

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN



**TECNOLÓGICO
DE ESTUDIOS SUPERIORES
DE CUAUTITLÁN IZCALLI**

**T
E
S
C
I**

**“DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES
CRÍTICOS”**

TESIS

**QUE PARA OBTENER EL GRADO DE:
MAESTRO EN TECNOLOGÍAS DE LA INFORMACIÓN**

PRESENTA:

JESÚS EDUARDO CARBAJAL LEDEZMA

DIRECTORA DE TESIS:

MTRA. MARÍA DEL CONSUELO MACÍAS GONZÁLEZ

AUTORIZACIÓN

AGRADECIMIENTOS

A lo largo de la elaboración de este trabajo, he contado con la confianza, el apoyo y las valiosas recomendaciones de personas sumamente capacitadas y especializadas.

Deseo expresar mi más profundo agradecimiento a mi madre, María de la Luz Ledesma Santiago, por su amor incondicional y su apoyo constante en cada etapa del camino. A mi padre, José Eduardo Carbajal Trejo, por su fortaleza. A mis hermanos, Evelyn Carbajal Ledesma y Joseph Bryan Carbajal Ledesma, por estar siempre a mi lado con su compañía y palabras motivadoras. A mis sobrinos, Brittany Rosaly Castañeda Carbajal, Eithan Damian Hernández Carbajal y Dariel Carbajal Ramírez, quienes me han impulsado a seguir adelante.

Finalmente, agradezco profundamente a mi directora de tesis, Mtra. María del Consuelo Macías González, por su orientación y dedicación incansable durante todo este proceso. Su apoyo ha sido fundamental para alcanzar este logro.

DEDICATORIA

A mis padres, María de la Luz y José Eduardo, por su amor incondicional, su paciencia infinita y su apoyo constante en cada momento de mi vida.

A mis hermanos, Evelyn y Joseph, por estar siempre a mi lado, brindándome su cariño, ánimo y fortaleza en los momentos difíciles.

A mis sobrinos, Brittany, Eithan y Dariel, cuyas sonrisas e inocencia me han recordado la importancia de seguir soñando y esforzándome por alcanzar mis metas.

A la Mtra. María del Consuelo Macías González, por ser una guía excepcional y por su fe en mi capacidad, lo cual me motivó a superar todos los obstáculos.

Dedico este trabajo con profundo agradecimiento y amor.

ÍNDICE

INTRODUCCIÓN.....	6
CAPÍTULO 1. MARCO CONTEXTUAL	8
1.1 Planteamiento del problema.....	9
2.1 Justificación.	10
3.1 Antecedentes.....	11
4.1 Objetivo general.	12
5.1 Objetivos específicos.....	12
6.1 Metas.	13
7.1 Impacto en el sector productivo y generación de conocimiento.	14
8.1 Reconocimiento del proyecto.	15
Análisis de Resultados.....	18
Conclusión.	19
9.1 Vinculación con el sector productivo.....	21
CAPÍTULO 2. MARCO TEÓRICO	23
10.1 Diseño.....	26
11.1 Diagrama de casos de uso.....	28
12.1 Diagrama de clases.....	30
Login.	31
SistemaEvaluación.	31
Evaluación.....	32
Corrección.....	32
Relaciones.	32
13.1 Diagrama de secuencia.....	33
Actores involucrados:	34
Pasos de la secuencia:	34
14.1 Diagrama de estados.	35
Estados principales:	35
15.1 Diagrama entidad relación.	36
Entidades:	37

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES

CRÍTICOS V

16.1	Maquetado.....	38
	Inicio de Sesión:.....	38
	Panel de Control:	39
	Gestión de usuarios:.....	40
17.1	Tabla de requerimientos.....	41
CAPÍTULO 3. MARCO METODOLÓGICO		45
18.1	Desarrollo.	47
	Fases Del Desarrollo.....	47
19.1	Pruebas de funcionamiento.....	51
	Acceso inicial.....	51
	Interfaz inicial.....	51
	Gestión de servidores.....	52
	Gestión de usuarios.....	52
	Comunicación.....	52
	Evaluación.	52
	Aplicación de correcciones.....	53
CAPÍTULO 4. APLICACIÓN DE LA METODOLOGÍA Y DISCUSIÓN DE RESULTADOS		54
	Acceso inicial.....	56
	Interfaz principal.	58
	Gestión de servidores.....	59
	Gestión de usuarios.....	60
	Comunicación.....	62
	Evaluación.	62
	Aplicación de correcciones.....	67
20.1	Validación y verificación.....	73
21.1	Discusión de resultados.	74
CAPÍTULO 5. CONCLUSIONES Y PERSPECTIVAS PARA TRABAJOS FUTUROS		77
REFERENCIAS		79

ANEXOS	80
Configuraciones.....	80

TABLA DE ILUSTRACIONES.

ILUSTRACIÓN 1 EJEMPLO DE ENCUESTA 1.	15
ILUSTRACIÓN 2 EJEMPLO DE ENCUESTA 2.	16
ILUSTRACIÓN 3 EJEMPLO DE ENCUESTA 3.	16
ILUSTRACIÓN 4 EJEMPLO DE ENCUESTA 4.	17
ILUSTRACIÓN 5 EJEMPLO DE ENCUESTA 5.	17
ILUSTRACIÓN 6 ANÁLISIS DE CUESTIONARIO.	20
ILUSTRACIÓN 7 DIAGRAMA DE CASOS DE USO.	28
ILUSTRACIÓN 8 DIAGRAMA DE CLASES.	31
ILUSTRACIÓN 9 DIAGRAMA DE SECUENCIA.	33
ILUSTRACIÓN 10 DIAGRAMA DE ESTADOS.	35
ILUSTRACIÓN 11 DIAGRAMA ENTIDAD-RELACIÓN.	36
ILUSTRACIÓN 12 MAQUETADO-INICIO DE SESIÓN.....	38
ILUSTRACIÓN 13 MAQUETADO - SISTEMA DE EVALUACIÓN.....	40
ILUSTRACIÓN 14 GESTIÓN DE USUARIOS.....	41
ILUSTRACIÓN 15 DIAGRAMA DE METODOLOGÍA.....	47
ILUSTRACIÓN 16 LOGIN.	48
ILUSTRACIÓN 17 INTERFAZ PRINCIPAL.....	49
ILUSTRACIÓN 18 GESTIÓN.	49
ILUSTRACIÓN 19 ADMINISTACIÓN DE SERVIDORES.....	50
ILUSTRACIÓN 20 ADMINISTRACIÓN DE USUARIOS.	50
ILUSTRACIÓN 21 ACCESO INICIAL.	56
ILUSTRACIÓN 22 CAMBIO DE PASSWORD.	57
ILUSTRACIÓN 23 CONFIRMACIÓN DE CAMBIO.	57
ILUSTRACIÓN 24 VISUALIZACIÓN INICIAL.	58
ILUSTRACIÓN 25 AGREGANDO SERVIDOR 1.	59
ILUSTRACIÓN 26 AGREGANDO SERVIDOR 2.	59
ILUSTRACIÓN 27 ELIMINAR SERVIDOR 2.	60
ILUSTRACIÓN 28 AGREGAR USUARIOS.	60
ILUSTRACIÓN 29 ACTUALIZAR USUARIOS.	61
ILUSTRACIÓN 30 CONFIRMACIÓN - ELIMINAR USUARIOS.	61
ILUSTRACIÓN 31 ELIMINAR USUARIOS.	61
ILUSTRACIÓN 32 CONEXIÓN EXITOSA.	62
ILUSTRACIÓN 33 EVALUACIÓN INICIAL.	63
ILUSTRACIÓN 34 EXPORTAR EVALUACIÓN INICIAL.....	64
ILUSTRACIÓN 35 EXPORTADO.	65
ILUSTRACIÓN 36 RESULTADOS PRIMERA EVALUACIÓN.	66
ILUSTRACIÓN 37 EVIDENCIA INICIAL.....	67
ILUSTRACIÓN 38 APLICACIÓN DE CORRECCIONES.	68
ILUSTRACIÓN 39 RESULTADOS.	69
ILUSTRACIÓN 40 SEGUNDA EVALUACIÓN.....	70
ILUSTRACIÓN 41 EXPORTAR SEGUNDA EVALUACIÓN.	71
ILUSTRACIÓN 42 EXPORTADO 2.....	72
ILUSTRACIÓN 43 RESULTADOS SEGUNDA EVALUACIÓN.	73

LISTA DE ABREVIATURAS Y TABLA DE SÍMBOLOS.

