistema tengan permisos de escritura. Deberán protegerse utilizando el “sticky bit”, que previene que usuarios borren contenidos creados por otros usuarios.

Será necesario identificar aquellos ficheros que puedan ser modificados por todos los usuarios, independientemente de los permisos que posean.

Será necesario identificar aquellos ficheros que tengan activado el bit de SUID o SGID.

3.2.23. PE.4 Configuración de automatización de tareas

Se recomienda crear los ficheros /etc/cron.allow y /etc/at.allow en los que se incorporarán los nombres de los usuarios que pueden utilizar el servicio de automatización de tareas. Sólo el usuario root tendrá capacidad para ello (Mode = 644)

4. Diseño

4.1. Lista de Reglas XCCDF

Las recomendaciones de seguridad contenidas en el apartado anterior se implementarán mediante reglas XCCDF y comprobaciones OVAL.

A continuación, se incluye una tabla que muestra el identificador asignado a las diferentes reglas XCCDF. La tabla incluye también las tres categorías de seguridad del ENS (Alta, Media, Baja) identificadas por la norma, así como las recomendaciones incluidas en cada categoría. Las categorías del ENS serán implementadas haciendo uso de perfiles (profiles) de XCCDF:

Regla			**Identificador**	**ENS**		
SI: Protección del sistema				**A**	**M**	**B**
	SI.1	Particiones y sistemas de archivos	test_system_partitions	Si	Si	Si
	SI.2	Configuración segura (arranque)	test_grub2_secure_boot_enabled	Si	Si	Si
	SI.3	Configuración segura (particiones)	test_secure_mount_options	Si	Si	Si
	SI.4	Configuración segura (red)	test_secure_network_configuration	Si	Si	Si
	SI.5	Configuración segura (kernel)	test_kernel_parametes	Si	**No**	**No**
	SI.6	Configuración TCP wrappers	test_secure_tcp_wrappers	Si	Si	Si
	SI.7	Seguridad de las contraseñas	test_password_quality	Si	Si	Si
	SI.8	Configuración para Auditoría	test_audit_configuration	Si	Si	**No**
US: Recursos de usuario						
	US.1	Configuración volcados memoria	test_core_dumps	Si	Si	Si
	US.2	Limitación recursos usuario	test_user_limits	Si	Si	Si
	US.3	Bloqueo de atajos críticos	test_ctrl_alt_del_reboot_disabled	Si	Si	Si
	US.4	Establecimiento cuotas disco	test_disk_quotas	Si	Si	Si
AS: Acceso al Sistema						
	AS.1	Configuración de banners	test_login_banners_enabled	Si	Si	Si
	AS.2	Configuración SSH	test_ssh_configuration	Si	Si	Si
	AS.3	Configuración de Autenticación	test_auth_configuration	Si	Si	Si
	AS.4	Configuración intentos de acceso	test_login_configuration	Si	Si	**No**
EN: Elementos no necesarios						
	EL.1	Eliminación servicios no necesarios	test_services_not_required	Si	Si	Si

	EL.2	Eliminación paquetes no necesarios	test_packages_not_required	Si	Si	Si
	EL.3	Eliminación usuarios no necesarios	test_users_not_required	Si	Si	Si
PE: Configuración de permisos y entornos						
	PE.1	Configuración entornos de usuario	test_user_environment	Si	Si	Si
	PE.2	Configuración directorios de usuario	test_user_directories	Si	Si	Si
	PE.3	Configuración permisos de usuario	test_user_permissions	Si	Si	Si
	PE.4	Configuración automatiz. de tareas	test_restrict_at_cron_users	Si	Si	Si

Tabla 6: Lista de reglas XCCDF para CCN-STIC-619

4.2. Elementos OVAL

Este apartado describe brevemente los elementos OVAL utilizados en la implementación. La tabla a continuación incluye los tipos de objetos utilizados y su función.

Objeto OVAL	Función
environmentvariable58	Permite comprobar el valor de una variable de entorno
file	Permite comprobar atributos de un fichero (existencia, permisos, etc..)
partition	Permite comprobar atributos de un punto de montaje en el sistema
rpminfo	Permite comprobar atributos y versión de un paquete instalado en el sistema
textfilecontent54	Permite comprobar el contenido de un archivo de texto, línea por línea, usando expresiones regulares

Tabla 7: Objetos OVAL utilizados

4.3. Comprobaciones OVAL

Este apartado describe todas las comprobaciones OVAL implementadas para verificar las reglas identificadas. La numeración de los sub-apartados es idéntica a la del punto 3.2 del documento, donde se definen los controles, lo que permite trazar fácilmente la implementación con los controles requeridos.

4.3.1. SI1. Particiones y sistemas de archivos

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL	**Control**
oval:test_system_partitions:def:1	SI1. Particiones y Sistemas de archivos
Elementos OVAL	**Comprobaciones**
oval:test_mount_root_own_partition:tst:1 oval:test_mount_root_own_partition:obj:1	/ en partición independiente
oval:test_mount_boot_own_partition:tst:1	/boot en partición independiente

oval:test_mount_boot_own_partition:obj:1	
oval:test_mount_var_own_partition:tst:1 oval:test_mount_var_own_partition:obj:1	/var en partición independiente
oval:test_mount_tmp_own_partition:tst:1 oval:test_mount_tmp_own_partition:obj:1	/tmp en partición independiente
oval:test_mount_var_log_own_partition:tst:1 oval:test_mount_var_log_own_partition:obj:1	/var/log en partición independiente
oval:test_mount_home_own_partition:tst:1 oval:test_mount_home_own_partition:obj:1	/home en partición independiente
oval:test_mount_var_log_audit_own_partition:tst:1 oval:test_mount_var_log_audit_own_partition:obj:1	/var/log/audit en partición independiente
oval:test_mount_var_www_own_partition:tst:1 oval:test_mount_var_www_own_partition:obj:1	/var/www en partición independiente

Tabla 8: Comprobaciones OVAL para SI1 Particiones y sistemas de archivos

4.3.2. SI2. Configuración segura de arranque

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_grub_secure_boot_enabled:def:1	**Control** SI2. Configuración segura de arranque
Oval Elements	**Comprobaciones** /etc/default/grub
oval:test_grub2_disable_interactive_boot:tst:1 oval:test_grub2_disable_interactive_boot:obj:1	GRUB_TIMEOUT = 0
oval:test_grub2_disable_recovery:tst:1 oval:test_grub2_disable_recovery:obj:1	GRUB_DISABLE_RECOVERY = true

Tabla 9: Comprobaciones OVAL para SI2 Configuración segura de arranque

4.3.3. SI3. Configuración segura de particiones

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /boot
oval:test_boot_partition_noauto:tst:1 oval:test_boot_partition_noauto:obj:1 oval:state_boot_partition_noauto:ste:1	noauto

oval:test_boot_partition_noexec:tst:1 oval:test_boot_partition_noexec:obj:1 oval:state_boot_partition_noexec:ste:1	noexec
oval:test_boot_partition_nodev:tst:1 oval:test_boot_partition_nodev:obj:1 oval:state_boot_partition_nodev:ste:1	nodev
oval:test_boot_partition_nosuid:tst:1 oval:test_boot_partition_nosuid:obj:1 oval:state_boot_partition_nosuid:ste:1	nosuid
oval:test_boot_partition_ro:tst:1 oval:test_boot_partition_ro:obj:1 oval:state_boot_partition_ro:ste:1	ro

Tabla 10: Comprobaciones OVAL para SI3 (Protección de la partición /boot)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /var/log
oval:test_var_log_partition_noexec:tst:1 oval:test_var_log_partition_noexec:obj:1 oval:state_var_log_partition_noexec:ste:1	noexec
oval:test_var_log_partition_nodev:tst:1 oval:test_var_log_partition_nodev:obj:1 oval:state_var_log_partition_nodev:ste:1	nodev
oval:test_var_log_partition_nosuid:tst:1 oval:test_var_log_partition_nosuid:obj:1 oval:state_var_log_partition_nosuid:ste:1	nosuid
oval:test_var_log_partition_rw:tst:1 oval:test_var_log_partition_rw:obj:1 oval:state_var_log_partition_rw:ste:1	rw

Tabla 11: Comprobaciones OVAL para SI3 (Protección de la partición /var/log)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /var/log/audit
oval:test_var_log_audit_partition_noexec:tst:1 oval:test_var_log_audit_partition_noexec:obj:1 oval:state_var_log_audit_partition_noexec:ste:1	noexec
oval:test_var_log_audit_partition_nodev:tst:1 oval:test_var_log_audit_partition_nodev:obj:1 oval:state_var_log_audit_partition_nodev:ste:1	nodev
oval:test_var_log_audit_partition_nosuid:tst:1 oval:test_var_log_audit_partition_nosuid:obj:1	nosuid

oval:state_var_log_audit_partition_nosuid:ste:1	
oval:test_var_log_audit_partition_rw:tst:1 oval:test_var_log_audit_partition_rw:obj:1 oval:state_var_log_audit_partition_rw:ste:1	rw

Tabla 12: Comprobaciones OVAL para SI3 (Protección de la partición /var/log/audit)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /var/www
oval:test_var_www_partition_noexec:tst:1 oval:test_var_www_partition_noexec:obj:1 oval:state_var_www_partition_noexec:ste:1	noexec
oval:test_var_www_partition_nodev:tst:1 oval:test_var_www_partition_nodev:obj:1 oval:state_var_www_partition_nodev:ste:1	nodev
oval:test_var_www_partition_nosuid:tst:1 oval:test_var_www_partition_nosuid:obj:1 oval:state_var_www_partition_nosuid:ste:1	nosuid
oval:test_var_www_partition_rw:tst:1 oval:test_var_www_partition_rw:obj:1 oval:state_var_www_partition_rw:ste:1	rw

Tabla 13: Comprobaciones OVAL para SI3 (Protección de la partición /var/www)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /home
oval:test_home_partition_noexec:tst:1 oval:test_home_partition_noexec:obj:1 oval:state_home_partition_noexec:ste:1	noexec
oval:test_home_partition_nodev:tst:1 oval:test_home_partition_nodev:obj:1 oval:state_home_partition_nodev:ste:1	nodev
oval:test_home_partition_nosuid:tst:1 oval:test_home_partition_nosuid:obj:1 oval:state_home_partition_nosuid:ste:1	nosuid
oval:test_home_partition_rw:tst:1 oval:test_home_partition_rw:obj:1 oval:state_home_partition_rw:ste:1	rw

Tabla 14: Comprobaciones OVAL para SI3 (Protección de la partición /home)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /tmp
oval:test_tmp_partition_noexec:tst:1 oval:test_tmp_partition_noexec:obj:1 oval:state_tmp_partition_noexec:ste:1	noexec
oval:test_tmp_partition_nodev:tst:1 oval:test_tmp_partition_nodev:obj:1 oval:state_tmp_partition_nodev:ste:1	nodev
oval:test_tmp_partition_nosuid:tst:1 oval:test_tmp_partition_nosuid:obj:1 oval:state_tmp_partition_nosuid:ste:1	nosuid
oval:test_tmp_partition_rw:tst:1 oval:test_tmp_partition_rw:obj:1 oval:state_tmp_partition_rw:ste:1	rw

Tabla 15: Comprobaciones OVAL para SI3 (Protección de la partición /tmp)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /media
oval:test_media_partition_noexec:tst:1 oval:test_media_partition_noexec:obj:1 oval:state_media_partition_noexec:ste:1	noexec
oval:test_media_partition_nodev:tst:1 oval:test_media_partition_nodev:obj:1 oval:state_media_partition_nodev:ste:1	nodev
oval:test_media_partition_nosuid:tst:1 oval:test_media_partition_nosuid:obj:1 oval:state_media_partition_nosuid:ste:1	nosuid
oval:test_media_partition_ro:tst:1 oval:test_media_partition_ro:obj:1 oval:state_media_partition_ro:ste:1	rw

