https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153

Vol. 4, Núm. 1. enero-marzo 2026, págs. 71 - 80

# Automatización de auditorías de seguridad en sistemas operativos mediante OpenSCAP

*Automation of security audits for operating systems using OpenSCAP*

**Información del reporte:**



Para citar este reporte técnico:

Hernández Fuentes, F.A. (2026). Automatización de auditorías de seguridad en sistemas operativos mediante OpenSCAP. *Cuadernos Técnicos Universitarios de la DGTIC, 4* (1), páginas (71 - 80). https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153

**Félix Alejandro Hernández Fuentes**

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

felixhdz@ciencias.unam.mx

ORCID: 0000-0002-4791-485X

## Resumen

La auditoría de configuraciones de seguridad en sistemas operativos, a cargo de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, representaba un reto debido al tiempo considerable requerido por las revisiones efectuadas de forma manual y a la necesidad de garantizar altos niveles de cumplimiento con prácticas y recomendaciones de seguridad reconocidas internacionalmente. En este contexto, se evaluó el uso de la herramienta OpenSCAP para automatizar tanto la revisión como la corrección de configuraciones de seguridad. La evaluación se llevó a cabo en un entorno de pruebas con sistemas operativos de uso común en la Universidad. La herramienta permitió realizar auditorías automatizadas conforme a buenas prácticas, aplicar correcciones de forma autónoma y medir objetivamente el nivel de cumplimiento antes y después de las acciones correctivas. Los resultados mostraron que el uso de OpenSCAP redujo significativamente el tiempo de ejecución de las auditorías. Además, las correcciones automáticas aplicadas mejoraron notablemente el cumplimiento de las recomendaciones de seguridad, alcanzando niveles superiores al 90%. No obstante, se identificaron configuraciones que requirieron intervenciones manuales, sobre todo aquellas relacionadas con la gestión de contraseñas de arranque, la administración de particiones y el control de acceso a servicios críticos. Estos resultados mostraron que la automatización permitió disminuir la carga operativa

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 72 - 80

y hacer más uniformes los procesos de verificación, sin sustituir completamente la necesidad de supervisión técnica en casos específicos. Se concluyó que integrar mecanismos de automatización en los procedimientos institucionales contribuye a un modelo más eficiente de gestión de seguridad de la información en la Universidad.

**Palabras clave:** Automatización de auditorías de seguridad, CIS *benchmarks*, configuración segura de sistemas operativos, OpenSCAP, seguridad informática.

***Abstract***

*The security configuration audit of operating systems, managed by the Dirección General de Cómputo y de Tecnologías de Información y Comunicación, posed a challenge due to the considerable time required for manual reviews and the need to ensure high levels of compliance with internationally recognized security practices and recommendations. In this context, the use of the OpenSCAP tool was evaluated to automate both the review and correction of security configurations. The evaluation was conducted in a test environment with commonly used operating systems at the University. The tool enabled automated audits based on best practices, autonomously applied corrections, and objectively measured compliance levels before and after corrective actions. The results showed that the use of OpenSCAP significantly reduced the execution time of audits. Additionally, the automated corrections applied improved compliance with security recommendations, reaching levels above 90%. However, certain configurations were identified that required manual intervention, particularly those related to boot password management, partition administration, and access control to critical services. These results demonstrated that automation helped reduce operational workload and made verification processes more uniform, without completely replacing the need for human supervision in specific cases. It was concluded that integrating automation mechanisms into institutional procedures contribute to a more efficient model for information security management at the University.*

***Keywords:*** *CIS benchmarks, information security, OpenSCAP, secure operating systems configuration, security audit automation.*

# 1. INTRODUCCIÓN

Hoy en día, la seguridad de la información es señalada como un aspecto fundamental para proteger las infraestructuras tecnológicas, tanto en el sector público como en el privado. Con el aumento de la complejidad de los entornos digitales y la frecuencia de los incidentes de seguridad, resulta indispensable asegurar que los sistemas operativos que gestionan servicios críticos estén correctamente configurados.

En este contexto, la auditoría de configuraciones de seguridad se entiende como el proceso sistemático orientado a revisar el cumplimiento de las configuraciones de un sistema operativo con respecto a un conjunto de reglas establecidas en buenas prácticas de seguridad. Dentro de este proceso, en opinión del autor, la verificación corresponde a la comprobación técnica del estado real de cada configuración frente a una regla específica, mientras que la evaluación se refiere al análisis del grado de cumplimiento global del sistema a partir de los resultados obtenidos.