- **CIS:** Center for Internet Security
- **TI:** Tecnologías de la Información
- **SQL:** Structured Query Language
- **DDoS:** Distributed Denial of Service
- **CIS:** Center for Internet Security
- **CIS Benchmarks:** Conjunto de recomendaciones y mejores prácticas de configuración de seguridad desarrolladas por el Center for Internet Security
- **Scrum:** Nombre propio de la metodología ágil
- **IP:** Internet Protocol
- **WinRM:** Windows Remote Management
- **GUI:** Graphical User Interface (Interfaz Gráfica de Usuario)
- **WSMan:** Windows Management Instrumentation over SOAP (Servicio de Administración de Windows basado en SOAP)
- **TCP:** Transmission Control Protocol
- **HTTP:** Hypertext Transfer Protocol

RESUMEN

Este estudio se enfoca en la evolución tecnológica y el aumento en la complejidad de los ataques cibernéticos, resaltando la importancia de las configuraciones de seguridad en servidores críticos. A pesar de contar con herramientas como antivirus y firewalls, las deficiencias en estas configuraciones pueden dejar vulnerabilidades críticas sin protección.

El objetivo es proporcionar un enfoque detallado para mejorar la seguridad en las organizaciones, identificando configuraciones clave y ofreciendo correcciones de manera rápida y confiable. Se subraya la importancia de aplicar políticas de seguridad adecuadas, especialmente ante ataques dirigidos que podrían explotar fallos en la fortificación de los servidores.

Se sugiere el desarrollo de un software que simplifique la implementación de correcciones de seguridad, basado en las mejores prácticas regulativas como los CIS Benchmarks (Internet, 2024). No obstante, se recalca que este software no constituye una solución completa por sí solo, sino que debe combinarse con otras tecnologías de seguridad para garantizar una protección completa contra ataques cibernéticos.

Al concluir, se espera que este trabajo aporte un nuevo enfoque en las correcciones de seguridad, enfatizando la importancia de mantener adecuadamente el robustecimiento de servidores, más allá de simplemente depender de las últimas tecnologías o de realizar actualizaciones regulares del sistema operativo y las aplicaciones.

Palabras clave.

- **Corrección:** Aseguramiento de cambios aplicados a Servidores.
- **Reconstrucción:** Implementación de nuevas métricas de seguridad.
- **Reparar:** Gestionar lo que existe actualmente y establecer nuevas políticas.
- **Enmendar:** Determinar los elementos que afectan la infraestructura.
- **Proteger:** Mantener la integridad de los servicios que se ofrecen.
- **Estructura:** Consolidación de la información que se recopila de los sistemas informáticos.
- **Modelar:** Generar arquitecturas que permitan establecer la postura de seguridad.
- **Desarrollar:** Implementar un sistema que permita gestionar vulnerabilidades.
- **Diseño:** Enfoque de la tecnología empresarial y controles de seguridad.
- **Distribución:** Descubrir el estado de los sistemas informáticos característicos de cada organización.
- **Norma:** Conjunto de reglas, directrices o estándares para garantizar la seguridad de los sistemas informáticos.
- **Orden:** Asignación de prioridades y la jerarquización de medidas de seguridad.
- **Organización:** Estructura, planificación y gestión de los elementos y procesos relacionados con la seguridad de la información dentro de una entidad.
- **Ajuste:** Ajustar la configuración de sistemas y aplicaciones para asegurarse de que estén alineados con las mejores prácticas de seguridad y para mitigar posibles vulnerabilidades.
- **Régimen:** Son las prácticas y procedimientos establecidos para garantizar la seguridad de la información en una organización.
- **CIS Benchmarks** son un conjunto de recomendaciones y mejores prácticas de configuración de seguridad desarrolladas por el Center for Internet Security (CIS)

ABSTRACT

This study focuses on the technological evolution and the increasing complexity of cyberattacks, highlighting the importance of security configurations in critical servers. Despite the use of tools like antivirus and firewalls, deficiencies in these configurations can leave critical vulnerabilities unprotected.

The goal is to provide a detailed approach to improving security in organizations by identifying key configurations and offering swift and reliable fixes. The importance of applying proper security policies is emphasized, particularly in the face of targeted attacks that could exploit weaknesses in server fortification.

The development of software that simplifies the implementation of security fixes, based on best regulatory practices such as the CIS Benchmarks (Internet, 2024), is suggested. However, it is emphasized that this software does not constitute a complete solution on its own, but rather should be combined with other security technologies to ensure full protection against cyberattacks.

Keywords.

- **Correction:** Ensuring changes applied to servers.
- **Reconstruction:** Implementation of new security metrics.
- **Repair:** Managing current systems and establishing new policies.
- **Amend:** Identifying elements that affect the infrastructure.
- **Protect:** Maintaining the integrity of the services provided.
- **Structure:** Consolidation of information collected from computer systems.
- **Model:** Creating architectures that establish the security posture.
- **Develop:** Implementing a system that allows managing vulnerabilities.
- **Design:** Focusing on business technology and security controls.
- **Distribution:** Discovering the state of the computer systems characteristic of each organization.
- **Standard:** A set of rules, guidelines, or standards to ensure the security of computer systems.
- **Order:** Prioritizing and ranking security measures.
- **Organization:** Structure, planning, and management of elements and processes related to information security within an entity.
- **Adjustment:** Fine-tuning the configuration of systems and applications to ensure they align with security best practices and to mitigate potential vulnerabilities.
- **Regimen:** Practices and procedures established to ensure information security within an organization.
- **CIS Benchmarks:** A set of recommendations and best practices for security configuration developed by the Center for Internet Security (CIS).

INTRODUCCIÓN

A lo largo del tiempo la tecnología ha ido evolucionando en gran escala, así mismo los ataques cibernéticos se han vuelto cada vez más complejos y sofisticados lo que lleva a que sean más difíciles de detectar o prevenir, sin embargo, a pesar de que existen diferentes niveles de protección como antivirus, firewall y algunas otras tecnologías difícilmente se presta atención a las propias configuraciones de los servidores que abren las brechas de seguridad dejando expuestos aspectos importantes de protección.

Aunque en muchas ocasiones se llega a ser conscientes de la existencia y/o deficiencia de algunas configuraciones en servidores no se le da importancia de aplicar correctamente políticas de seguridad que brinden una mayor protección a nuestra infraestructura de servidores que pueden ser críticos para una organización.

El desconocimiento de cómo deben ser aplicadas las políticas de seguridad o configuraciones también llega a ser muy importante al enfrentarse a ataques cibernéticos dirigidos los cuales podrían aprovecharse de la falta de robustecimiento (hardening) que incluso el tiempo de aplicación correcciones es prolongado y es posible que no se le dé atención adecuada.

El objetivo de este trabajo de investigación es aportar a las organizaciones un enfoque certero de cuál es la postura de seguridad, cuáles son las configuraciones que se deberían establecer y/o mejorar y de la misma manera aplicar las correcciones necesarias de forma rápida, confiable y automática.

Este trabajo de investigación está enfocado al personal de ciberseguridad y contribuirá optimizar los tiempos de implementación de correcciones de seguridad con el uso de un software que les aporte visibilidad y una mejor manera con base a las mejores prácticas otorgadas por la regulación CIS Benchmarks.

Sin embargo, el desarrollo de este software y la corrección de configuraciones no blinda los servidores por completo, sino que trabajando en conjunto con las demás

tecnologías que componen la infraestructura de seguridad de las organizaciones puedan dar un mejor nivel de prevención de ataques cibernéticos dirigidos.

Al finalizar este trabajo de investigación y desarrollo dará al mundo en general un nuevo enfoque en correcciones de seguridad en el que puedan notar que el hecho de tener las mejores tecnologías o aplicar simples actualizaciones de sistema operativo, actualizaciones de aplicaciones no es suficiente, sino que es una ardua labor que depende de nosotros mantener el robustecimiento adecuado en los servidores.

CAPÍTULO 1. MARCO CONTEXTUAL

1.1 Planteamiento del problema.

Los sistemas informáticos representan una parte muy importante en el entorno, laboral, personal y global, la necesidad de proteger la infraestructura crítica o de uso cotidiano se ha vuelto más importante que nunca a medida que las amenazas cibernéticas evolucionan y obliga a la industria a enfrentarse a diversos tipos de ataques como malware, phishing, spam, SQL inyección, DDoS, etc.