Tabla 16: Comprobaciones OVAL para SI3 (Protección de la partición /media)

Definición OVAL:	**Control:**
oval:test_secure_mount_options:def:1	SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones**
	/usr
oval:test_usr_partition_nodev:tst:1 oval:test_usr_partition_nodev:obj:1 oval:state_usr_partition_nodev:ste:1	nodev
oval:test_usr_partition_ro:tst:1 oval:test_usr_partition_ro:obj:1 oval:state_usr_partition_ro:ste:1	ro

Tabla 17: Comprobaciones OVAL para SI3 (Protección de la partición /usr)

Definición OVAL:	**Control:**
oval:test_secure_mount_options:def:1	SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones**
	/opt
oval:test_opt_partition_nodev:tst:1 oval:test_opt_partition_nodev:obj:1 oval:state_opt_partition_nodev:ste:1	nodev
oval:test_opt_partition_ro:tst:1 oval:test_opt_partition_ro:obj:1 oval:state_opt_partition_ro:ste:1	ro

Tabla 18: Comprobaciones OVAL para SI3 (Protección de la partición /opt)

Definición OVAL:	**Control:**
oval:test_secure_mount_options:def:1	SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones**
	/
oval:test_root_partition_rw:tst:1 oval:test_root_partition_rw:obj:1 oval:state_root_partition_rw:ste:1	rw

Tabla 19: Comprobaciones OVAL para SI3 (Protección de la partición /)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /boot/efi
oval:test_boot_efi_partition_umask:tst:1 oval:test_boot_efi_partition_umask:obj:1 oval:state_boot_efi_partition_umask:ste:1	umask=0077
oval:test_boot_efi_partition_shorname:tst:1 oval:test_boot_efi_partition_shortname:obj:1 oval:state_boot_efi_partition_shortname:ste:1	shortname=winnt <dump> 0 <pass> 0.

Tabla 20: Comprobaciones OVAL para SI3 (Protección de la partición /boot/efi)

Definición OVAL: oval:test_secure_mount_options:def:1	**Control:** SI3. Configuración segura de particiones
Elementos OVAL	**Comprobaciones** /swap
oval:test_swap_partition_defaults:tst:1 oval:test_swap_efi_partition_defaults:obj:1 oval:state_swap_partition_defaults:ste:1	defaults
oval:test_swap_partition_parameters:tst:1 oval:test_swap_partition_parameters:obj:1 oval:state_swap_partition_parameters:ste:1	<dump> 0 <pass> 0

Tabla 21: Comprobaciones OVAL para SI3 (Protección de la partición /swap)

4.3.4. SI.4 Configuración segura de red

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL: oval:test_secure_network_configuration:def:1	**Control:** SI4. Configuración Segura de red
Elementos OVAL	**Comprobaciones** /etc/sysconfig/network-scripts/ifcfg-.*
oval:test_sysconfig_networking_bootproto:tst:1 oval:test_sysconfig_networking_bootproto:obj:1	BOOT_PROTO ! = [bootp, dhcp]

Tabla 22: Comprobaciones OVAL para SI4 Configuración segura de red

4.3.5. SI.5 Configuración segura del kernel

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_kernel_parameters:def:1	**Control** SI5. Configuración segura del kernel
Elementos OVAL	**Comprobaciones** /etc/sysctl.conf
oval:test_sysctl_ipv4_echo_ignore_all:tst:1 oval:test_sysctl_ipv4_echo_ignore_all:obj:1	net.ipv4.icmp_echo_ignore_all = 1
oval:test_sysctl_ipv4_ignore_broadcasts:tst:1 oval:test_sysctl_ipv4_ignore_broadcasts:obj:1	net.ipv4.icmp_echo_ignore_broadcasts = 1
oval:test_sysctl_ipv4_forward:tst:1 oval:test_sysctl_ipv4_forward:obj:1	net.ipv4.ip_forward = 0
oval:test_sysctl_ipv4_all_tx_redirects:tst:1 oval:test_sysctl_ipv4_all_tx_redirects:obj:1	net.ipv4.conf.all.send_redirects = 0
oval:test_sysctl_ipv4_all_rx_redirects:tst:1 oval:test_sysctl_ipv4_all_rx_redirects:obj:1	net.ipv4.conf.all.accept_redirects = 0
oval:test_sysctl_ipv4_rx_redirects:tst:1 oval:test_sysctl_ipv4_rx_redirects:obj:1	net.ipv4.conf.default.accept_redirects = 0
oval:test_sysctl_ipv4_tx_redirects:tst:1 oval:test_sysctl_ipv4_tx_redirects:obj:1	net.ipv4.conf.default.send_redirects = 0
oval:test_sysctl_ipv4_sec_redirects:tst:1 oval:test_sysctl_ipv4_sec_redirects:obj:1	net.ipv4.conf.default.secure_redirects = 0
oval:test_sysctl_ipv4_allsec_redirects:tst:1 oval:test_sysctl_ipv4_allsec_redirects:obj:1	net.ipv4.conf.all.secure_redirects = 0
oval:test_sysctl_ipv4_allrx_src_rte:tst:1 oval:test_sysctl_ipv4_allrx_src_rte:obj:1	net.ipv4.conf.all.accept_source_route = 0
oval:test_sysctl_ipv4_rx_src_rte:tst:1 oval:test_sysctl_ipv4_rx_src_rte:obj:1	net.ipv4.conf.default.accept_source_route = 0
oval:test_sysctl_ipv4_all_log_martians:tst:1 oval:test_sysctl_ipv4_all_log_martians:obj:1	net.ipv4.conf.all.log_martians = 1
oval:test_sysctl_ipv4_log_martians:tst:1 oval:test_sysctl_ipv4_log_martians:obj:1	net.ipv4.conf.default.log_martians = 1
oval:test_sysctl_ipv4_icmp_ignore_bogus:tst:1 oval:test_sysctl_ipv4_icmp_ignore_bogus:obj:1	net.ipv4.icmp_ignore_bogus_error_responses = 1
oval:test_sysctl_ipv4_tcp_syncookies:tst:1 oval:test_sysctl_ipv4_tcp_syncookies:obj:1	net.ipv4.tcp_syncookies = 1
oval:test_sysctl_ipv4_all_rp_filter:tst:1 oval:test_sysctl_ipv4_all_rp_filter:obj:1	net.ipv4.conf.all.rp_filter = 1
oval:test_sysctl_ipv4_rp_filter:tst:1 oval:test_sysctl_ipv4_rp_filter:obj:1	net.ipv4.conf.default.rp_filter = 1
oval:test_sysctl_ipv4_tcp_timestamps:tst:1 oval:test_sysctl_ipv4_tcp_timestamps:obj:1	net.ipv4.tcp_timestamps = 0

oval:test_sysctl_ipv6_all_disable:tst:1 oval:test_sysctl_ipv6_all_disable:obj:1	net.ipv6.conf.all.disable_ipv6 = 1
oval:test_sysctl_ipv6_disable:tst:1 oval:test_sysctl_ipv6_disable:obj:1	net.ipv6.conf.default.disable_ipv6 = 1
oval:test_sysctl_fs_suid_dump:tst:1 oval:test_sysctl_fs_suid_dump:obj:1	fs.suid_dumpable = 0
oval:test_sysctl_ipv4_tcp_syn_backlog:tst:1 oval:test_sysctl_ipv4_tcp_syn_backlog:obj:1	net.ipv4.tcp_max_syn_backlog = 1280

Tabla 23: Comprobaciones OVAL para SI5 Configuración segura del kernel

4.3.6. SI.6 Configuración segura de tcp wrappers

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL	**Control**
oval:test_secure_tcp_wrappers:def:1	SI6. Configuración segura de TCP wrappers
Elementos OVAL	**Comprobaciones**
	/etc
oval:test_file_exists_etc_hosts_allow:tst:1 oval:test_file_exists_etc_hosts_allow:obj:1	Existe el archivo hosts.allow
oval:test_etc_hosts_deny_all:tst:1 oval:test_etc_hosts_deny_all:obj:1	hosts.deny contiene all:all

Tabla 24: Comprobaciones OVAL para SI6 Configuración segura de TCP wrappers

4.3.7. SI.7 Seguridad de las contraseñas

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL	**Control**
oval:test_password_quality:def:1	SI7. Seguridad de las contraseñas
Elementos OVAL	**Comprobaciones**
	/etc/security/pwquality.conf
oval:test_pam_pwquality_minlen:tst:1 oval:test_pam_pwquality_minlen:obj:1	minlen = 8
oval:test_pam_pwquality_minclass:tst:1 oval:test_pam_pwquality_minclass:obj:1	minclas = 3

Tabla 25: Comprobaciones OVAL para SI7 Seguridad de las contraseñas

4.3.8. SI.8 Configuración para auditoría

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_audit_configuration:def:1	**Control** SI8. Configuración para auditoría
Elementos OVAL	**Comprobaciones** /etc/audit/auditd.conf
oval:test_audit_max_log_size:tst:1 oval:test_audit_max_log_size:obj:1	max_log_file = 10
oval:test_audit_max_num_logs:tst:1 oval:test_audit_max_num_logs:obj:1	num_logs = 12
oval:test_audit_log_rotate_active:tst:1 oval:test_audit_log_rotate_active:obj:1	max_log_file_action = ROTATE

Tabla 26: Comprobaciones OVAL para SI8 Configuración para auditoría

4.3.9. US.1 Configuración de volcados de memoria

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_core_dumps:def:1	**Control** US1. Configuración de volcados de memoria
Elementos OVAL	**Comprobaciones** /etc/security/limits.conf
oval:test_security_limits_hard_core:tst:1 oval:test_security_limits_hard_core:obj:1	* hard core 0

Tabla 27: Comprobaciones OVAL para US1 Configuración de volcados de memoria

4.3.10. US.2 Configuración de límites de usuario

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_user_limits:def:1	**Control** US2. Configuración de límites de usuario
Elementos OVAL	**Comprobaciones** /etc/security/limits.conf
oval:test_security_limits_hard_maxlogins:tst:1 oval:test_security_limits_hard_maxlogins:obj:1	* hard maxlogins 2
oval:test_security_limits_hard_nproc:tst:1 oval:test_security_limits_hard_nproc:obj:1	* hard nproc 500

Tabla 28: Comprobaciones OVAL para US2 Configuración de recursos de usuario

4.3.11. US.3 Bloqueo de atajos críticos

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_ctrl_alt_del_reboot_disabled:def:1	**Control** US3. Bloqueo de atajos críticos
Elementos OVAL	**Comprobaciones**
oval:test_file_exists_ctrl_alt_del_target:tst:1 oval:test_ctrl_alt_del_reboot_disabled:obj:1	Comprobar si existe el archivo: /etc/systemd/system/ctrl-alt-del.target
oval:test_ctrl_alt_del_burst_disabled:tst:1 oval:test_ctrl_alt_del_burst_disabled:obj:1	Comprobar en /etc/systemd/system.conf: CtrlAltDelBurstAction=none

Tabla 29: Comprobaciones OVAL para US3 Bloqueo de atajos críticos

4.3.12. US.4 Establecimiento de cuotas de disco

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_disk_quotas:def:1	**Control** US4. Establecimiento de cuotas de disco
Elementos OVAL	**Comprobaciones** /etc/fstab
oval:test_etc_fstab_home_quota_is_set:tst:1 oval:test_etc_fstab_home_quota_is_set:obj:1	usrquota | grpquota en /home