Diversos estudios han destacado la importancia de utilizar herramientas que automaticen las auditorías de configuraciones y permitan verificar su cumplimiento con buenas prácticas reconocidas en seguridad.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 73 - 80

Webb, Henderson y Webb (2019) mostraron que el uso de software de código abierto, como OpenSCAP, facilita la automatización del monitoreo y la verificación de cumplimiento en entornos de prueba automatizados, reduciendo tanto costos como carga operativa. Liu y Hu (2023) destacaron la efectividad de aplicar el *Security Content Automation Protocol* (SCAP) [definido por el National Institute of Standards and Technology (NIST, 2025) como un estándar para automatizar la evaluación de configuraciones de seguridad] en equipos informáticos locales, evidenciando mejoras en la consistencia y confiabilidad de los procesos de auditoría.

Por su parte, Bandara *et al.* (2024) resaltaron cómo el uso de OpenSCAP y otras herramientas de automatización puede simplificar las auditorías de seguridad, permitiendo detectar y corregir vulnerabilidades de forma más rápida y mantener el cumplimiento con estándares vigentes. Asimismo, Urtamo y Costin (2023) demostraron la viabilidad del uso de herramientas basadas en SCAP, como OpenSCAP, para automatizar la verificación de políticas de seguridad y el escaneo de vulnerabilidades en sistemas operativos compatibles con este estándar. Finalmente, Bakhtiyarov y Mammadov (2024) analizaron la aplicabilidad de OpenSCAP en entornos empresariales, destacando su capacidad para generar reportes reproducibles y consistentes con estándares de seguridad reconocidos.

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) llevó a cabo auditorías de configuraciones de sistemas operativos siguiendo las recomendaciones del *Center for Internet Security* (CIS), una organización reconocida internacionalmente por sus guías de buenas prácticas de seguridad, conocidas como *CIS Benchmarks* (CIS, 2025). Estas auditorías forman parte de los servicios institucionales de seguridad informática que ofrece la DGTIC, orientados a fortalecer la protección de los sistemas operativos y aplicaciones utilizados en la Universidad, en concordancia con la *Política General de Seguridad de la Información en la DGTIC* (DGTIC, 2023; DGTIC, 2024).

No obstante, este proceso, realizado de manera manual, implicaba un esfuerzo considerable por parte del personal técnico y presentaba limitaciones, principalmente asociadas al tiempo requerido para completar cada revisión. Ante este escenario, surgió el propósito de automatizar las auditorías de configuraciones con el fin de reducir el trabajo manual, facilitar la reproducción de los resultados y mantener el cumplimiento con las recomendaciones de seguridad reconocidas.

En este contexto, el objetivo de este proyecto fue evaluar la viabilidad de utilizar OpenSCAP como herramienta de apoyo para la DGTIC en la automatización de auditorías de configuraciones de seguridad, con el propósito de hacer más eficiente y uniforme este proceso.

## 2. DESARROLLO TÉCNICO

La auditoría de configuraciones de seguridad en sistemas operativos es un proceso complejo y susceptible a errores humanos cuando se realiza de manera manual. En múltiples organizaciones, se siguen lineamientos como los *CIS Benchmarks*, cuya implementación permite establecer un nivel mínimo de seguridad aceptable en los sistemas evaluados.

Sin embargo, cuando el número de sistemas auditados es elevado, la revisión manual no resulta eficiente. Este es el caso de la Universidad, donde las tareas de auditoría requieren un tiempo considerable por parte del personal técnico y pueden presentar variaciones en los resultados, lo que dificulta la estandarización de los procesos de verificación.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 74 - 80

Existen diversas soluciones para la automatización de auditorías de configuraciones de seguridad. Algunas herramientas propietarias están disponibles, pero su uso suele verse limitado por el costo de licencias, la falta de flexibilidad en la personalización de políticas y la dependencia de un proveedor específico. En contraste, tal como lo mencionan Webb *et al.* (2019), las herramientas de código abierto han mostrado mayor flexibilidad y adaptabilidad a distintos contextos organizacionales. Esta idea se aplicó en el contexto institucional a través de la adopción de una solución de código abierto capaz de ejecutar auditorías automatizadas y alineadas con buenas prácticas de seguridad.