En la tesis de Juan Merlos García (Merlos, 2021). “Bastionado de servidores”, destaca que las entidades cada vez toman más en cuenta la correcta configuración de los de la infraestructura provocando un constante monitoreo del estado de seguridad de servidores, equipos cliente, servicios o aplicaciones.

Este trabajo de investigación va enfocado a los profesionales en seguridad informática o ciberseguridad que pretenden robustecer las configuraciones de la infraestructura crítica con el fin de aportar a las organizaciones forma más eficiente de lograr ese objetivo.

El principal problema yace en la complejidad de aplicar las correcciones de seguridad necesarias por lo que a pesar de las medidas de seguridad las vulnerabilidades persisten y son explotadas causando brechas de seguridad ocasionando pérdidas de interrupciones de operaciones.

Sin embargo, existen algunos otros factores que deben ser considerados al momento de cuestionar el robustecimiento de la infraestructura:

- Se cuentan con políticas de hardening.
- Que tan complejo es implementar políticas de hardening.
- Las tareas de configuración de estas políticas conllevan mucho tiempo.
- Se cuenta con el conocimiento para saber cuándo y dónde se deben aplicar.

Tomando esto en consideración surge la premisa como se pueden aplicar las configuraciones de seguridad de manera que se optimicen los tiempos y sobre todo asegurar que se apliquen correctamente.

Por lo anterior, y puesto que el robustecimiento de la infraestructura de las organizaciones es un proceso esencial que requiere tiempo, esfuerzo y dedicación, las configuraciones de seguridad a menudo se implementan de manera ineficiente. Además, las herramientas automatizadas de hardening, como las de CIS, suelen ser muy costosas. Por ello, el presente trabajo de investigación titulado “Diseño de Aplicación Automatizada de Hardening en Servidores Críticos” tiene como propósito proporcionar un software gratuito que aplique de manera más eficiente y confiable las correcciones de seguridad, beneficiando a la comunidad en general.

2.1 Justificación.

En algunas ocasiones, las organizaciones tienden a reaccionar ante incidentes en lugar de prevenirlos en términos de protección de sistemas informáticos, ya sean críticos o de usuario final. No obstante, antes de aplicar las correcciones de seguridad y configuraciones necesarias en los servidores, es crucial considerar varios factores.

El proceso de hardening o robustecimiento de la seguridad de los servidores, especialmente los servidores críticos, requiere tiempo para su implementación y validación. Además, se necesita un conocimiento avanzado sobre el sistema operativo para aplicar las correcciones de manera adecuada.

La implementación de las correcciones de seguridad necesarias mejora significativamente la postura de seguridad frente a amenazas que se han vuelto más sofisticadas y difíciles de detectar por antivirus, filtros de correo, filtrado web e incluso firewalls. Estos ataques buscan principalmente afectar o extraer información.

Mediante esta investigación y el desarrollo de software, se pretende optimizar los tiempos de implementación de configuraciones de seguridad de manera confiable, contribuyendo al conocimiento sobre la postura de seguridad de los servidores. Sin embargo, aplicar las configuraciones no garantiza una protección completa de los servidores, ya que también depende de herramientas adicionales como antivirus y firewalls.

Asimismo, esta investigación ayudará a los ingenieros en ciberseguridad a entender mejor el sistema operativo y las configuraciones de seguridad, mejorando así el robustecimiento de los servidores.

Por lo tanto, es esencial realizar evaluaciones constantes de los servidores no solo para mejorar las configuraciones, sino también para obtener otros beneficios, como la visibilidad durante auditorías. Muchas organizaciones son auditadas y deben demostrar que aplican las mejores prácticas para mantener la protección de sus sistemas informáticos y la información, que a menudo es el objetivo de los ataques cibernéticos.

3.1 Antecedentes.

Los sistemas informáticos representan una parte fundamental en el entorno laboral, personal y global. La necesidad de proteger tanto la infraestructura crítica como la de uso cotidiano se ha vuelto más importante que nunca a medida que las amenazas cibernéticas evolucionan. La industria debe enfrentarse a diversos tipos de ataques, como malware, phishing, spam, inyecciones SQL, y DDoS, entre otros (Szor, 2005).

En este contexto, es crucial definir el alcance del proyecto, identificando los servidores y sistemas que serán objeto de verificación y determinando qué configuraciones de seguridad serán auditadas. Documentar los CIS Benchmarks es esencial para establecer los lineamientos de seguridad que se seguirán en el proyecto. Es necesario vincular estos CIS Benchmarks con el sistema operativo específico para asegurar que las configuraciones sean adecuadas y efectivas.

Seleccionar herramientas de automatización, como Python, permitirá desarrollar software que integre las herramientas necesarias para la verificación de seguridad. El diseño de la arquitectura del software debe facilitar la implementación de scripts y programas que realicen auditorías automáticas. Realizar pruebas para asegurar que las verificaciones y remediaciones se llevan a cabo correctamente es fundamental, así como validar que las configuraciones resultantes cumplan con los CIS Benchmarks. Finalmente, es importante implementar una evaluación final para analizar y remediar las auditorías.

En muchas ocasiones, las organizaciones tienden a reaccionar ante incidentes en lugar de prevenirlos, especialmente en términos de protección de sistemas informáticos, ya sean críticos o de usuario final. Antes de aplicar las correcciones de seguridad y configuraciones necesarias en los servidores, es crucial considerar varios factores (Erickson, 2008).

El proceso de hardening o robustecimiento de la seguridad de los servidores, especialmente los servidores críticos, requiere tiempo para su implementación y validación. Además, se necesita un conocimiento avanzado sobre el sistema operativo para aplicar las correcciones de manera adecuada.

4.1 Objetivo general.

Automatización mediante el diseño de un software para verificar la corrección de las configuraciones de seguridad en servidores críticos, siguiendo la regulación establecida por CIS Benchmarks.

5.1 Objetivos específicos.

- Definir el alcance en base a la determinación de los servidores y sistemas que serán objeto de la verificación, así como identificar qué configuraciones de seguridad serán auditadas.
- Documentar CIS Benchmarks con el objetivo de indicar los lineamientos que nos interesan para el proyecto.

- Vincular CIS Benchmarks con el sistema operativo específico.
- Seleccionar Herramientas de Automatización, Python.
- Desarrollar el Software, realizando el diseño de arquitectura del software que pueda integrar las herramientas seleccionadas para la verificación, implementar scripts y programas que utilicen las herramientas para realizar auditorías automáticas.
- Realizar pruebas donde se asegure que las verificaciones y remediaciones se realizan correctamente, así como validar que las configuraciones resultantes cumplan con los CIS Benchmarks.
- Implementar para la evaluación final aplicada al análisis y remediación de auditorías.

6.1 Metas.

Con base en el proyecto enfocado en mejorar la seguridad de las configuraciones en servidores críticos y en la creación de un software que implemente correcciones basadas en mejores prácticas, las metas medibles y alcanzables incluyen:

Reducción de correcciones de seguridad: Disminuir el número de correcciones de seguridad críticas en un 70%, se aplicarán las mejores prácticas de seguridad y las correcciones sugeridas por la aplicación automatizada de Hardening en servidores críticos, de acuerdo a los parámetros que cumplan o no cumplan los servidores evaluados.

Mejora en la evaluación de seguridad: Implementar y ejecutar evaluaciones de hardening en el 100% de los servidores críticos de la organización dentro de los primeros tres meses del proyecto, generando informes detallados sobre el estado de la seguridad y las recomendaciones de mejora.

Tiempos de corrección: Reducir el tiempo promedio de identificación y corrección de configuraciones de seguridad deficientes en un 50% comparado con el proceso

manual, utilizando la aplicación automatizada de Hardening en servidores críticos para aplicar correcciones basadas en los CIS Benchmarks.

Conformidad con Normativas: Alcanzar un cumplimiento del 90% con las normativas de seguridad aplicables (por ejemplo, CIS Benchmarks) en todos los servidores críticos dentro de los primeros seis meses de la implementación del software, asegurando que las configuraciones estén alineadas con los estándares regulativos.

7.1 Impacto en el sector productivo y generación de conocimiento.

El impacto de crear un software que permita realizar evaluaciones de hardening y aplicar las correcciones sería significativo en varios aspectos clave de la seguridad y la operatividad de las organizaciones. Este tipo de software mejoraría la seguridad al reducir las vulnerabilidades y la superficie de ataque, disminuyendo así la probabilidad de explotación de fallos conocidos. Además, facilitaría el cumplimiento de normativas y estándares de seguridad, lo cual es crucial para industrias reguladas (ALBAN, 2020).