Tabla 30: Comprobaciones OVAL para US4 Establecimiento de cuotas de disco

4.3.13. AS.1 Configuración de Avisos

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_login_banners_enabled:def:1	**Control** AS1. Configuración de avisos
Elementos OVAL	**Comprobaciones** /etc/dconf/db/gdm.d/01-banner-message
oval:test_etc_issue_banner_exists:tst:1 oval:test_etc_issue_banner_exists:obj:1	Comprobar que existe el archive
oval:test_gnome_banner_enabled:tst:1 oval:test_gnome_banner_enabled:obj:1	Comprobar que el aviso está activado

Tabla 31: Comprobaciones OVAL para AS1 Configuración de avisos

4.3.14. AS.2 Configuración segura de SSH

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_ssh_configuration:def:1	**Control** AS2. Configuración segura de SSH
Elementos OVAL	**Comprobaciones** /etc/ssh/sshd_config
oval:test_openssh_version:tst:1 oval:test_openssh_version:obj:1 oval:state_rpm_openssh_version:ste:1	Versión OpenSSH >= 7.4
oval:test_openssh_ciphers:tst:1 oval:test_openssh_ciphers:obj:1	Cifrados permitidos: aes128-ctr, aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc, rijndael-cbc
oval:test_openssh_disable_known_hosts:tst:1 oval:test_openssh_disable_known_hosts:obj:1	IgnoreUserKnownHosts yes
oval:test_openssh_no_empty_passwords:tst:1 oval:test_openssh_no_empty_passwords:obj:1	PermitEmptyPasswords no
oval:test_openssh_no_userenv_set:tst:1 oval:test_openssh_no_userenv_set:obj:1	PermitUserEnvironment no
oval:test_openssh_no_rsh_emulation:tst:1 oval:test_openssh_no_rsh_emulation:obj:1	IgnoreRhosts no
oval:test_openssh_banner_set:tst:1 oval:test_openssh_banner_set:obj:1	Banner /etc/issue
oval:test_openssh_no_root_login:tst:1 oval:test_openssh_no_root_login:obj:1	PermitRootLogin no
oval:test_openssh_allow_admins_only:tst:1 oval:test_openssh_allow_admins_only:obj:1	AllowGroups adm
oval:test_openssh_login_grace_time:tst:1 oval:test_openssh_login_grace_time:obj:1	LoginGraceTime 2m
oval:test_openssh_client_alive_interval:tst:1 oval:test_openssh_client_alive_interval:obj:1	ClientAliveInterval 60
oval:test_openssh_no_x11_forwarding:tst:1 oval:test_openssh_no_x11_forwarding:obj:1	X11Forwarding no

Tabla 32: Comprobaciones OVAL para AS2 Configuración de SSH

4.3.15. AS.3 Configuración de la autenticación

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_auth_configuration:def:1	**Control** AS3. Configuración de la autenticación
Elementos OVAL	**Comprobaciones** /etc/pam.d/system-auth
oval:test_pam_pwhistory_remember:tst:1 oval:test_pam_pwhistory_remember:obj:1	password requisite pwhistory.so remember=7
oval:test_pam_wheel_deny_root:tst:1 oval:test_pam_wheel_deny_root:obj:1	auth requisite pam_wheel.so deny

Tabla 33: Comprobaciones OVAL para AS3 Configuración de la autenticación

4.3.16. AS.4 Configuración de los intentos de acceso

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_login_configuration:def:1	**Control** AS4. Configuración de los intentos de acceso
Elementos OVAL	**Comprobaciones** /etc/pam.d/system-auth
oval:test_pam_pwquality_retry:tst:1 oval:test_pam_pwquality_retry:obj:1	password requisite pwquality.so retry=3
oval:test_pam_fail_delay:tst:1 oval:test_pam_fail_delay:obj:1	auth requisite pam_faildelay.so delay=10000000
oval:test_pam_silent_login_errors:tst:1 oval:test_pam_silent_login_errors:obj:1	auth requisite pam_tally2.so silent
oval:test_pam_register_login_attempts:tst:1 oval:test_pam_register_login_attempts:obj:1	auth requisite pam_tally2.so file=/var/log/tallylog
oval:test_pam_lock_after_n_attempts:tst:1 oval:test_pam_lock_after_n_attempts:obj:1	auth requisite pam_tally2.so deny=5
oval:test_pam_lock_root_after_n_attempts:tst:1 oval:test_pam_lock_root_after_n_attempts:obj:1	auth requisite pam_tally2.so even_deny_root

Tabla 34: Comprobaciones OVAL para AS4 Configuración de los intentos de acceso

4.3.17. EL.1 Desactivación de servicios no necesarios

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_services_not_required:def:1	**Control** EL1. Desactivación de servicios no necesarios
Elementos OVAL	**Comprobaciones** /etc/systemd/system/multi-user.target.wants
oval:test_service_cups_not_started:tst:1 oval:test_file_exists_cups_service:obj:1	Comprobar que no existe el fichero cups.service en la ruta indicada

Tabla 35: Comprobaciones OVAL para EL1 Desactivación de servicios no necesarios

4.3.18. EL.2 Eliminación de paquetes no necesarios

Se realizarán las comprobaciones que se indican a continuación:

Oval Definition oval:test_packages_not_required:def:1	**Control** EL2. Eliminación de paquetes no necesarios
Oval Elements	**Comprobaciones** /etc/passwd
oval:test_rpm_gnome_weather_not_installed:tst:1 oval:test_rpm_gnome_weather_not_installed:obj:1	Comprobar si se ha instalado el paquete gnome-weather
oval:test_rpm_gnome_contacts_not_installed:tst:1 oval:test_rpm_gnome_contacts_not_installed:obj:1	Comprobar si se ha instalado el paquete gnome-contacts

Tabla 36: Comprobaciones OVAL para EL2 Eliminación de paquetes no necesarios

4.3.19. EL.3 Eliminación de usuarios no necesarios

Se realizarán las comprobaciones que se indican a continuación:

Oval Definition oval:test_users_not_required:def:1	**Control** EL3. Eliminación de usuarios no necesarios
Oval Elements	**Comprobaciones** /etc/passwd
oval:test_users_not_required:tst:1 oval:test_users_not_required:obj:1	Comprobar si existen usuarios no necesarios (ftp, games)

Tabla 37: Comprobaciones OVAL para EL3 Eliminación de usuarios no necesarios

4.3.20. PE.1 Configuración de entornos de usuario

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_users_environment:def:1	**Control** PE1. Configuración de entornos de usuario
Oval Elements	**Comprobaciones** /etc/profile
oval:test_root_path_contains_no_dots:tst:1 oval:test_root_path_contains_no_dots:obj:1 oval:state_env_var_contains_dots:ste:1	PATH no contiene “.”
oval:test_profile_history_size:tst:1 oval:test_profile_history_size:obj:1	HISTSIZE=1000
oval:test_profile_session_timeout:tst:1 oval:test_profile_session_timeout:obj:1	TMOUT=600

Tabla 38: Comprobaciones OVAL para PE1 (Comprobación de /etc/profile)

Definición OVAL oval:test_users_environment:def:1	**Control** PE1. Configuración de entornos de usuario
Oval Elements	**Comprobaciones** /etc/bashrc
No implementado (*)	umask 027

Tabla 39: Comprobaciones OVAL para PE1 (Comprobación de /etc/bashrc)

(*) La lógica de establecimiento de umask en bashrc para CentOS7 es compleja, ya que la máscara por defecto depende del user_id. Por este motivo, se considera fuera el alcance de este TFM implementar la comprobación indicada.

4.3.21. PE.2 Configuración de directorios de usuario

Definición OVAL oval:test_user_directories:def:1	**Control** PE2. Configuración de directorios de usuario
Elementos OVAL	**Comprobaciones** /home/keko
oval:test_file_perm_home_users:tst:1 oval:test_file_perm_home_users:obj:1 oval:state_file_perm_home_users:ste:1	Mode = 0700

Tabla 40: Comprobaciones OVAL para PE2 Configuración de directorios de usuario

4.3.22. PE.3 Configuración de permisos de usuario

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL oval:test_user_permisions:def:1	**Control** PE3. Configuración de permisos de usuario
Elementos OVAL	**Comprobaciones** /etc/passwd
oval:test_file_owner_etc_passwd:tst:1 oval:test_file_owner_etc_passwd:obj:1 oval:state_file_owner_etc_passwd:ste:1	user_id = 0 (root)
oval:test_file_group_etc_passwd:tst:1 oval:test_file_group_etc_passwd:obj:1 oval:state_file_group_etc_passwd:ste:1	group_id = 0 (root)
oval:test_file_perm_etc_passwd:tst:1 oval:test_file_perm_etc_passwd:obj:1 oval:state_file_perm_etc_passwd:ste:1	Mode = 0644 suid = false sgid = false

Tabla 41: Comprobaciones OVAL para PE3 (permisos /etc/passwd)

Definición OVAL oval:test_user_permisions:def:1	**Control** PE3. Configuración de permisos de usuario
Elementos OVAL	**Comprobaciones** /etc/group
oval:test_file_owner_etc_group:tst:1 oval:test_file_owner_etc_group:obj:1 oval:state_file_owner_etc_group:ste:1	user_id = 0 (root)
oval:test_file_group_etc_group:tst:1 oval:test_file_group_etc_group:obj:1 oval:state_file_group_etc_group:ste:1	group_id = 0 (root)
oval:test_file_perm_etc_group:tst:1 oval:test_file_perm_etc_group:obj:1 oval:state_file_perm_etc_group:ste:1	Mode = 0644 suid = false sgid = false

Tabla 42: Comprobaciones OVAL para PE3 (permisos /etc/group)

Definición OVAL oval:test_user_permisions:def:1	**Control** PE3. Configuración de permisos de usuario
Elementos OVAL	**Comprobaciones** /etc/shadow
oval:test_file_owner_etc_shadow:tst:1 oval:test_file_owner_etc_shadow:obj:1 oval:state_file_owner_etc_shadow:ste:1	user_id = 0 (root)

oval:test_file_group_etc_shadow:tst:1 oval:test_file_group_etc_shadow:obj:1 oval:state_file_group_etc_shadow:ste:1	group_id = 0 (root)
oval:test_file_perm_etc_shadow:tst:1 oval:test_file_perm_etc_shadow:obj:1 oval:state_file_perm_etc_shadow:ste:1	Mode = 0400 suid = false sgid = false

Tabla 43: Comprobaciones OVAL para PE3 (permisos /etc/shadow)

Definición OVAL	**Control**
oval:test_user_permisions:def:1	PE3. Configuración de permisos de usuario
Elementos OVAL	**Comprobaciones** Otras comprobaciones
No implementado (*)	Sticky Bit para directorios "*world writable*"
No implementado (*)	identificar aquellos ficheros que puedan ser modificados por todos los usuarios, independientemente de los permisos que posean.
No implementado (*)	identificar aquellos ficheros que tengan activado el bit de SUID o SGID.

Tabla 44: Comprobaciones OVAL para PE3 (Otras comprobaciones)

(*) La comprobación requiere del uso de características avanzadas de OVAL, como variables, comportamiento específico (behaviour) y filtros. Por su complejidad, se considera fuera el alcance de este TFM implementar la comprobación indicada.