Entre las alternativas disponibles dentro del software libre, destaca OpenSCAP (OpenSCAP, 2025), un proyecto desarrollado por la comunidad, respaldado por Red Hat y alineado con el estándar SCAP. Tanto Bandara *et al.* (2024) como Bakhtiyarov y Mammadov (2024) coincidieron en que OpenSCAP puede aplicarse con buenos resultados en entornos empresariales, facilitando auditorías automatizadas, generando reportes consistentes y contribuyendo al cumplimiento de estándares reconocidos de seguridad.

A diferencia de otras herramientas, OpenSCAP permite integrar políticas de seguridad preexistentes, como los *CIS Benchmarks*, y adaptarlas a las necesidades específicas de cada organización. Lo anterior lo convierte en una opción adecuada para el contexto de la Universidad, donde la diversidad tecnológica y el volumen de sistemas requieren soluciones escalables y sostenibles.

El presente trabajo se desarrolló a partir de un proceso institucional de auditoría manual de configuraciones de sistemas operativos, llevado a cabo por la DGTIC conforme a los *CIS Benchmarks*. Con base en este contexto, se diseñó una metodología orientada a evaluar, de manera objetiva, el impacto de la automatización de auditorías y la aplicación de remediaciones automáticas mediante OpenSCAP. Dicha metodología se fundamentó en la ejecución comparativa de auditorías iniciales y posteriores a las acciones correctivas, cuyos resultados se presentan en la Sección 3.

## 2.1 METODOLOGÍA

El trabajo se estructuró siguiendo un enfoque sistemático dividido en cuatro etapas: diseño, configuración, instalación y pruebas. Este enfoque permitió operacionalizar el objetivo planteado, asegurando un proceso automatizado, reproducible y técnicamente consistente para la auditoría de configuraciones de sistemas operativos mediante OpenSCAP.

En la etapa de diseño, se seleccionaron tres sistemas operativos de uso común en la Universidad: Ubuntu 24.04, Debian 12 y Fedora 42. Esta selección se basó en la disponibilidad de perfiles de seguridad alineados con los *CIS Benchmarks* y en su compatibilidad con OpenSCAP. Asimismo, la planificación se apoyó en estudios recientes sobre automatización de auditorías y buenas prácticas en la verificación de configuraciones de seguridad.

Los perfiles utilizados correspondieron al nivel 1 (*Level* 1) de los *CIS Benchmarks*, ya que éste está orientado a proporcionar configuraciones de seguridad recomendadas que pueden aplicarse sin afectar de manera significativa la funcionalidad del sistema. En el contexto institucional de la Universidad, este nivel ofrece un equilibrio adecuado entre fortalecimiento de la seguridad y estabilidad operativa.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 75 - 80

Durante la configuración, se prepararon máquinas virtuales con la instalación por defecto de cada sistema operativo, sin aplicar ajustes de seguridad previos. Todas las pruebas se realizaron en un entorno virtualizado mediante VMware Workstation 17 Pro, utilizando máquinas virtuales independientes para cada plataforma y conectividad de red estándar en modo NAT, sin exposición a servicios externos, con el fin de evitar interferencias durante la evaluación.

En todos los casos, se asignó la misma configuración base de recursos de hardware: un procesador con dos núcleos, 4GB de memoria RAM y 40GB de almacenamiento, con el fin de mantener un entorno homogéneo de evaluación y asegurar que las variaciones observadas en los resultados se debieran exclusivamente a la aplicación de las auditorías y remediaciones, y no a diferencias en la infraestructura subyacente.

Las características técnicas específicas del entorno experimental, incluyendo las versiones exactas de OpenSCAP y los perfiles CIS utilizados en cada sistema operativo, se resumen en la Tabla 1, con el objetivo de asegurar la reproducibilidad del procedimiento.

**Tabla 1**

*Características técnicas del entorno experimental*

| Sistema operativo | Versión OpenSCAP | Perfil CIS utilizado |
|---|---|---|
| Ubuntu 24.04 (64-bit) | 1.3.9 | CIS Ubuntu Linux 24.04 LTS Benchmark for Level 1 – Workstation |
| Debian 12 (64-bit) | 1.3.7 | CIS Debian Benchmark for Level 1 – Workstation |
| Fedora 42 (64-bit) | 1.4.3 | DRAFT – CIS Fedora Benchmark for Level 1 – Workstation |

*Nota.* Todas las máquinas virtuales fueron desplegadas mediante virtualización de tipo hosted sobre VMware Workstation 17 Pro (versión 17.6.2 build-24409262), con configuraciones de hardware equivalentes.