En términos de eficiencia operativa, un software de este tipo automatizaría tareas repetitivas, liberando tiempo de los equipos de seguridad para centrarse en tareas más estratégicas. La consistencia y precisión serían garantizadas, minimizando errores humanos y asegurando que todas las configuraciones sigan las mejores prácticas. Esto también contribuiría a una gestión centralizada, permitiendo la aplicación coordinada y controlada de cambios a gran escala (Iza Sanhueza, 2020).

El software proporcionaría una mejor visibilidad y control, permitiendo el monitoreo continuo de las configuraciones de seguridad y proporcionando alertas y reportes sobre cambios no autorizados o desviaciones. Además, ofrecería una plataforma centralizada para gestionar políticas de seguridad, facilitando la implementación y

mantenimiento de una postura de seguridad robusta y coherente a lo largo de toda la infraestructura.

Por último, la creación de este software contribuiría a la reducción de costos al prevenir incidentes de seguridad que pueden ser costosos en términos de respuesta, recuperación y posibles sanciones. La automatización de las evaluaciones y correcciones optimizaría el uso de recursos humanos y tecnológicos, mientras que la mejora de la resiliencia permitiría a las organizaciones adaptarse rápidamente a nuevas amenazas, asegurando así una robustez y resistencia operacional frente a ataques y fallos (Merlos, 2021) (Schneier, 2015).

8.1 Reconocimiento del proyecto.

Se realizaron encuestas dirigidas a personal estratégico con experiencia en ciberataques y correlación de incidentes, con el objetivo de recopilar información cualitativa y cuantitativa sobre la percepción de la necesidad y efectividad de la herramienta propuesta.

Datos generales:

Nombre:	
Puesto:	
Empresa:	
Años de experiencia en ciberseguridad:	

1. ¿Considera importante contar con una herramienta que evalúe y aplique automáticamente las configuraciones de hardening de Windows Server en su organización?

- ☐ Muy importante
- ☐ Importante
- ☐ Moderadamente importante
- ☐ Poco importante
- ☐ No es importante

2. ¿Actualmente, realiza auditorías de las configuraciones de hardening de sus Windows Server?

- ☐ Sí, de manera regular
- ☐ Sí, pero no de manera regular
- ☐ No, pero está planeado
- ☐ No, y no está planeado

Ilustración 1 Ejemplo de encuesta 1.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS XVI

3. ¿Está familiarizado con los estándares de seguridad de CIS Benchmarks aplicables a Windows Server?

- ☐ Sí, completamente
- ☐ Algo familiarizado
- ☐ Poco familiarizado
- ☐ No estoy familiarizado

4. ¿Cuáles considera que son los principales desafíos para asegurar las configuraciones de hardening de sus Windows Server? (Seleccione las que apliquen)

- ☐ Falta de herramientas especializadas para Windows Server
- ☐ Falta de conocimientos técnicos en el equipo
- ☐ Complejidad en la implementación de estándares de seguridad en Windows Server
- ☐ Falta de regulaciones internas claras para servidores Windows Server

Ilustración 2 Ejemplo de encuesta 2.

5. ¿Su organización actualmente utiliza algún software que permita evaluar y aplicar automáticamente las configuraciones de seguridad en Windows Server?

- ☐ Sí
- ☐ No

6. ¿Considera que una herramienta basada en login que valide y aplique automáticamente las configuraciones de hardening de Windows Server con base en CIS Benchmarks sería útil para su organización?

- ☐ Sí, sería muy útil
- ☐ Sí, sería útil
- ☐ No estoy seguro
- ☐ No, no sería útil

7. ¿Cuáles serían las características más importantes para usted en una herramienta de este tipo? (Seleccione las más relevantes)

- ☐ Fácil integración con los sistemas Windows Server actuales
- ☐ Aplicación automática de configuraciones de seguridad basadas en CIS Benchmarks
- ☐ Reportes detallados sobre configuraciones de seguridad en Windows Server
- ☐ Alertas en tiempo real sobre vulnerabilidades en Windows Server
- ☐ Recomendaciones automáticas de mejoras basadas en CIS Benchmarks para Windows Server
- ☐ Actualizaciones automáticas de las regulaciones de CIS Benchmarks aplicables a Windows Server
- ☐ Otros: _____

Ilustración 3 Ejemplo de encuesta 3.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS XVII

8. ¿Qué tipo de Windows Server considera prioritario auditar y ajustar automáticamente con esta herramienta? (Seleccione los que apliquen)

- ☐ Servidores de bases de datos en Windows Server
- ☐ Servidores web en Windows Server
- ☐ Servidores de aplicaciones en Windows Server
- ☐ Servidores de correo electrónico en Windows Server
- ☐ Otros: _____

9. ¿Qué frecuencia considera adecuada para evaluar y aplicar automáticamente las configuraciones de seguridad de sus Windows Server?

- ☐ Semanalmente
- ☐ Mensualmente
- ☐ Trimestralmente
- ☐ Solo en auditorías anuales
- ☐ Otro: _____

10. ¿Cuál es su principal expectativa al utilizar una herramienta que permita evaluar y aplicar automáticamente configuraciones de Windows Server con base en CIS Benchmarks?

- ☐ Mejorar la seguridad general de la organización en entornos Windows Server
- ☐ Cumplir con normativas y regulaciones de seguridad aplicables a Windows Server
- ☐ Reducir el riesgo de ciberataques en Windows Server
- ☐ Optimizar la gestión de vulnerabilidades en Windows Server
- ☐ Otros: _____

Ilustración 4 Ejemplo de encuesta 4.

11. ¿Le gustaría recibir más información sobre herramientas que implementen evaluaciones y correcciones automáticas basadas en CIS Benchmarks para Windows Server?

- ☐ Sí
- ☐ No

12. ¿Considera que el uso de una herramienta de evaluación y corrección automática de Windows Server podría mejorar su cumplimiento regulatorio y normativo?

- ☐ Sí, significativamente
- ☐ Sí, en cierta medida
- ☐ No estoy seguro
- ☐ No

Ilustración 5 Ejemplo de encuesta 5.

Análisis de Resultados.

El análisis de los datos obtenidos del cuestionario revela varios patrones importantes en cuanto a la familiaridad y el uso de herramientas de evaluación de seguridad basadas en CIS Benchmarks. A continuación, se destacan los puntos clave:

- **Familiaridad con herramientas de evaluación automatizada:** La gran mayoría de los encuestados (80%) considera que una herramienta que evalúe y aplique configuraciones de seguridad automáticamente es "muy importante", lo que subraya la creciente necesidad de soluciones automatizadas en entornos críticos de servidores. Sin embargo, este alto nivel de interés contrasta con la familiaridad general con los estándares CIS, donde solo el 60% se siente completamente familiarizado.
- **Auditorías y uso de herramientas:** Aunque el 45% de los participantes realiza auditorías regulares de hardening en sus servidores Windows, un 35% admite no hacerlo con regularidad, lo que sugiere la existencia de brechas operativas. Además, solo el 40% de las organizaciones utiliza actualmente software automatizado para evaluar y aplicar configuraciones de seguridad, lo que destaca una oportunidad significativa para mejorar las prácticas de seguridad mediante la adopción de herramientas especializadas.
- **Desafíos para asegurar configuraciones:** El desafío más comúnmente citado (40%) es la "falta de herramientas especializadas", seguido de la "falta de conocimientos técnicos" (30%). Esto indica que, además de las herramientas, hay una necesidad palpable de capacitación adicional para que los equipos de TI implementen y mantengan correctamente los controles de seguridad en los servidores críticos.
- **Preferencias y expectativas sobre herramientas automáticas:** La mayoría de los encuestados (85%) considera que una herramienta basada

en login que valide y aplique automáticamente las configuraciones de hardening sería útil, reflejando la importancia de la automatización en la gestión de la seguridad. Los encuestados priorizan características como la "aplicación automática de configuraciones basadas en CIS Benchmarks" (75%), lo que indica un fuerte deseo de soluciones que reduzcan la intervención manual y faciliten la implementación.