4.3.23. PE.4 Configuración de automatización de tareas

Se realizarán las comprobaciones que se indican a continuación:

Definición OVAL	**Control**
oval:test_restrict_at_cron_users:def:1	PE4. Config. de la Automatización de tareas
Elementos OVAL	**Comprobaciones**
oval:test_file_exists_cron_allow:tst:1 oval:test_file_exists_cron_allow:obj:1	Comprobar que existe el fichero: /etc/cron.allow
oval:test_file_exists_at_allow:tst:1 oval:test_file_exists_at_allow:obj1	Comprobar que existe el fichero: /etc/at.allow
oval:test_file_owner_cron_allow:tst:1 oval:test_file_owner_cron_allow:obj:1 oval:state_file_owner_cron_allow:ste:1	user_id = 0 (root)
oval:test_file_group_cron_allow:tst:1 oval:test_file_group_cron_allow:obj:1 oval:state_file_group_cron_allow:ste:1	group_id = 0 (root)

oval:test_file_perm_cron_allow:tst:1 oval:test_file_perm_cron_allow :obj:1 oval:state_file_perm_cron_allow:ste:1	Mode = 0644 suid = false sgid = false
oval:test_file_owner_at_allow:tst:1 oval:test_file_owner_at_allow:obj:1 oval:state_file_owner_at_allow:ste:1	user_id = 0 (root)
oval:test_file_group_at_allow:tst:1 oval:test_file_group_at_allow:obj:1 oval:state_file_group_at_allow:ste:1	group_id = 0 (root)
oval:test_file_perm_at_allow:tst:1 oval:test_file_perm_at_allow :obj:1 oval:state_file_perm_at_allow:ste:1	Mode = 0644 suid = false sgid = false

Tabla 45: Comprobaciones OVAL para PE4 Configuración de la automatización de tareas

4.4. Scripts de Remedio Automático

El protocolo XCCDF ofrece la posibilidad de incluir un script de remedio automático que modifique la configuración del sistema cuando falle la comprobación de una regla. Esta sección contiene diversos scripts que permiten cumplir las reglas definidas en el apartado 4.3 de este documento.

Sólo se han desarrollado para este TFM scripts básicos, basados principalmente en añadir o modificar el contenido de una o más líneas del tipo “parámetro = valor” en un archivo de configuración, comprobar los permisos de un archivo, crear o eliminar archivos de texto y otras acciones sencillas.

```
#####################################################
# CCN-STIC-619 CentOS7 Fixes (CentOS7-xccdf.xml)
#####################################################
# SI.2 Configuracion segura de arranque
#####################################################
# GRUB_TIMEOUT
if ! grep -q GRUB_TIMEOUT /etc/default/grub; then
      echo GRUB_TIMEOUT=0 &gt;&gt; /etc/default/grub;
else
      sed -i "s/^\(GRUB_TIMEOUT\).*/\1=0/g" /etc/default/grub
      fi
# GRUB_DISABLE_RECOVERY
if ! grep -q GRUB_DISABLE_RECOVERY /etc/default/grub; then
      echo GRUB_DISABLE_RECOVERY=true &gt;&gt; /etc/default/grub;
else
      sed -i "s/^\(GRUB_DISABLE_RECOVERY\).*/\1=true/g" /etc/default/grub
      fi

#####################################################
# SI.5 Configuracion segura del kernel
#####################################################
cp /etc/sysctl.conf /etc/sysctl.conf.bak
rm -rf /etc/sysctl.conf
touch /etc/sysctl.conf

# Deshabilitar ping
echo "net.ipv4.icmp_echo_ignore_all = 1" &gt&gt /etc/sysctl.conf

# Evitar Re-envío de Paquetes entre interfaces
```

```
echo "net.ipv4.ip_forward = 0" &gt&gt /etc/sysctl.conf
# Evitar la modificación de tablas de encaminamiento
echo "net.ipv4.conf.all.send_redirects = 0" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.all.accept_redirects = 0" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.default.accept_redirects = 0" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.default.send_redirects = 0" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.default.secure_redirects = 0" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.all.secure_redirects = 0" &gt&gt /etc/sysctl.conf
# Deshabilitar el source routing
echo "net.ipv4.conf.all.accept_source_route = 0" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.default.accept_source_route = 0" &gt&gt /etc/sysctl.conf
# Activa los logs para paquetes anormales o excepcionales
echo "net.ipv4.conf.all.log_martians = 1" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.default.log_martians = 1" &gt&gt /etc/sysctl.conf
# Ignorar peticiones broadcast
echo "net.ipv4.icmp_echo_ignore_broadcasts = 1" &gt&gt /etc/sysctl.conf
# Ignorar mensajes de error mal formados
echo "net.ipv4.icmp_ignore_bogus_error_responses = 1" &gt&gt /etc/sysctl.conf
# Protegerse ante ataques tcp syn
echo "net.ipv4.tcp_syncookies = 1" &gt&gt /etc/sysctl.conf
# Habilitar reverse path filtering
echo "net.ipv4.conf.all.rp_filter = 1" &gt&gt /etc/sysctl.conf
echo "net.ipv4.conf.default.rp_filter = 1" &gt&gt /etc/sysctl.conf
# Deshabilitar vulnerabilidad de marca de tiempo en TCP
echo "net.ipv4.tcp_timestamps = 0" &gt&gt /etc/sysctl.conf
# Bloqueo de ipv6
echo "net.ipv6.conf.all.disable_ipv6 = 1" &gt&gt /etc/sysctl.conf
echo "net.ipv6.conf.default.disable_ipv6 = 1" &gt&gt /etc/sysctl.conf
# Bloqueo de core dumps de programas con SUID
echo "fs.suid_dumpable = 0" &gt&gt /etc/sysctl.conf
# Establecer tamaño de las colas de espera de TCP
echo "net.ipv4.tcp_max_syn_backlog = 1280" &gt&gt /etc/sysctl.conf

#####################################################
# SI.6 Configuracion segura de TCP wrappers
#####################################################
# hosts.allow
if ! grep -q . /etc/hosts.allow; then
      echo '#localhost' &gt;&gt; /etc/hosts.allow;
      fi
# hosts.deny
echo all:all &gt; /etc/hosts.deny

#####################################################
# SI.7 Seguridad de las contraseñas
#####################################################
# minlen = 8
if ! grep -q '^minlen.*' /etc/security/pwquality.conf; then
      echo 'minlen = 8' &gt;&gt; /etc/security/pwquality.conf;
else
      sed -i "s/^\(minlen\).*/\1=8/g" /etc/security/pwquality.conf;
      fi
# minclass = 3
if ! grep -q '^minclass.*' /etc/security/pwquality.conf; then
      echo 'minclass = 3' &gt;&gt; /etc/security/pwquality.conf;
else
      sed -i "s/^\(minclass\).*/\1=3/g" /etc/security/pwquality.conf;
      fi

#####################################################
# SI.8 Configuracion para auditoria
#####################################################
# max_log_file = 10
if ! grep -q '^max_log_file.*' /etc/audit/auditd.conf; then
```

```
      echo 'max_log_file = 10' &gt;&gt; /etc/audit/auditd.conf;
else
      sed -i "s/^\(max_log_file\).*/\1 = 10/g" /etc/audit/auditd.conf;
      fi
# num_logs = 12
if ! grep -q '^num_logs.*' /etc/audit/auditd.conf; then
      echo 'num_logs = 12' &gt;&gt; /etc/audit/auditd.conf;
else
      sed -i "s/^\(num_logs\).*/\1 =12/g" /etc/audit/auditd.conf;
      fi
# max_log_file_action = ROTATE
if ! grep -q '^max_log_file_action.*' /etc/audit/auditd.conf; then
      echo 'max_log_file_action = ROTATE' &gt;&gt; /etc/audit/auditd.conf;
else
      sed -i "s/^\(max_log_file_action\).*/\1 = ROTATE/g" /etc/audit/auditd.conf;
      fi

#####################################################
# US.1 Configuracion de volcados de memoria
#####################################################
# * hard core 0
if ! grep -q '^.*hard.*core.*' /etc/security/limits.conf; then
      echo '*   hard   core   0' &gt;&gt; /etc/security/limits.conf;
else
      sed -i "s/^.*hard.*core.*$/*   hard   core   0/g" /etc/security/limits.conf;
      fi

#####################################################
# US2. Configuracion de límites de usuario
#####################################################
# * hard maxlogins 2
if ! grep -q '^.*hard.*maxlogins.*' /etc/security/limits.conf; then
      echo '*   hard   maxlogins 2' &gt;&gt; /etc/security/limits.conf;
else
      sed -i "s/^.*hard.*maxlogins.*$/*   hard   maxlogins   2/g"
      /etc/security/limits.conf;
      fi
# * hard nproc 2
if ! grep -q '^.*hard.*nproc.*' /etc/security/limits.conf; then
      echo '*   hard   nproc 500' &gt;&gt; /etc/security/limits.conf;
else
      sed -i "s/^.*hard.*nproc.*$/*   hard   nproc   500/g"
      /etc/security/limits.conf;
      fi

#####################################################
# US3. Bloqueo de atajos críticos
#####################################################
# ctrl-alt-del.target
if ! grep -q . /etc/systemd/system/ctrl-alt-del.target; then
      touch /etc/systemd/system/ctrl-alt-del.target;
      fi
# CtrlAltDelBurstAction=none
if ! grep -q '^CtrlAltDelBurstAction*' /etc/systemd/system.conf; then
      echo 'CtrlAltDelBurstAction=none' &gt;&gt; /etc/systemd/system.conf;
else
      sed -i "s/^\(CtrlAltDelBurstAction\).*/\1=none/g" /etc/audit/auditd.conf;
      fi

#####################################################
# AS1. Configuración de avisos (banners)
#####################################################
# check /etc/issue
if ! grep -q . /etc/issue; then
```

```
touch /etc/issue
echo 'Este ordenador es propiedad de [Organización] y su utilización presupone el '
&gt;&gt; /etc/issue;
echo 'consentimiento del usuario para la monitorización de su actividad en todo
momento.' &gt;&gt; /etc/issue;
echo 'Cualquier uso  no autorizado del mismo puede constituye un delito tipificado
en el' &gt;&gt; /etc/issue;
echo 'codigo penal.' &gt;&gt; /etc/issue;
fi
# gnome login screen banner
if ! grep -q [org/gnome/login-screen] /etc/dconf/db/gdm.d/*; then
touch /etc/dconf/db/gdm.d/01-banner-message
echo '[org/gnome/login-screen]' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
echo 'banner-message-enable=true' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
echo -n 'banner-message-text="' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
echo -n 'Este ordenador es propiedad de [Organización] y su utilizacion presupone
el ' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
echo -n 'consentimiento del usuario para la monitorizacion de su actividad en todo
momento. ' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
echo -n 'Cualquier uso  no autorizado del mismo puede constituye un delito
tipificado en el ' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
echo 'codigo penal."' &gt;&gt; /etc/dconf/db/gdm.d/01-banner-message;
fi

#####################################################
# AS2. Configuración de ssh
#####################################################
# IgnoreUserKnownHosts yes
if ! grep -q '^IgnoreUserKnownHosts.*' /etc/ssh/sshd_config; then
      echo 'IgnoreUserKnownHosts yes' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(IgnoreUserKnownHosts\).*/\1 yes/g" /etc/ssh/sshd_config;
      fi
# PermitEmptyPasswords no
if ! grep -q '^PermitEmptyPasswords.*' /etc/ssh/sshd_config; then
      echo 'PermitEmptyPasswords no' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(PermitEmptyPasswords\).*/\1 no/g" /etc/ssh/sshd_config;
      fi
# PermitUserEnvironment no
if ! grep -q '^PermitUserEnvironment.*' /etc/ssh/sshd_config; then
      echo 'PermitUserEnvironment no' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(PermitUserEnvironment\).*/\1 no/g" /etc/ssh/sshd_config;
      fi
# IgnoreRhosts no
if ! grep -q '^IgnoreRhosts.*' /etc/ssh/sshd_config; then
      echo 'IgnoreRhosts no' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(IgnoreRhosts\).*/\1 no/g" /etc/ssh/sshd_config;
      fi
# Banner /etc/issue
if ! grep -q '^Banner.*' /etc/ssh/sshd_config; then
      echo 'Banner /etc/issue' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(Banner\).*/\1 \/etc\/issue/g" /etc/ssh/sshd_config;
      fi
# PermitRootLogin no
if ! grep -q '^PermitRootLogin.*' /etc/ssh/sshd_config; then
      echo 'PermitRootLogin no' &gt;&gt; /etc/ssh/sshd_config;
```

```
else
      sed -i "s/^\(PermitRootLogin\).*/\1 no/g" /etc/ssh/sshd_config;
      fi
# AllowGroups adm
if ! grep -q '^AllowGroups.*' /etc/ssh/sshd_config; then
      echo 'AllowGroups adm' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(AllowGroups\).*/\1 adm/g" /etc/ssh/sshd_config;
      fi
# LoginGraceTime 2m
if ! grep -q '^LoginGraceTime.*' /etc/ssh/sshd_config; then
      echo 'LoginGraceTime 2m' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(LoginGraceTime\).*/\1 2m/g" /etc/ssh/sshd_config;
      fi
# ClientAliveInterval 60
if ! grep -q '^ClientAliveInterval.*' /etc/ssh/sshd_config; then
      echo 'ClientAliveInterval 60' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(ClientAliveInterval\).*/\1 60/g" /etc/ssh/sshd_config;
      fi
# X11Forwarding no
if ! grep -q '^X11Forwarding.*' /etc/ssh/sshd_config; then
      echo 'X11Forwarding no' &gt;&gt; /etc/ssh/sshd_config;
else
      sed -i "s/^\(X11Forwarding\).*/\1 no/g" /etc/ssh/sshd_config;
      fi

#####################################################
# AS3. Configuración de la autenticación
#####################################################
# password requisite pwhistory.so remember=7
if ! grep -q '^password.*requisite.*pam_pwhistory\.so.*remember.*'
/etc/pam.d/system-auth; then
      echo 'password requisite pam_pwhistory.so remember=7' &gt;&gt;
/etc/pam.d/system-auth;
else
      sed -i "s/^\(password.*requisite.*pam_pwhistory\.so.*remember\).*/\1=7/g"
/etc/pam.d/system-auth;
fi
# auth requisite pam_wheel.so deny
if ! grep -q '^.*auth.*required.*pam_wheel\.so.*' /etc/pam.d/system-auth; then
      echo 'auth required pam_wheel.so deny' &gt;&gt; /etc/pam.d/system-auth;
else
      sed -i "s/^\(auth.*required.*pam_wheel\.so\).*/\1 deny/g" /etc/pam.d/system-
auth;
fi

#####################################################
# AS4. Configuración de intentos de acceso
#####################################################
# password requisite pwquality.so retry=3
if ! grep -q '^password.*requisite.*pam_pwquality\.so.*retry.*' /etc/pam.d/system-
auth; then
      echo 'password requisite pam_pwquality.so retry=3' &gt;&gt;
/etc/pam.d/system-auth;
```

```
else
      sed -i "s/^\(password.*requisite.*pam_pwquality\.so.*retry\).*/\1=3/g"
/etc/pam.d/system-auth;
fi
# auth requisite faildelay.so delay=10000000
if ! grep -q '^auth.*requi.*pam_faildelay\.so.*delay.*' /etc/pam.d/system-auth;
then
      echo 'auth requisite pam_faildelay.so delay=10000000' &gt;&gt;
/etc/pam.d/system-auth;
else
      sed -i "s/^\(auth.*requi.*pam_faildelay\.so.*delay\).*/\1=10000000/g"
/etc/pam.d/system-auth;
fi
# auth requisite tally2.so silent file=/var/log/tallylog deny=5 even_deny_root
if ! grep -q '^auth.*requi.*pam_tally2\.so*' /etc/pam.d/system-auth; then
      echo 'auth requisite pam_tally2.so silent file=/var/log/tallylog deny=5
even_deny_root' &gt;&gt; /etc/pam.d/system-auth;
else
      sed -i "s/^\(auth.*requi.*pam_tally2\.so\).*/\1 silent file=/var/log/tallylog
deny=5 even_deny_root/g" /etc/pam.d/system-auth;
fi

#####################################################
# EL1. Desactivación de servicios no necesarios
#####################################################
# CUPS
systemctl disable cups.service

#####################################################
# EL2. Eliminación de paquetes no necesarios
#####################################################
# gnome-weather
if rpm -q --quiet gnome-weather; then
    yum remove -y gnome-weather
      fi
# gnome-contacts
if rpm -q --quiet gnome-contacts; then
    yum remove -y gnome-contacts
      fi

#####################################################
# EL3. Eliminación de usuarios no necesarios
#####################################################
# Delete 'ftp' user
if grep -q '^ftp.*' /etc/passwd; then
      userdel ftp
      fi
# Delete 'games' user
if grep -q '^games.*' /etc/passwd; then
      userdel games
      fi

#####################################################
# PE1. Configuración de entornos de usuario
#####################################################
# HISTSIZE=1000
if ! grep -q '^HISTSIZE.*' /etc/profile; then
```

```
      echo 'HISTSIZE=1000' &gt;&gt; /etc/profile;
else
      sed -i "s/^\(HISTSIZE\).*/\1=1000/g" /etc/profile;
      fi
# TMOUT=600
if ! grep -q '^TMOUT.*' /etc/profile; then
      echo 'TMOUT=600' &gt;&gt; /etc/profile;
      echo 'export TMOUT' &gt;&gt; /etc/profile;
else
      sed -i "s/^\(TMOUT\).*/\1=600/g" /etc/profile;
      fi

#####################################################
# PE3. Configuración de permisos de usuario
#####################################################
# /etc/passwd
chown root:root: /etc/passwd
chmod 0644       /etc/passwd
#/etc/group
chown root:root /etc/group
chmod 0644      /etc/group
#/etc/shadow
chown root:root /etc/shadow
chmod 0400      /etc/shadow

#####################################################
# PE4. Configuración de la automatización de tareas
#####################################################
# cron.allow
echo 'root' &gt; /etc/cron.allow;
chmod 0644  /etc/cron.allow

# at.allow
echo 'root' &gt; /etc/at.allow;
chmod 0644  /etc/at.allow
```