En la etapa de instalación, se desplegó OpenSCAP en las máquinas virtuales configuradas. Se instalaron los paquetes necesarios, así como las dependencias y herramientas auxiliares requeridas para llevar a cabo las auditorías. Tanto la configuración como la instalación se documentaron, asegurando que el proceso pudiera reproducirse y verificarse en el futuro.

En la fase de pruebas, se realizaron dos auditorías por cada sistema operativo. La primera estableció la línea base de cumplimiento y la segunda se llevó a cabo después de aplicar las correcciones automáticas. Ambas auditorías se ejecutaron en condiciones controladas para asegurar que los resultados obtenidos fueran comparables.

OpenSCAP generó reportes que incluyeron:

- el porcentaje de cumplimiento global del sistema,
- el número de reglas cumplidas y no cumplidas,
- el detalle individual de cada regla evaluada,
- recomendaciones de corrección,

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 76 - 80

- la clasificación de severidad de las reglas (*high, medium, low*), y
- las referencias asociadas a cada control.

Cabe señalar que el porcentaje de cumplimiento reportado corresponde a una puntuación ponderada, calculada conforme al modelo de evaluación utilizado por OpenSCAP, el cual considera la severidad de las reglas evaluadas y no únicamente su número total.

Las auditorías de seguridad se realizaron utilizando perfiles de evaluación incluidos en los *CIS Benchmarks*, los cuales definen un conjunto de reglas orientadas a verificar configuraciones específicas del sistema operativo, tales como políticas de contraseñas, permisos de archivos, parámetros de red, servicios activos y controles de privilegios. De este modo, cada regla fue evaluada automáticamente por OpenSCAP, determinando su cumplimiento o incumplimiento con base en el estado real del sistema al momento de la auditoría.

Las remediaciones automáticas se aplicaron únicamente en aquellos casos en los que el perfil de auditoría incluía acciones de corrección explícitamente definidas. Estas acciones consistieron principalmente en la modificación de parámetros del sistema, ajustes en archivos de configuración y la habilitación o deshabilitación de servicios. No todas las reglas contaban con mecanismos de corrección automática, por lo que algunas configuraciones requirieron análisis o intervención manual posterior, con el fin de evitar afectaciones operativas.

Es importante señalar que la aplicación de remediaciones automáticas puede implicar riesgos operativos, como la modificación inadvertida de configuraciones críticas o la posible afectación de servicios. Por esta razón, las pruebas realizadas en este trabajo se llevaron a cabo exclusivamente en entornos controlados, utilizando máquinas virtuales y sin impacto sobre sistemas productivos. Asimismo, se consideró que la adopción de este tipo de mecanismos en entornos reales debe acompañarse de buenas prácticas, tales como la validación previa en ambientes de prueba, la realización de respaldos, la aplicación gradual de cambios y la supervisión técnica de las remediaciones implementadas.

El método utilizado garantizó transparencia y consistencia, tomando como referencia prácticas descritas en la literatura académica y en estándares internacionales, como los definidos por el NIST para SCAP (NIST, 2025). Gracias a esta base, fue posible obtener resultados medibles y confiables, alineados con el objetivo de este trabajo.

## 3. RESULTADOS

Las auditorías realizadas permitieron evaluar el impacto de OpenSCAP en los sistemas operativos seleccionados. El análisis se centró en tres plataformas de uso común en la Universidad: Ubuntu 24.04, Debian 12 y Fedora 42. El proceso incluyó una auditoría inicial para establecer la línea base, la aplicación de remediaciones automatizadas y una auditoría final para medir el cumplimiento alcanzado. Los reportes completos para los sistemas auditados (Ubuntu 24.04, Debian 12 y Fedora 42, línea base y post-remediación), generados por OpenSCAP y que detallan cada auditoría y sus resultados, se encuentran disponibles como material complementario en línea[1]. Cada archivo incluye el porcentaje de cumplimiento,

1 En la carpeta ubicada en https://drive.google.com/drive/folders/1LhdVMakP4duhh7Ro2Snh-5-69aLKvtlw que el autor se compromete a mantener disponible para consulta de los lectores de este reporte técnico.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 77 - 80

reglas cumplidas y no cumplidas, detalles de cada regla, recomendaciones de corrección, clasificación de severidad y referencias asociadas. Este material permite consultar los resultados directamente y profundizar en los detalles técnicos de las auditorías, asegurando transparencia y seguimiento del proceso.