- **Frecuencia de evaluaciones y expectativas:** La mayoría de los encuestados prefiere realizar evaluaciones y ajustes de seguridad de manera mensual (50%) o trimestral (40%), lo que sugiere un enfoque preventivo en la gestión de la seguridad. En cuanto a las expectativas, el objetivo principal es "mejorar la seguridad general" (90%), seguido de "cumplir con normativas" y "reducir el riesgo de ciberataques" (ambos con 80%).
- **Cumplimiento normativo y mejora de la seguridad:** El 80% de los encuestados cree que el uso de una herramienta automatizada mejoraría significativamente el cumplimiento normativo en su organización. Este hallazgo refuerza la idea de que las organizaciones buscan cada vez más herramientas que no solo fortalezcan la seguridad, sino que también ayuden a cumplir con regulaciones de seguridad cada vez más estrictas.

Conclusión.

En general, los resultados del cuestionario evidencian una fuerte demanda por herramientas de automatización de seguridad en entornos Windows Server, con un énfasis en la generación de informes detallados y la capacidad de aplicar automáticamente las configuraciones de seguridad basadas en CIS Benchmarks. Sin embargo, también se destaca una necesidad significativa de mejorar el conocimiento técnico y las capacidades del equipo en torno a la implementación y auditoría de estos estándares de seguridad.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS XX

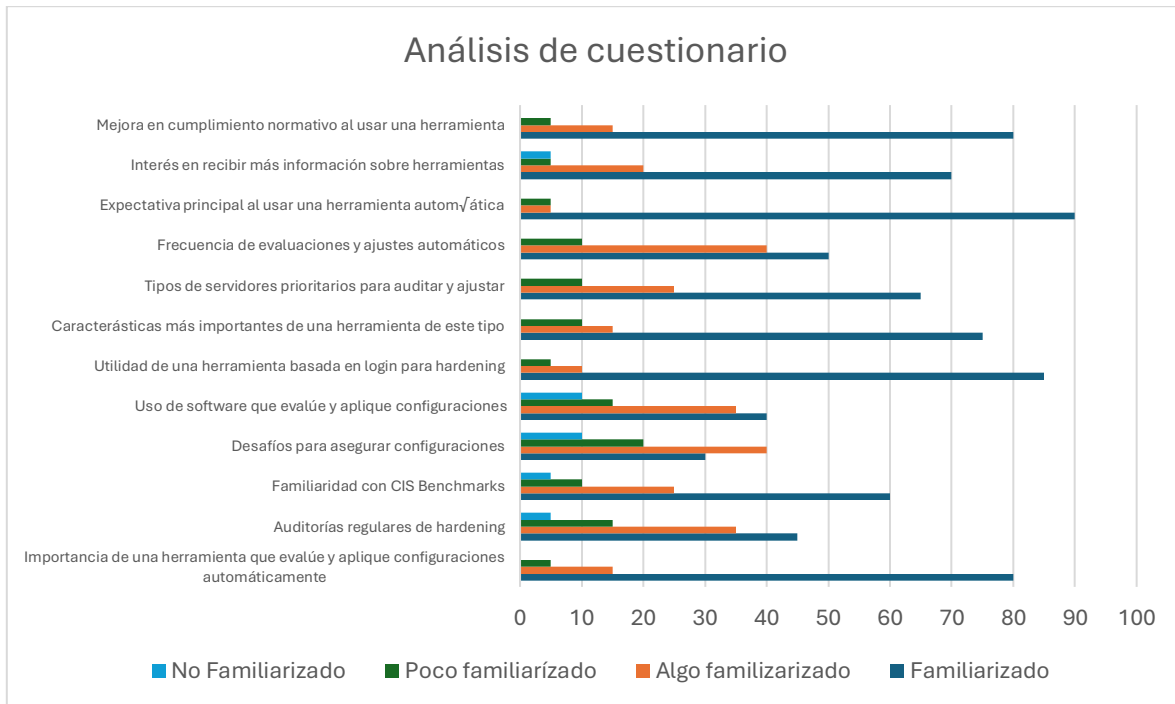


Ilustración 6 Análisis de cuestionario.

Este proyecto tiene como objetivo optimizar el proceso de **hardening** de servidores críticos, un proceso que requiere tiempo, conocimientos avanzados y evaluación continua. Las correcciones de seguridad, aunque esenciales, no son suficientes por sí solas para garantizar una protección total; deben complementarse con otras herramientas como antivirus y firewalls. Las evaluaciones regulares no solo mejoran la configuración de los servidores, sino que también facilitan auditorías y aseguran el cumplimiento de las mejores prácticas de seguridad.

Este enfoque ayuda a que los ingenieros en ciberseguridad comprendan mejor las configuraciones de seguridad del sistema operativo, lo que fortalece aún más los servidores críticos.

9.1 Vinculación con el sector productivo.

La vinculación con el sector productivo es un componente esencial para el éxito del desarrollo de un software que permita la evaluación y corrección de hardening de acuerdo con las regulaciones CIS. Esta colaboración directa con las empresas del sector permite comprender las problemáticas específicas que enfrentan en términos de seguridad de la configuración de servidores, facilitando el ajuste y adaptación de las funcionalidades del software para ofrecer soluciones efectivas y prácticas.

Mediante alianzas estratégicas con organizaciones del sector, el proyecto puede acceder a datos reales y casos de uso que enriquecen el proceso de desarrollo. Estas colaboraciones proporcionan un valioso feedback durante las fases de prueba y ajuste, y abren oportunidades para la implementación temprana del software en entornos operativos, permitiendo una validación práctica y directa de su eficacia y usabilidad en el contexto de las mejores prácticas regulativas como los CIS Benchmarks.

La vinculación con el sector productivo también promueve la transferencia de conocimientos y tecnología. Los expertos en ciberseguridad de las empresas colaboradoras pueden aportar su experiencia y perspectivas, ayudando a identificar áreas críticas y oportunidades de mejora en las evaluaciones y correcciones de hardening. Además, esta interacción fomenta la capacitación continua del equipo de desarrollo, alineando sus habilidades y conocimientos con las demandas actuales y futuras del mercado laboral en términos de cumplimiento de estándares de seguridad.

Finalmente, esta vinculación facilita la comercialización y adopción del software, al garantizar que el producto final no solo cumpla con los estándares de calidad y seguridad, sino que también se adapte a las necesidades y expectativas del sector productivo. La colaboración activa con las empresas asegura que el software sea una herramienta relevante y útil, que pueda integrarse fácilmente en los procesos y sistemas existentes, aportando un valor tangible y significativo a las organizaciones

que lo utilicen, y mejorando así la postura de seguridad general del entorno empresarial.

CAPÍTULO 2. MARCO TEÓRICO

La gestión de la seguridad en infraestructuras de TI se fundamenta en varios conceptos clave que se interrelacionan para garantizar la integridad, disponibilidad y confidencialidad de los sistemas informáticos. La corrección asegura que los cambios aplicados a los servidores sean efectivos y no introduzcan nuevas vulnerabilidades. Esto implica la revisión y validación continua de actualizaciones y parches (Stallings, 2016). La reconstrucción se refiere a la implementación de nuevas métricas de seguridad que permiten una evaluación continua del estado de seguridad, adoptando nuevos estándares y tecnologías para mejorar la postura de seguridad (Anderson, 2020).

La reparación implica gestionar los sistemas y políticas actuales, asegurando su correcto funcionamiento y actualizándolos cuando sea necesario. Esto incluye la identificación y mitigación de vulnerabilidades existentes (Charles P. Pfleeger, 2003). Enmendar se enfoca en determinar los elementos que afectan negativamente la infraestructura de TI, revisando configuraciones, políticas y prácticas para identificar áreas de mejora (Schneier, 2015). Por otro lado, proteger es esencial para mantener la integridad y disponibilidad de los servicios ofrecidos, implementando controles de seguridad como firewalls, sistemas de detección de intrusos y medidas de cifrado (Dafydd Stuttard, 2011).

En cuanto a la estructura, se refiere a la consolidación de la información recopilada de los sistemas informáticos, facilitando su análisis y gestión. Esto abarca la organización de datos de logs, eventos de seguridad y configuraciones del sistema (Szor, 2005). Modelar implica la generación de arquitecturas de seguridad que permitan establecer y mantener una postura robusta de seguridad, incluyendo el diseño y la implementación de redes seguras, segmentación de red y controles de acceso (Erickson, 2008). Desarrollar un sistema para gestionar vulnerabilidades es crucial, permitiendo la identificación, evaluación y mitigación de vulnerabilidades de manera eficiente (Schneier, 2015). El diseño se refiere al enfoque integral en la tecnología empresarial y los controles de seguridad, planificando la infraestructura y las medidas de seguridad desde el inicio (Stallings, 2016).