5. Implementación

5.1. Contenido SCAP generado

En este apartado se describen los contenidos SCAP generados como parte del desarrollo de este TFM. Para ello, se ha empleado la herramienta eSCAPe-1.2.2 (ESCAPE: Enhanced SCAP Content Editor) disponible en el sitio https://g2-inc.com. Adicionalmente, ha sido necesaria la edición manual de los archivos generados, al haber sido detectados diversos problemas durante el uso de la herramienta.

5.1.1. CentOS7-xccdf.xml

En la siguiente figura se muestra el contenido del archivo **CentOS7-xccdf.xml**, tal y como se presenta en la herramienta eSCAPe. El archivo incluye la definición de los tres perfiles (ENS Nivel Alto, Medio y Bajo) así como de las reglas a aplicar para cada perfil:

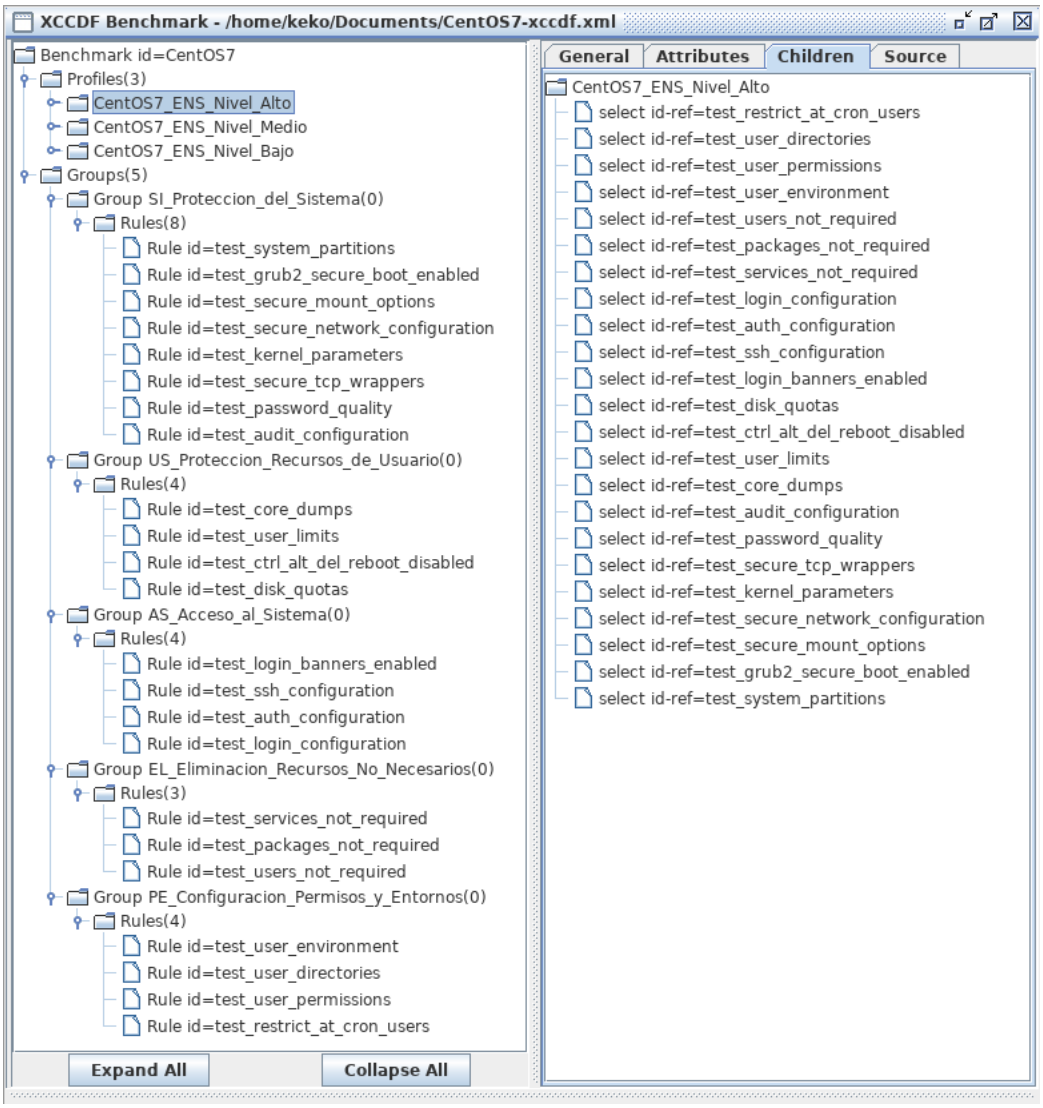

Figura 6: Contenido del Archivo CentOS7-xccdf.xml

5.1.2. CentOS7-oval.xml

En la siguiente figura, se muestra el contenido del archivo **CentOS7-oval.xml**, tal y como se presenta en la herramienta eSCAPe. El archivo incluye la implementación de todas las comprobaciones OVAL definidas en este documento:

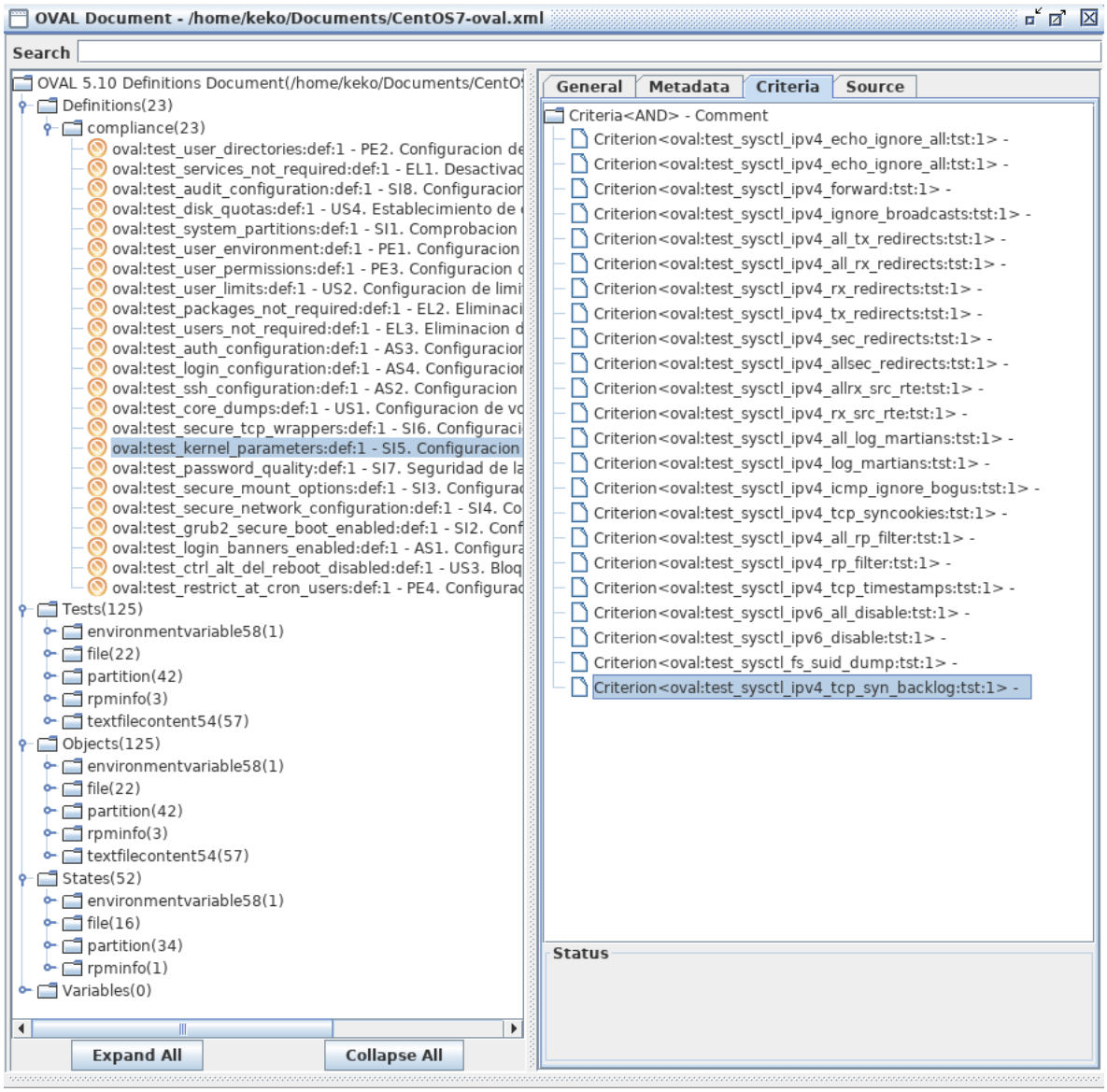

Figura 7: Contenido del Archivo CentOS7-oval.xml

Por último, se resume el contenido SCAP generado como parte del trabajo del TFM

Perfil	Reglas	Tests	Objetos	Estados
ENS Básico	20	95	95	52
ENS Medio	22	102	102	52
ENS Alto (Total)	**23**	**125**	**125**	**52**

Tabla 46: Resumen del Contenido SCAP Implementado

6. Demostración

Para demostrar el proyecto, se comprobará una versión recién instalada de CentOS7 contra la política de seguridad del ENS Nivel Alto, sin aplicar remedios. Posteriormente se aplicarán los remedios desarrollados en el apartado 4.4 de este TFM y se compararán los resultados.

6.1. Preparación del entorno de demostración

Serán necesarios los siguientes componentes:

- VirtualBox (u otra herramienta de virtualización)
- Imagen instalable de CentOS7 versión 7.7.1908
- OpenSCAP
- SCAP WorkBench
- Archivo CentOS7-xccdf.xml (desarrollado como parte del TFM)
- Archivo CentOS7-oval.xml (desarrollado como parte del TFM)

6.1.1. Preparación de la máquina virtual

La instalación de CentOS se realizará siguiendo el esquema de particiones exigido por la guía CCN-STIC-619 (ver apartado 3.2.1 de este documento) y tomando los valores por defecto del asistente de instalación.

6.1.2. Instalación de OpenSCAP

A continuación, se indican los pasos necesarios para instalar en la máquina virtual los componentes requeridos para la demostración del proyecto:

```
sudo yum install openscap-scanner scap-workbench
```

6.2. Demostración con Scap Workbench

En primer lugar, copiaremos los archivos CentOS7-xccdf.xml y CentOS7-oval.xml en la máquina virtual.

A continuación, abriremos SCAP Workbench y cargaremos el archivo CentOS7-xccdf.xml. Una vez cargada la lista, seleccionamos el perfil (profile) correspondiente al nivel alto de ENS y pulsamos el el botón “Scan”. Nos aseguraremos de que la casilla “*remediate*” no esté marcada. De este modo, obtendremos la caracterización inicial de la seguridad de la instalación por defecto, sin realizar ninguna modificación.

6.3. Resultados sobre la instalación por defecto

Como puede comprobarse en la imagen, la instalación por defecto de CentOS7 solamente cumple dos de las reglas de configuración exigidas en el perfil ENS Alto.

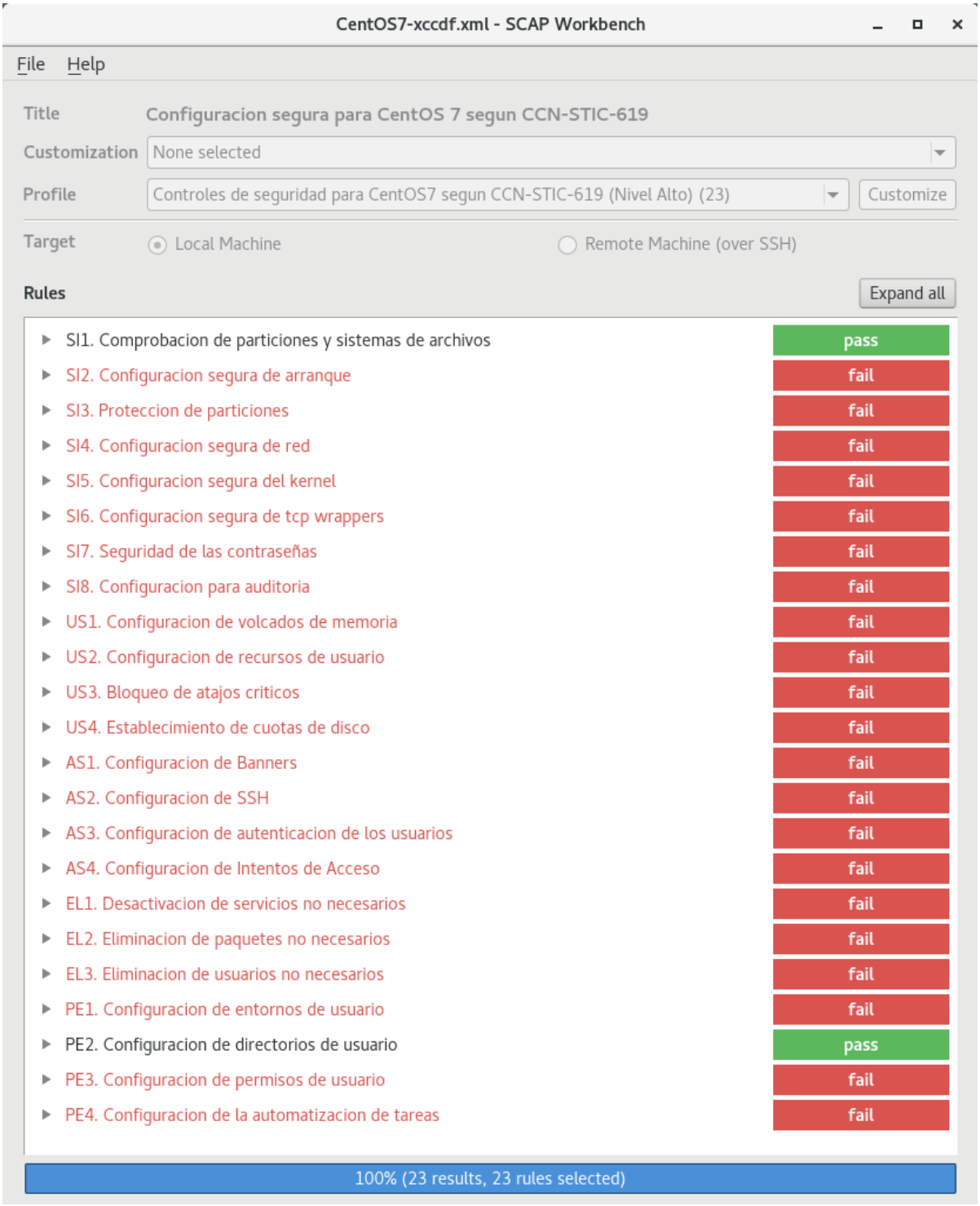

Figura 8: Resultado comprobación inicial ENS (Nivel Alto)

6.4. Resultados aplicando remedio automático

A continuación, se muestra el resultado de ejecutar de nuevo la comprobación, marcando la casilla "*remediate*", que aplica los scripts de remedio automático (apartado 4.4):

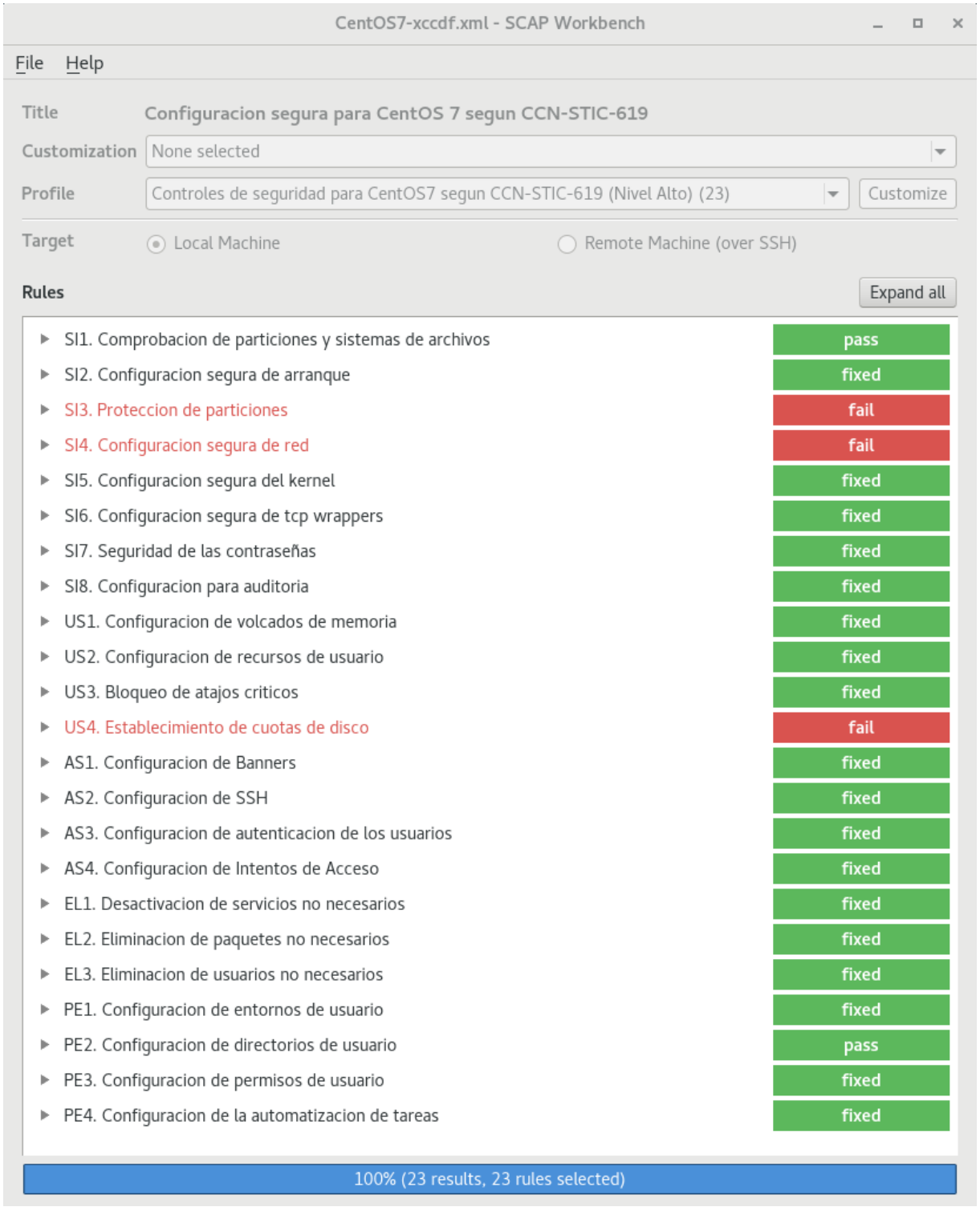

Figura 9: Resultado comprobación ENS (Nivel Alto) tras aplicar remedios

Como se puede apreciar en la figura anterior, los scripts de remedio desarrollados como parte del TFM han funcionado satisfactoriamente. Todas las reglas que inicialmente no han podido ser verificadas y a las que se ha aplicado satisfactoriamente el script de remedio, aparecen marcadas con la indicación “fixed”. Las reglas falladas (SI3, SI4 y US4) requieren de scripts de remedio de mayor complejidad, que no se han considerado dentro del alcance del TFM.