La auditoría inicial estableció la línea base de cumplimiento para los sistemas operativos evaluados. Los resultados mostraron niveles parciales de conformidad, que se resumen en la Tabla 2.

**Tabla 2**

*Resultados de la auditoría inicial de cumplimiento de configuraciones de seguridad*

| Sistema operativo | Reglas cumplidas | Reglas no cumplidas | Cumplimiento (%) |
|---|---|---|---|
| Ubuntu 24.04 | 242 | 113 | 65.76 |
| Debian 12 | 235 | 112 | 68.56 |
| Fedora 42 | 144 | 113 | 71.54 |

*Nota.* Los resultados corresponden a la auditoría inicial efectuada mediante OpenSCAP, con base en los *CIS Benchmarks*.

Los reportes generados por OpenSCAP mostraron que los tres sistemas evaluados presentaban configuraciones no conformes en áreas críticas y operativas. Entre los principales hallazgos, se identificaron los siguientes:

- la gestión de contraseñas,
- los parámetros de red,
- el control de privilegios mediante *sudo*,
- los permisos de tareas programadas, y
- la configuración de herramientas de integridad como AIDE.

Todas estas no conformidades fueron identificadas de acuerdo con las reglas definidas en los *CIS Benchmarks*, lo que permitió precisar los incumplimientos más relevantes en los sistemas auditados.

Después de aplicar las remediaciones automáticas con OpenSCAP, se realizó otro ciclo de auditoría para medir el impacto de las correcciones. Los resultados se muestran en la Tabla 3.

**Tabla 3**

*Resultados de la auditoría posterior a las remediaciones automáticas*

| Sistema operativo | Reglas cumplidas | Reglas no cumplidas | Cumplimiento (%) |
|---|---|---|---|
| Ubuntu 24.04 | 347 | 6 | 92.39 |
| Debian 12 | 334 | 16 | 93.04 |
| Fedora 42 | 245 | 12 | 93.93 |

*Nota*. Los resultados corresponden a la segunda auditoría tras remediaciones automáticas con OpenSCAP, basada

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 Vol. 4, Núm. 1. enero-marzo 2026, págs. 78 - 80

en los CIS Benchmarks.

Los resultados representan mejoras de 26, 24 y 22 puntos porcentuales, respectivamente. Esto demuestra la efectividad de OpenSCAP para corregir configuraciones inseguras y uniformizar el proceso de auditoría en distintas plataformas.

La ejecución de las revisiones se volvió más rápida y eficiente gracias al uso de OpenSCAP. Además, permitió aplicar remediaciones automáticas y mejorar el cumplimiento de los sistemas auditados. Esto redujo la carga operativa sobre el personal técnico y garantizó resultados más consistentes. No obstante, algunos casos aún requirieron atención manual, particularmente en configuraciones relacionadas con la administración de particiones, seguridad física y control de accesos. Lo anterior confirma que la supervisión técnica sigue siendo indispensable.

En términos operativos, la auditoría manual de configuraciones requería, en promedio, alrededor de 13 días de trabajo, con la participación de dos integrantes del equipo técnico. En contraste, la auditoría automatizada con OpenSCAP permitió evaluar el sistema, aplicar las remediaciones disponibles y generar los reportes correspondientes en menos de una hora, requiriendo la intervención de una sola persona. Esta diferencia evidencia una reducción sustancial en el tiempo de ejecución y en el esfuerzo humano necesario para llevar a cabo el proceso de auditoría.

Los resultados obtenidos, con niveles de cumplimiento superiores al 90%, demostraron la eficacia de la herramienta para mejorar la conformidad de las configuraciones y fortalecer los procesos de auditoría institucionales. Asimismo, el procedimiento permitió generar reportes estructurados y verificables, incrementando la capacidad de la DGTIC para identificar y corregir desviaciones en configuraciones críticas. En conjunto, estos hallazgos confirman que la automatización mediante OpenSCAP puede aplicarse de manera efectiva en entornos con diversidad tecnológica, ofreciendo una base sólida para su adopción a mayor escala dentro de la Universidad.