La distribución implica descubrir y evaluar el estado de los sistemas informáticos dentro de una organización, identificando áreas que requieren atención y mejora (Anderson, 2020). Las normas son conjuntos de reglas, directrices o estándares diseñados para garantizar la seguridad de los sistemas informáticos (Charles P. Pfleeger, 2003). El orden se refiere a la asignación de prioridades y la jerarquización de medidas de seguridad, estableciendo qué aspectos deben abordarse primero en función de su impacto potencial (Schneier, 2015). La organización implica la estructura, planificación y gestión de todos los elementos y procesos relacionados con la seguridad de la información, asegurando una respuesta coordinada y efectiva ante incidentes de seguridad (Anderson, 2020).

El ajuste implica modificar la configuración de sistemas y aplicaciones para alinearse con las mejores prácticas de seguridad y mitigar posibles vulnerabilidades, como la actualización de configuraciones de software y hardware (Stallings, 2016). Finalmente, el régimen comprende las prácticas y procedimientos establecidos para garantizar la seguridad de la información, que deben ser consistentes y revisados regularmente para mantener su efectividad (Charles P. Pfleeger, 2003). Estos conceptos y prácticas son esenciales para proteger los sistemas y datos de las organizaciones contra amenazas y vulnerabilidades, asegurando así un entorno seguro y confiable (Dafydd Stuttard, 2011).

El diseño de software debe considerar desde el inicio la integración de medidas de seguridad, implementando principios de diseño seguro y controles de acceso adecuados (Schneier, 2015). Esto asegura que la seguridad esté incorporada en cada etapa del desarrollo. La automatización de procesos puede mejorar la eficiencia y reducir errores humanos, pero también puede introducir nuevas vulnerabilidades si no se gestionan adecuadamente. Un ejemplo es la implementación de scripts automatizados para la gestión de parches y actualizaciones, que, aunque eficiente, requiere una supervisión constante para evitar riesgos (Anderson, 2020).

Comparar las configuraciones de seguridad actuales de los servidores críticos con las mejores prácticas recomendadas por CIS Benchmarks puede identificar áreas de mejora. Esto asegura que los servidores estén configurados de manera robusta y actualizada, reduciendo así el riesgo de vulnerabilidades (Stallings, 2016). Utilizar CIS Benchmarks para evaluar y mejorar las configuraciones de seguridad asegura que los servidores y sistemas estén alineados con los estándares de la industria, reduciendo el riesgo de vulnerabilidades y garantizando una postura de seguridad más sólida (Charles P. Pfleeger, 2003).

10.1 Diseño.

Este sistema ha sido meticulosamente diseñado para gestionar de manera integral los procesos de evaluación de seguridad bajo los estrictos estándares de los CIS Benchmarks, proporcionando al usuario, quien asume también el rol de administrador, una herramienta poderosa y flexible para el control y la mejora continua de la postura de seguridad de la organización. En su núcleo, el sistema se fundamenta en un flujo que inicia con la autenticación segura, garantizando que solo usuarios autorizados accedan a las funcionalidades críticas. Desde este punto, el usuario puede seleccionar un sistema o servicio que será evaluado exhaustivamente según los controles CIS, con resultados que reflejan si la infraestructura ha superado los estándares, fallado en ciertos aspectos, o si algunos controles no son aplicables.

El sistema no solo identifica estos fallos, sino que también sugiere correcciones automáticas, optimizando el tiempo y los esfuerzos del administrador. Además, tras la implementación de dichas correcciones, el sistema facilita una segunda evaluación para validar la resolución efectiva de los problemas detectados. Esta capacidad de reevaluar los sistemas asegura que las soluciones aplicadas han cumplido con su propósito, garantizando una mayor seguridad en el entorno evaluado.

Con el fin de mejorar la trazabilidad y el seguimiento, cada evaluación puede ser nombrada de manera personalizada, permitiendo una rápida identificación y clasificación de los reportes generados. Estas evaluaciones no solo pueden ser almacenadas, sino también impresas en reportes detallados que documentan tanto la evaluación inicial como la reevaluación posterior a las correcciones. Esto facilita la creación de registros formales y la distribución de información crítica en informes de cumplimiento.

Finalmente, la capacidad de gestionar credenciales y usuarios dentro del sistema ofrece un nivel adicional de control y seguridad, asegurando que las evaluaciones y sus resultados sean manejados dentro de un entorno administrado y regulado. Este sistema, por tanto, no solo sirve como una herramienta reactiva ante incumplimientos de seguridad, sino como un elemento proactivo que refuerza el cumplimiento normativo y mejora continuamente la seguridad operativa de la organización.

11.1 Diagrama de casos de uso.

Este sistema permite al usuario, que también actúa como administrador, llevar a cabo un flujo completo de evaluación de seguridad basado en los CIS Benchmarks. El proceso comienza con el inicio de sesión seguro, seguido de la selección de un sistema o servicio para evaluar. El sistema ejecuta la evaluación, mostrando los resultados que pueden ser "Pasó", "Falló" o "No Aplica". Si hay fallos, el usuario puede aplicar las correcciones sugeridas por el sistema y ejecutar una segunda evaluación para verificar la resolución de los problemas. Además, el usuario puede asignar un nombre a cada evaluación para facilitar su identificación y generar un reporte imprimible que incluya todos los detalles de las evaluaciones realizadas. Por último, el sistema también permite la gestión de credenciales, brindando una solución integral para el control y la mejora continua de la seguridad.

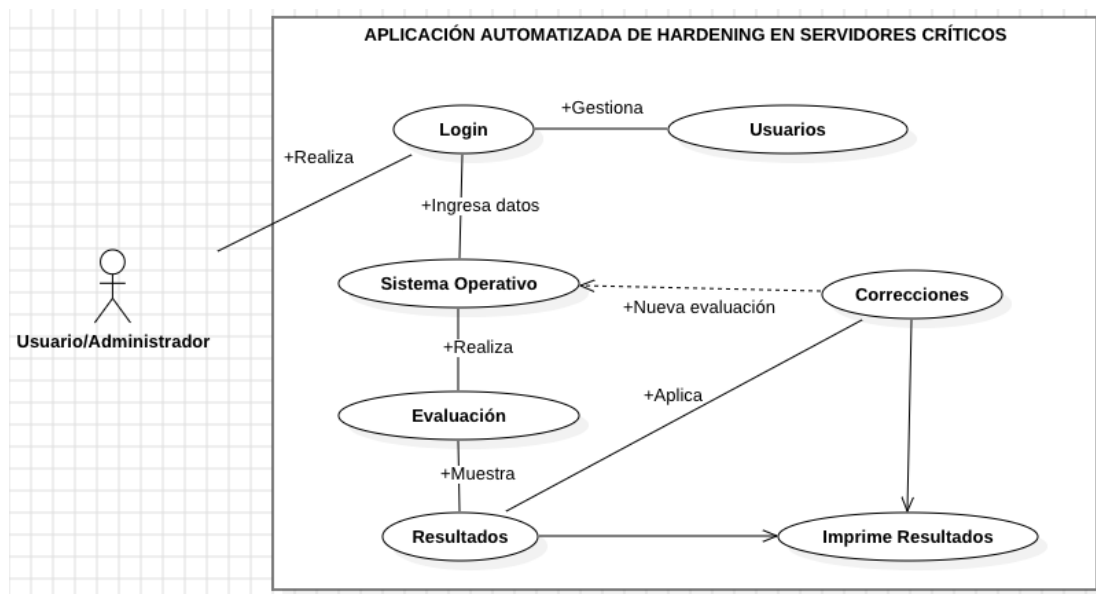


Ilustración 7 Diagrama de casos de uso.

- **Login del Usuario/Administrador:**
 - El usuario inicia sesión en el sistema proporcionando credenciales válidas.
- **Enviar Evaluación de Seguridad:**
 - El usuario selecciona un sistema o servicio a evaluar.
 - El software ejecuta la evaluación basada en los CIS Benchmarks.
 - El sistema muestra el resultado de la evaluación (Pasó, Falló o No Aplica).
- **Revisión de Resultados:**
 - El usuario revisa los resultados de las evaluaciones.
- **Aplicar Correcciones:**
 - El usuario selecciona las correcciones que deben aplicarse basadas en los controles que fallaron.
 - El sistema sugiere las correcciones disponibles y permite al usuario aplicarlas.
- **Segunda Evaluación:**
 - Después de aplicar las correcciones, el usuario vuelve a ejecutar la evaluación.
 - El software realiza una nueva evaluación basada en los CIS Benchmarks para validar si los problemas fueron corregidos.
 - El sistema muestra el resultado de esta segunda evaluación.