Una vez realizadas las comprobaciones y aplicados los remedios, Scap-Workbench genera un informe de resultados, que contiene información detallada sobre todas las comprobaciones realizadas, los remedios aplicados en su caso y el resultado obtenido. Las figuras siguientes muestran un resumen del contenido del informe generado.

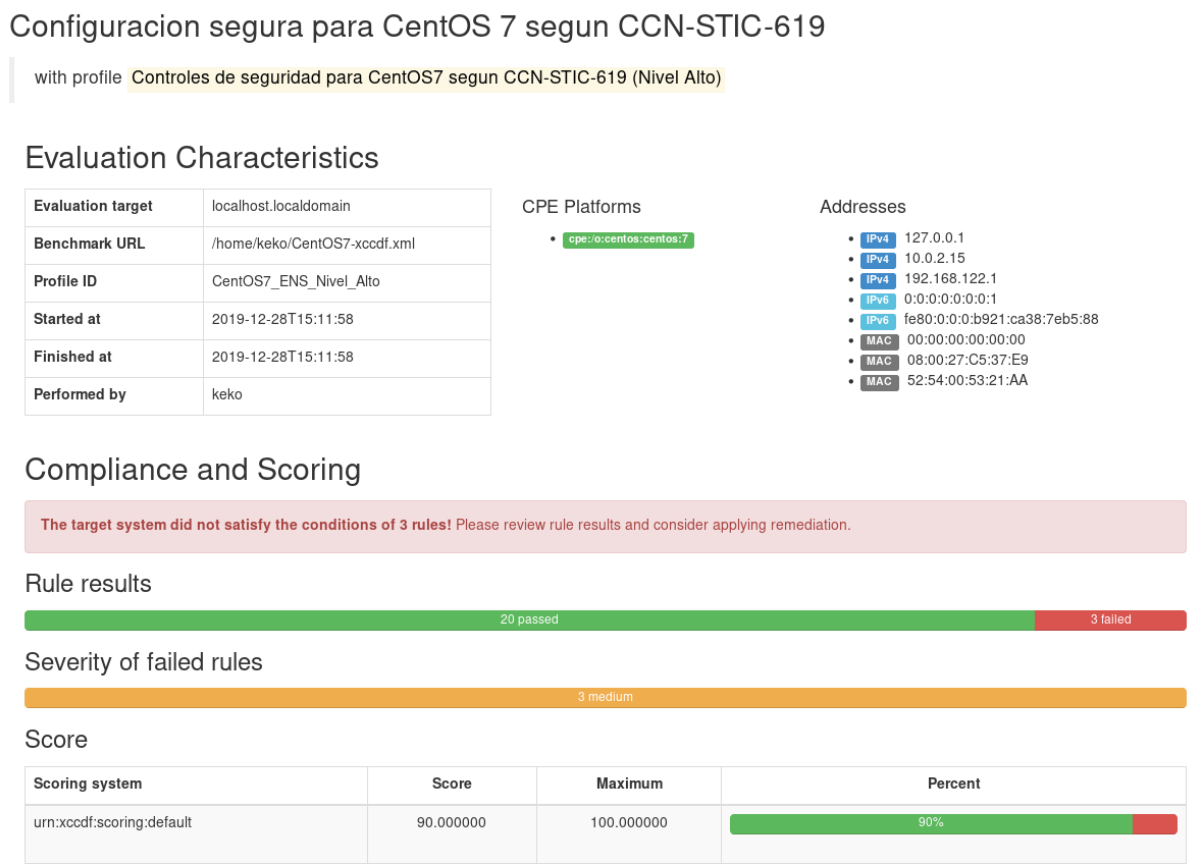

Figura 10: Informe Resultados comprobación ENS (Nivel Alto)

La figura muestra el resumen del cumplimiento una vez aplicados los remedios automáticos. Como puede comprobarse, la puntuación obtenida tras el análisis es de 90% (20 de 23 reglas pasadas)

Title	Severity	Result
Configuracion segura para CentOS 7 segun CCN-STIC-619 3x fail		
ID: SI_Proteccion_del_Sistema 2x fail		
SI1. Comprobacion de particiones y sistemas de archivos	medium	pass
SI2. Configuracion segura de arranque	medium	fixed
SI3. Proteccion de particiones	medium	fail
SI4. Configuracion segura de red	medium	fail
SI5. Configuracion segura del kernel	medium	fixed
SI6. Configuracion segura de tcp wrappers	medium	fixed
SI7. Seguridad de las contraseñas	medium	fixed
SI8. Configuracion para auditoria	medium	fixed
ID: US_Proteccion_Recursos_de_Usuario 1x fail		
US1. Configuracion de volcados de memoria	medium	fixed
US2. Configuracion de recursos de usuario	medium	fixed
US3. Bloqueo de atajos criticos	medium	fixed
US4. Establecimiento de cuotas de disco	medium	fail
ID: AS_Acceso_al_Sistema		
AS1. Configuracion de Banners	medium	fixed
AS2. Configuracion de SSH	medium	fixed
AS3. Configuracion de autenticacion de los usuarios	medium	fixed
AS4. Configuracion de Intentos de Acceso	medium	fixed
ID: EL_Eliminacion_Recursos_No_Necesarios		
EL1. Desactivacion de servicios no necesarios	medium	fixed
EL2. Eliminacion de paquetes no necesarios	medium	fixed
EL3. Eliminacion de usuarios no necesarios	medium	fixed
ID: PE_Configuracion_Permisos_y_Entornos		
PE1. Configuracion de entornos de usuario	medium	fixed
PE2. Configuracion de directorios de usuario	medium	pass
PE3. Configuracion de permisos de usuario	medium	fixed
PE4. Configuracion de la automatizacion de tareas	medium	fixed

Figura 11: Resumen de reglas y resultados comprobación ENS (Nivel Alto)

Como se puede comprobar, el informe generado es muy detallado pues permite consultar el resultado de todas las comprobaciones y remedios aplicados, tan sólo pulsando sobre la regla deseada.

A modo de ejemplo, en la página siguiente se muestra la información asociada a la regla US2. Configuración de recursos de usuario, donde se aprecian las comprobaciones realizadas inicialmente (con resultado fallido) y el resultado obtenido tras aplicar el script de remedio automático.

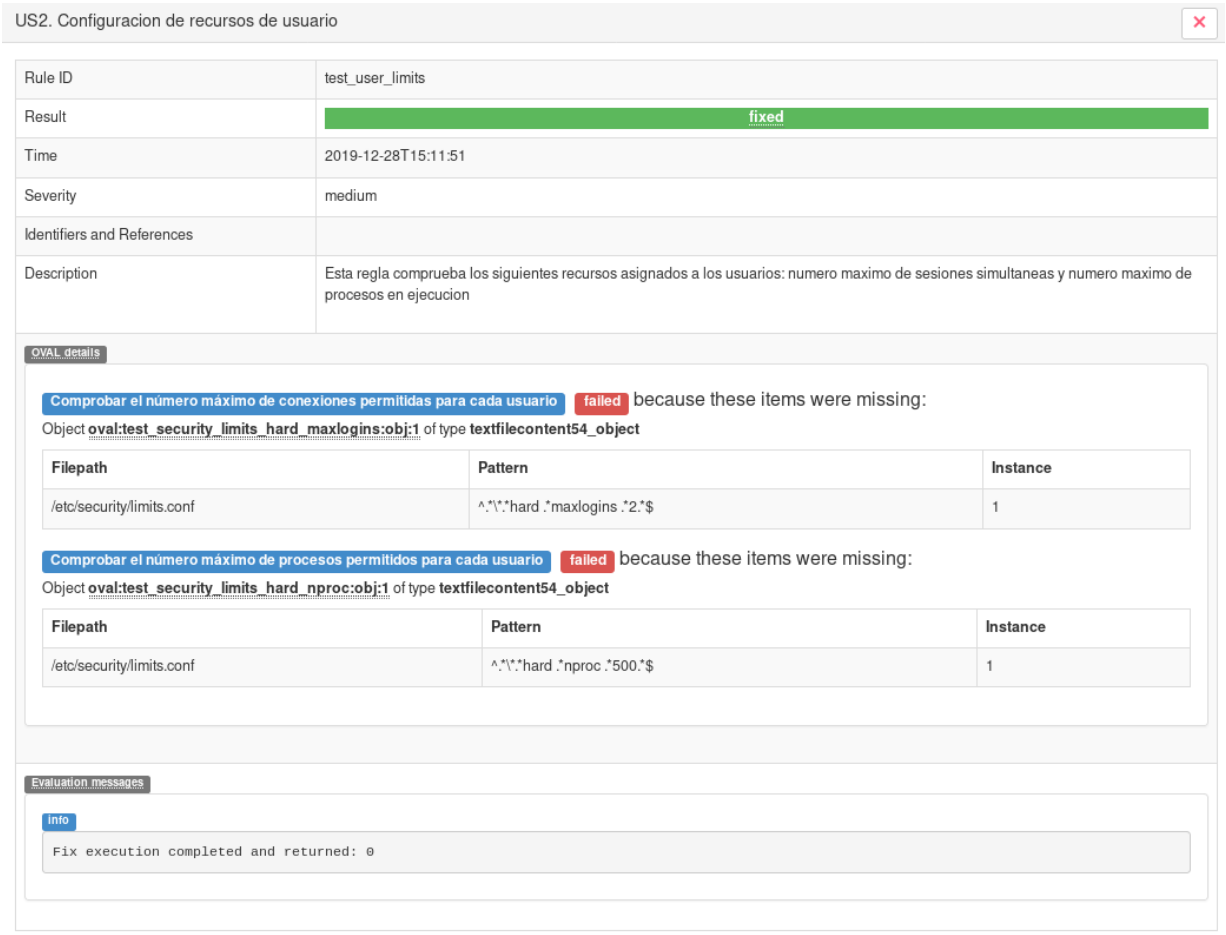

Figura 12: Ejemplo del Resultado. Regla US2 Configuración de recursos de usuario

7. Opciones de Despliegue

En este apartado se analizarán posibles modelos de despliegue en entornos reales. En primer lugar, se demostrará la comprobación periódica de la política de seguridad de forma automática mediante oscap-daemon (`oscapd`). A continuación, se analizarán las posibilidades de despliegue durante la instalación aplicando la política al instalador de CentOS (anaconda) durante la instalación del sistema operativo.