## 4. CONCLUSIONES

En este reporte técnico, se expuso la necesidad de automatizar las auditorías de configuraciones de sistemas operativos basadas en las recomendaciones de los *CIS Benchmarks* en la Universidad. El propósito fue reducir la carga operativa, obtener resultados más uniformes y reproducibles, así como elevar el nivel de cumplimiento de las configuraciones evaluadas. El proceso previo requería de mucho tiempo y esfuerzo por parte del personal técnico, que debía revisar y documentar los resultados de cada regla de seguridad de manera manual.

Los resultados demostraron que la implementación de OpenSCAP redujo de manera significativa el tiempo necesario para completar las auditorías. Además, permitió alcanzar niveles de cumplimiento superiores al 90% en los sistemas evaluados. La herramienta ejecutó auditorías alineadas con buenas prácticas de seguridad reconocidas internacionalmente, aplicó remediaciones automáticas y generó reportes consistentes y reproducibles. No obstante, se identificaron configuraciones que requirieron intervención manual, particularmente aquellas relacionadas con la gestión de contraseñas, la administración de particiones y el control de accesos a servicios críticos. Esto confirma la necesidad de mantener supervisión técnica en casos específicos.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 **Vol. 4, Núm. 1.** enero-marzo 2026, págs. 79 - 80

Se recomienda seguir incorporando la automatización en los procesos institucionales de auditoría y ampliar la aplicación de los perfiles *CIS Benchmark* a más sistemas operativos. Además, sería importante que todos los servidores sean auditados antes de su puesta en marcha, complementando este proceso con auditorías periódicas durante su operación. Estas medidas ayudarían a fortalecer los procesos de auditoría, haciéndolos más eficientes, replicables y sostenibles. Así, se contribuiría a mantener y mejorar la seguridad de la información en la Universidad.

## AGRADECIMIENTOS

Quiero expresar mi sincero agradecimiento a la Coordinación de Seguridad de la Información de la DGTIC por su generosa acogida y por brindarme la oportunidad de realizar este trabajo. También agradezco profundamente a los revisores anónimos por sus valiosos comentarios y sugerencias, los cuales han sido fundamentales para mejorar de manera sustancial este reporte técnico.

## REFERENCIAS

Bakhtiyarov, B., & Mammadov, V. (2024). OpenSCAP technology application to enterprise. *PAHTEI-Proceedings of Azerbaijan High Technical Educational Institutions, 42*(05), 221-228. https://doi.org/10.36962/pahtei42072024-24

Bandara, E., Shetty, S., Rahman, A., Mukkamala, R., Foytik, P., & Liang, X. (2024). RMF-GPT — OpenAI GPT-3.5 LLM, Blockchain, NFT, Model Cards and OpenSCAP Enabled Intelligent RMF Automation System. *2024 International Conference on Computing, Networking and Communications (ICNC)*, 653-658. https://doi.org/10.1109/ICNC59896.2024.10555963

Center for Internet Security. (2025). *CIS Benchmarks: Security configuration guides*. https://www.cisecurity.org/cis-benchmarks/

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2023). *Política General de Seguridad de la Información en la DGTIC*. Universidad Nacional Autónoma de México. https://www.tic.unam.mx/politica-general-seguridad-informacion/

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2024). *Seguridad informática para sistemas operativos y aplicaciones*. Universidad Nacional Autónoma de México. https://sistemas.tic.unam.mx/index.php/seguridad-informatica-sistemas-operativos-aplicaciones/

Liu, Y., & Hu, B. (2023). Security baseline verification technology for domestic computer terminal based on SCAP. *2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS)*, 171-174. https://doi.org/10.1109/ICPICS58376.2023.10235334

National Institute of Standards and Technology. (30 de septiembre de 2025). *Security Content Automation Protocol (SCAP)*. https://csrc.nist.gov/projects/security-content-automation-protocol

OpenSCAP. (2025). *OpenSCAP project*. https://www.open-scap.org/

Urtamo, I., & Costin, A. (2023). On tools for practical and effective security policy management and vulnerability scanning. En B. Shishkov (Ed.), *Business Modeling and Software Design. BMSD 2023*.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.153 **Vol. 4, Núm. 1.** enero-marzo 2026, págs. 80 - 80

*Lecture Notes in Business Information Processing* (Vol. 483, pp. 375-382). Springer. https://doi.org/10.1007/978-3-031-36757-1_28

Webb, J. A., Henderson, M. W., & Webb, M. L. (2019). An open source approach to automating surveillance and compliance of automatic test systems. *2019 IEEE AUTOTESTCON*, 1-8. https://doi.org/10.1109/AUTOTESTCON43700.2019.8961077