- **Asignar Nombre a la Evaluación:**
 - El usuario puede asignar un nombre específico a cada evaluación realizada, para su posterior identificación y seguimiento.
- **Imprimir Evaluación:**
 - El usuario tiene la capacidad de imprimir o generar un reporte de la evaluación, incluyendo el nombre asignado y los resultados (tanto de la evaluación inicial como de la segunda evaluación, si aplica).
- **Gestión de Usuarios:**
 - Si es necesario, el usuario puede gestionar sus propias credenciales o las de otros si hay más personas involucradas.

12.1 Diagrama de clases.

Este sistema de evaluación de seguridad se basa en la interacción entre varias clases que representan los roles y procesos críticos involucrados. La clase **Usuario/Administrador** permite a un usuario con credenciales autenticadas iniciar sesión, gestionar sus credenciales y seleccionar los sistemas a evaluar. Cada **SistemaEvaluación** contiene información esencial sobre el servidor a evaluar, incluyendo su IP, credenciales de acceso, y el resultado de la evaluación. Los métodos dentro de esta clase permiten ejecutar la evaluación, mostrar los resultados y sugerir las correcciones necesarias.

La clase **Evaluación** almacena detalles de cada evaluación, como su ID, nombre, fecha, y los resultados de las evaluaciones iniciales y posteriores a las correcciones. Permite asignar nombres a las evaluaciones y generar reportes imprimibles. Por otro lado, la clase **Corrección** gestiona las posibles correcciones que pueden ser aplicadas a los sistemas evaluados. Cada corrección tiene un identificador único, una descripción detallada y un estado que indica si ha sido aplicada o no. Estas clases están relacionadas jerárquicamente: un usuario/administrador puede

acceder a múltiples sistemas de evaluación, cada sistema genera una o más evaluaciones, y cada evaluación puede tener asociadas varias correcciones, proporcionando un flujo robusto para asegurar y optimizar la seguridad en los sistemas evaluados.

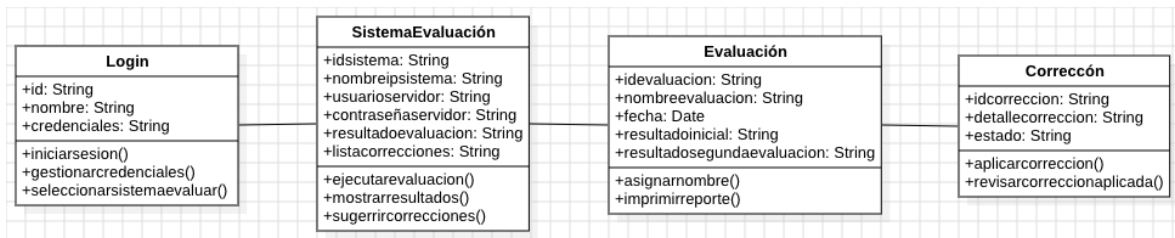


Ilustración 8 Diagrama de clases.

Login.

- **Atributos:**
 - id: str String
 - nombre: str String
 - credenciales: String
- **Métodos:**
 - iniciarsesion()
 - gestionarcredenciales()
 - seleccionarsistemaevaluar()

SistemaEvaluación.

- **Atributos:**
 - idsistema: String
 - nombreipsistema: String
 - usuarioservidor: String
 - contraseñaservidor: String
 - resultadoevaluación: String
 - listacorrecciones: String

- **Métodos:**
 - ejecutar Evaluación()
 - mostrar resultado()
 - sugerir correcciones()

Evaluación.

- **Atributos:**
 - id Evaluación: String
 - nombre Evaluación: String
 - fecha: Date
 - resultado inicial: String
 - resultado segunda Evaluación: String
- **Métodos:**
 - asignar nombre()
 - imprimir reporte()

Corrección.

- **Atributos:**
 - id corrección: String
 - detalle corrección: String
 - estado: String
- **Métodos:**
 - aplicar corrección()
 - revisar corrección Aplicada()

Relaciones.

- **Usuario/Administrador** tiene acceso a uno o más **SistemaEvaluación**.
- **SistemaEvaluación** genera uno o más **Evaluación**.
- **Evaluación** puede tener una o más **Correcciones** asociadas.

13.1 Diagrama de secuencia.

El diagrama de secuencia ilustra el flujo de interacción entre los actores y componentes del sistema en el proceso de evaluación de seguridad basado en los CIS Benchmarks. Muestra cada paso desde que el usuario o administrador se autentica en el sistema, selecciona un servicio para evaluar, y recibe los resultados, hasta la generación del reporte final. Este diagrama ayuda a comprender el orden de las acciones y cómo el sistema responde en cada etapa, destacando la interacción del usuario con el sistema y el flujo de control para la aplicación de correcciones.

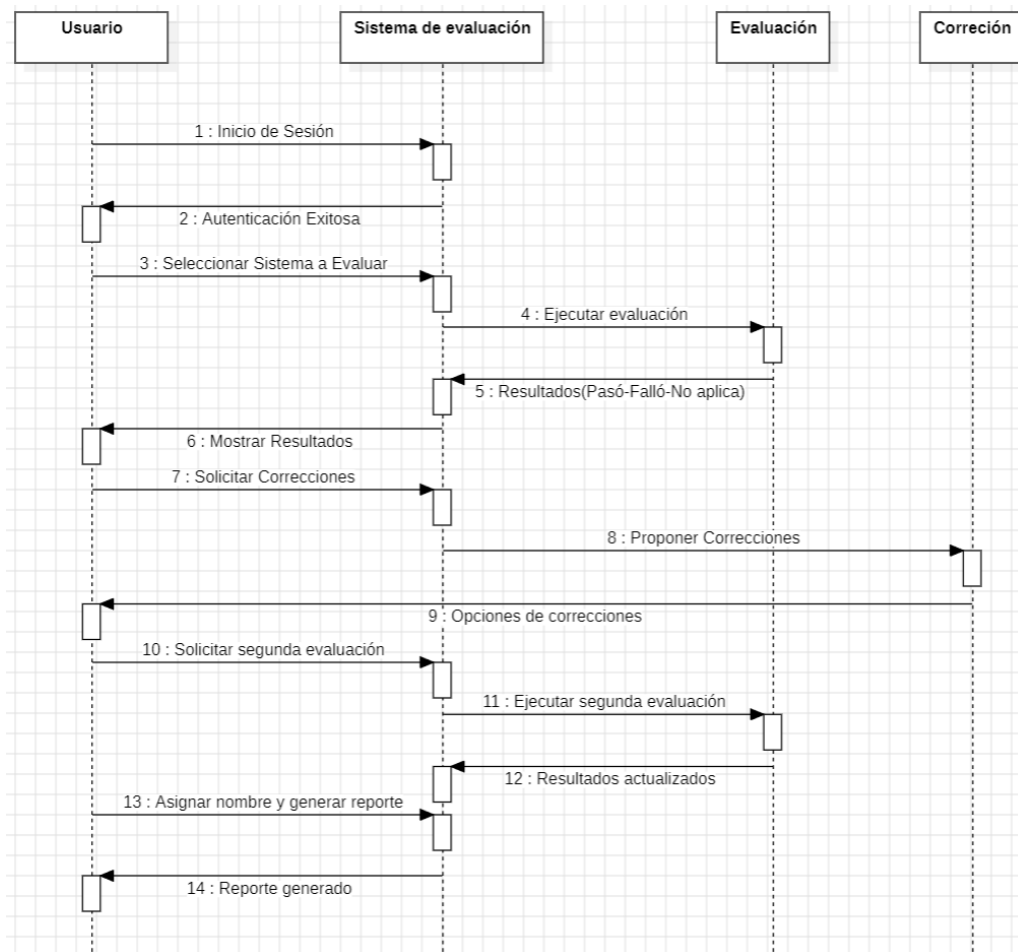


Ilustración 9 Diagrama de secuencia.

Actores involucrados:

- Usuario/Administrador
- Sistema de Evaluación (backend del sistema)
- Evaluación
- Corrección

Pasos de la secuencia:

- **Inicio de sesión:** El usuario ingresa credenciales para autenticarse.
- **Seleccionar Sistema para Evaluar:** El usuario selecciona un sistema o servicio que desea evaluar.
- **Ejecutar Evaluación:** El sistema realiza la evaluación y proporciona los resultados.
- **Mostrar Resultados:** El sistema muestra los resultados ("Pasó", "Falló", "No Aplica").
- **Aplicar Correcciones:** Si el resultado es "Falló", el sistema sugiere correcciones, y el usuario decide cuáles aplicar.
- **Segunda Evaluación:** El usuario solicita una segunda evaluación para verificar las correcciones.
- **Asignar Nombre y Generar Reporte:** El usuario asigna un nombre a la evaluación y puede generar e imprimir un reporte con los resultados.