7.1. Comprobación periódica mediante oscapd

En este apartado se indicará como configurar `oscapd` para que realice la comprobación de la política de seguridad una vez al día. En primer lugar, descargaremos el código fuente de `oscapd` en nuestro sistema para instalarlo.

Para ello, ejecutamos la siguiente instrucción:

```
git clone https://github.com/OpenSCAP/openscap-daemon/
```

A continuación, ejecutamos el programa de instalación:

```
cd openscap-daemon; sudo python2 setup.py install
```

Por último, activamos el servicio oscapd

```
systemctl start oscapd.service
```

El servicio soporta dos interfaces de control: dbus y línea de comandos. En nuestro caso, utilizaremos la interfaz de línea de comandos. Para ello, utilizamos el comando `oscapd-cli`. A continuación, se muestran las entradas necesarias para crear, de forma interactiva, una tarea que compruebe la política de seguridad definida para nuestro sistema una vez al día:

```
#> oscapd-cli task-create -i

Creating new task in interactive mode
      Title: Daily Security Policy Check
      Target (empty for localhost):
      Choose SSG content by number (empty for custom content):
      Input file (absolute path): /home/keko/CentOS7-xccdf.xml
      Tailoring file (absolute path, empty for no tailoring):
      Choose profile by number (empty for (default) profile): 1
      Online remediation (1, y or Y for yes, else no): no
      Schedule:
      - not before (YYYY-MM-DD HH:MM in UTC, empty for NOW):
      - repeat after (hours,@daily,@weekly,@monthly, 0:no repeat): @daily

Task created with ID '1'. It is currently set as disabled.
You can enable it with `oscapd-cli task 1 enable
```

Como indica la propia herramienta, debemos activar la tarea para que sea ejecutada periódicamente, según se indica a continuación:

```
#> oscapd-cli task 1 enable
```

Una vez habilitada, podemos comprobar los resultados de la ejecución mediante la opción 'info'

```
#> oscapd-cli task 1 info

Title    | Daily Security Policy Check
ID       | 1
Target   | localhost
Created  | 2019-12-17 18:28:01
Modified | 2019-12-17 18:28:01

Latest results:
---+---------------------+----------
ID | Timestamp           | Status
---+---------------------+----------
2  | 2019-12-18 19:19:32 | Compliant
1  | 2019-12-17 19:11:07 | Compliant
```

7.2. Despliegue durante la instalación empleando anaconda

Tal y como se indica en el apartado 2.2.5, el instalador anaconda nos permite aplica la política de seguridad definida para el sistema durante su instalación y antes incluso del primer arranque. Con carácter general, el instalador evaluará el cumplimiento de la política indicada y aplicará los remedios (*fixes*) definidos al sistema tras su instalación inicial.

Anaconda permite aplicar ciertos *fixes* especiales durante la instalación en lugar de hacerlo al final. Al aplicarse durante la fase de instalación, es posible realizar de forma sencilla determinadas comprobaciones y aplicar remedios que son más complejos de efectuar con el sistema ya instalado (por ejemplo: reglas de particionado, control de paquetes instalados o requisitos de complejidad de las contraseñas, ya que la contraseña de root se define durante el proceso de instalación).

Para que el instalador aplique correctamente estos *fixes* especiales, deberán identificarse como aplicables al sistema durante la instalación. Para ello, definiremos las correspondientes reglas como aplicables al sistema: `urn:redhad:anaconda:pre`

A continuación, se incluye un resumen de las comprobaciones especiales permitidas por Anaconda durante la instalación del sistema.

7.2.1. Reglas de Particionado

Anaconda soporta la definición de reglas de particionado para el sistema, que serán comprobadas durante la instalación, de forma que no se permite continuar con la instalación hasta que no se cumple la condición indicada por la regla. Con carácter general, se pueden establecer requisitos para las particiones del sistema aplicando la sintaxis siguiente:

```
part MOUNTPOINT [--mountoptions=OPT1[,OPT2[,OPT3…]]]
```

Tomemos, por ejemplo, la partición /boot. De acuerdo a lo indicado en los apartados 3.2.1, 4.3.1 y 4.3.3, /boot deberá estar montada con las opciones: `noauto`, `noexec`, `nodev`, `nosuid` y `ro`. De acuerdo con la sintaxis anterior, el formato del fix dentro del archivo XCCDF sería el siguiente:

```
<fix reboot=”false” disruption=”high” system=”urn:redhat:anaconda:pre”>
part /boot --mountoptions=”nodev,noauto,noexec,nosuid,ro” </fix>
```

7.2.2.Reglas de Instalación de Paquetes

Anaconda soporta la definición de reglas de instalación de paquetes, que permiten identificar paquetes que es obligatorio instalar (`package --add`) y paquetes que no deben ser instalados (`–package --remove`). Es importante destacar que el instalador no garantiza el cumplimiento de la directiva `remove` ya que, aunque se indique que un paquete no debe ser instalado, lo será si forma parte de las dependencias de otro paquete que sí se ha marcado para su instalación en el sistema.

```
<fix reboot=”false” disruption=”high” system=”urn:redhat:anaconda:pre”>
package --remove=packageToRemoveA --remove=packageToRemoveB
package --add=packageToAddA       --add=packageToAddB
</fix>
```

7.2.3.Reglas de robustez de las contraseñas

Anaconda tiene un soporte limitado para comprobar la robustez de las contraseñas. Soporta una directiva para indicar la longitud mínima de las contraseñas introducidas durante la instalación (`passwd --minlen=N`). Por limitaciones en el programa de instalación, únicamente se muestra un aviso al usuario si la contraseña elegida no cumple el requisito de longitud mínima, ya que el instalador no tiene capacidad para forzar una entrada con una longitud mínima predeterminada. Por este motivo, el soporte en este sentido es muy limitado.

7.2.4.Reglas del gestor de arranque

Anaconda tiene un soporte limitado para la configuración del gestor de arranque durante la instalación. Soporta una única directiva (`bootloader --passwd`) para obligar a establecer una contraseña para el gestor de arranque del sistema.

8. Conclusiones y líneas de futuro

8.1. Conclusiones

8.1.1. Guías de Bastionado. Guía CCN-STIC-619

El modelo basado en guías de bastionado empleando procedimientos paso a paso no garantiza adecuadamente la seguridad de los sistemas. Tras realizar para este TFM la implementación de las recomendaciones y controles empleando SCAP, pueden extraerse las siguientes conclusiones sobre la guía editada por el CCN:

1. **Los requisitos contenidos en la guía pueden ser implementados de diversas formas, que ofrecen diferentes grados de protección.** En el caso por ejemplo del requisito “deshabilitar el acceso a la línea de comandos de grub”, podrían considerarse válidas las siguientes soluciones:
    - Configurar una contraseña en el gestor de arranque para acceder a la línea de comandos
    - Deshabilitar la línea de comandos
    - Arrancar inmediatamente el sistema, sin esperar a la entrada del usuario

    En este caso, el protocolo SCAP permite a los expertos en seguridad diseñar e implementar la comprobación de forma automática y transparente, ofreciendo una mayor garantía que la edición de guías paso a paso lo que supone una clara mejora para la seguridad de los sistemas.

2. **La guía contiene referencias a requisitos deseables o no definidos claramente** (con expresiones como “siempre que sea posible”, “es recomendable”). El protocolo SCAP permite establecer una definición objetiva y priorizada (por la severidad asignada a cada regla) de los controles a implementar

3. **Los requisitos de la guía son incompletos.** Por ejemplo, cuando se habla de la inclusión del directorio actual en la variable de entorno “PATH”, la guía menciona lo siguiente: “el PATH no debe figurar el directorio actual (.)”. Los perfiles de protección consultados para la elaboración de este TFM consideran habitualmente además del anterior, los siguientes controles de seguridad:
    - PATH no comienza con “:” o “.”
    - PATH no contiene “::” o “..”
    - PATH no termina en “:” o “.”

4. **La guía no constituye un mecanismo sencillo ni fácilmente mantenible para gestionar la configuración de seguridad de los sistemas**. La guía obliga a que el bastionado se lleve a cabo de forma manual, con una importante intervención de los administradores, de forma que resulta compleja (y costosa) la automatización, el sostenimiento en el tiempo (actualizaciones) y en general la comodidad y escalabilidad del proceso.

8.1.2. Ventajas de SCAP

A la vista de lo anterior, podemos decir que el protocolo SCAP presenta las siguientes ventajas:

- SCAP proporciona un modelo escalable, fácilmente mantenible, auditable e interoperable de implementar y auditar controles de seguridad, así como de identificar vulnerabilidades y problemas de configuración.
- SCAP define un estándar abierto, que permite compartir contenidos entre herramientas de seguridad.
- Los controles y comprobaciones de seguridad definidos mediante SCAP no están sujetos a interpretación o ambigüedad. Se emplea un lenguaje de programación (OVAL, XCCDF) tanto para para definir como para verificar los controles necesarios. SCAP permite, por tanto, definir y compartir guías y políticas de seguridad definidas mediante un lenguaje estándar.
- El lenguaje puede ser comprendido tanto por personas como por máquinas y permite la colaboración y la reutilización de contenido entre sistemas/usuarios/configuraciones.
- La posibilidad de compartir, descargar y aplicar guías de seguridad de forma automática supone, en la práctica, un incremento significativo de la seguridad de los sistemas sin incrementar apreciablemente el esfuerzo dedicado a configuración y mantenimiento por parte de los administradores.
- SCAP permite la comprobación automática y periódica de los controles, lo cual facilita la gestión y el mantenimiento de los sistemas. Las capacidades de remedio constituyen una ventaja significativa, al permitir modificar automáticamente la configuración de un sistema para que cumpla con una política de seguridad determinada, facilitando por tanto el cumplimiento de las políticas de seguridad definidas, con menor esfuerzo por parte de los administradores
- SCAP permite el despliegue automático de políticas de seguridad durante la instalación de los sistemas
- SCAP proporciona medios adecuados para la revisión, control de configuración y actualización de los controles de seguridad definidos.

8.2. Líneas de futuro

Su definición e implantación por parte del NIST, así como por Red Hat (uno de los principales distribuidores de software basado en Linux en la actualidad) hace presagiar que, en el futuro, el uso del protocolo SCAP se generalice a gran parte de la comunidad interesada en la seguridad de los sistemas. Actualmente, la mayoría de las herramientas y fabricantes de soluciones seguridad utilizan de alguna forma el protocolo SCAP.

A nivel nacional es previsible que en el futuro el CCN comience la distribución de contenido SCAP en relación con las políticas de seguridad definidas para garantizar la seguridad de los sistemas bajo su responsabilidad, aprovechando las ventajas enumeradas en el apartado anterior.

Bibliografía

1. Baker. (2011). *The OVAL Language Specification. Version 5.10.* MITRE Corporation.
2. BOE num. 68 de 19 de Marzo de 2004. (12 de Marzo de 2004). *RD 421/2004 por el que se regula el Centro Criptológico Nacional*. Boletín Oficial del Estado.
3. CCN-STIC-619. (2019). *Implementación de Seguridad sobre CentOS7 (Cliente Independiente).* CCN-STIC.
4. Cheikes. (2011). *Common Platform Enumeration: Naming Specification Version 2.3.* NIST.
5. FIRST.org. (2019). *Common Vulnerability Scoring System Version 3.1.* FIRST.org.
6. *OpenScap*. (Consultado el 27 de Diciembre de 2019). Obtenido de www.openscap.org
7. Waltermire. (2011). *Specification for the Open Checklist Interactive Language (OCIL) Version 2.0.* NIST.
8. Waltermire. (2012). *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2.* NIST.
9. Waltermire. (2018). *The Technical Specification for the Security Content Automation Protocol (SCAP) Version 1.3.* NIST.