14.1 Diagrama de estados.

El diagrama de estados describe las diferentes etapas por las que pasa el sistema de evaluación de seguridad desde que el usuario inicia sesión hasta la generación del reporte. Cada estado representa una fase clave del flujo, como "Autenticado", "Evaluación en Progreso", o "Aplicando Correcciones". Este diagrama permite visualizar las posibles transiciones y situaciones en las que se puede encontrar el sistema, mostrando cómo responde ante diferentes acciones del usuario y el resultado de cada evaluación.

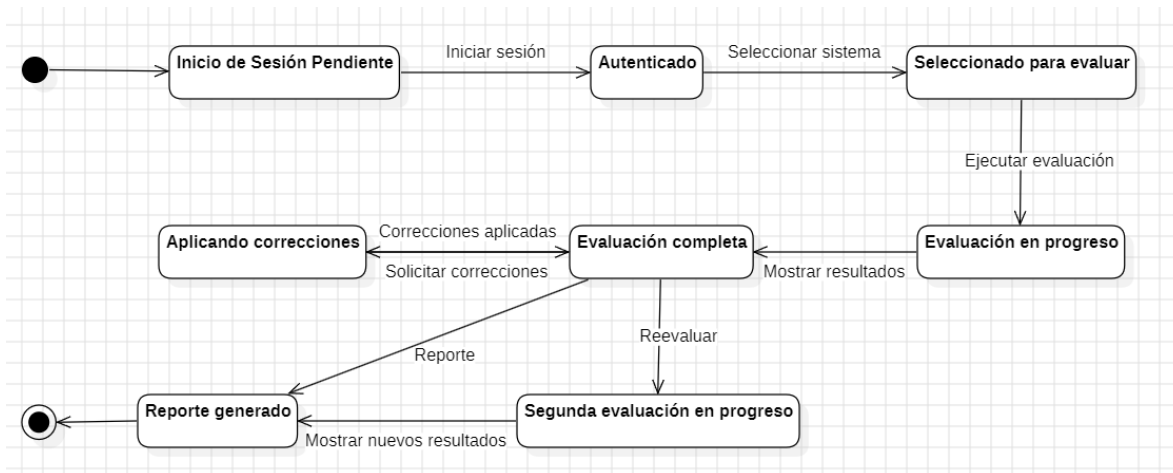


Ilustración 10 Diagrama de estados.

Estados principales:

- **Inicio de Sesión Pendiente:** Espera que el usuario ingrese credenciales.
- **Autenticado:** Usuario autenticado y listo para seleccionar un sistema.
- **Seleccionado para Evaluar:** Un sistema está listo para ser evaluado.
- **Evaluación en Progreso:** El sistema realiza la evaluación de acuerdo con los CIS Benchmarks.
- **Evaluación Completada:** La evaluación muestra el estado de cada control ("Pasó", "Falló", "No Aplica").
- **Aplicando Correcciones:** Correcciones sugeridas están siendo aplicadas.

- **Segunda Evaluación en Progreso:** Después de aplicar las correcciones, se realiza otra evaluación.
- **Reporte Generado:** Un reporte con los resultados de la evaluación está listo para impresión.

15.1 Diagrama entidad relación.

El diagrama entidad-relación define las principales entidades y sus relaciones dentro del sistema de evaluación de seguridad. Describe cómo el "Usuario/Administrador" interactúa con los "Sistemas de Evaluación", que a su vez generan una o más "Evaluaciones". Cada evaluación puede tener asociadas varias "Correcciones" aplicables a los fallos detectados. Este diagrama proporciona una vista estructural del sistema, mostrando cómo están organizados los datos y cómo se relacionan las diferentes entidades para realizar un seguimiento y control de las evaluaciones de seguridad.

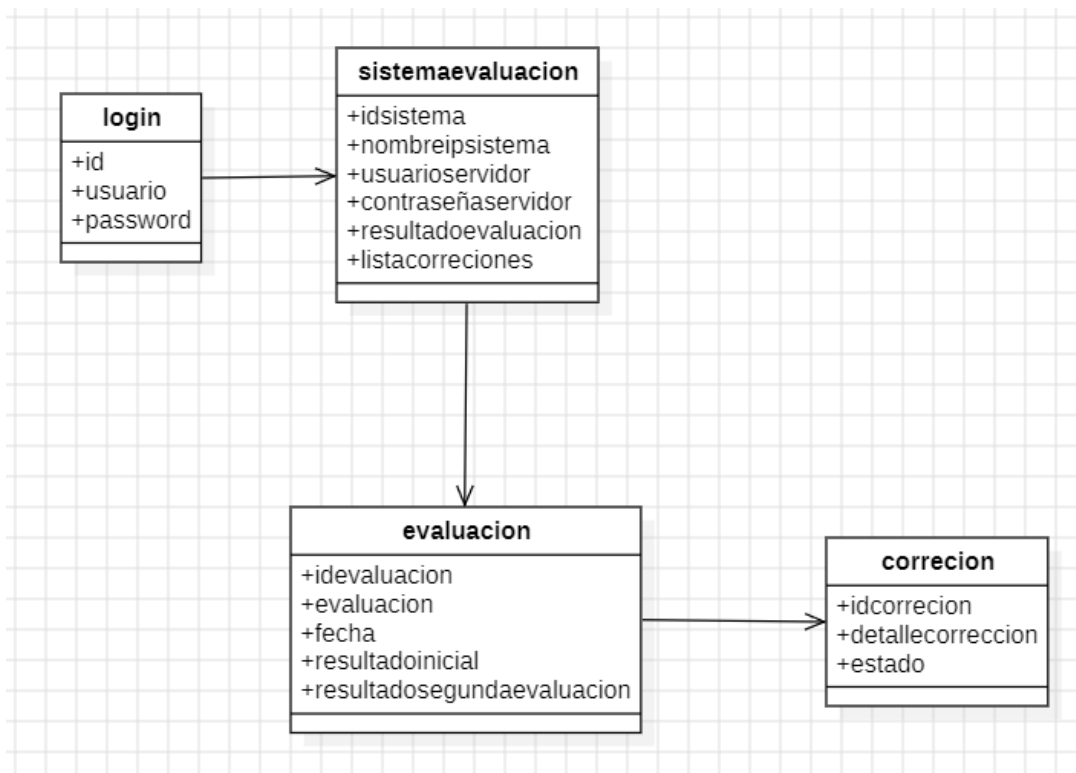


Ilustración 11 Diagrama entidad-relación.

Entidades:

- **Usuario/Administrador**
 - **Atributos:** id, usuario, password
 - **Relación:** Tiene acceso a uno o más SistemaEvaluación.
- **SistemaEvaluación**
 - **Atributos:** idsistema, nombreipsistema, usuarioservidor, contraseñaservidor, resultadoevaluación, listacorrecciones
 - **Relación:** Genera uno o más Evaluación.
- **Evaluación**
 - **Atributos:** idevaluación, nombreevaluación, fecha, resultadoinicial, resultadosegundaevaluación
 - **Relación:** Puede tener una o más Corrección asociadas.
- **Corrección**
 - **Atributos:** idcorrección, detallecorrección, estado
 - **Relación:** Está asociada con una Evaluación.

16.1 Maquetado.

El diseño del sistema de gestión de seguridad en infraestructuras de TI se centra en proporcionar una interfaz intuitiva y segura, facilitando al usuario o administrador la ejecución de evaluaciones de seguridad basadas en los estándares CIS Benchmarks. El maquetado está organizado en pantallas específicas que guían al usuario desde el inicio de sesión hasta la generación de reportes detallados, incluyendo funcionalidades clave como la selección de sistemas a evaluar, la visualización de resultados, la aplicación de correcciones, y la posibilidad de realizar una segunda evaluación para validar las mejoras. Además, cada sección del maquetado está diseñada para optimizar la experiencia y la eficiencia en la gestión de seguridad, con opciones adicionales para la administración de usuarios y credenciales, proporcionando un control continuo y completo sobre el entorno evaluado.

Inicio de Sesión:

- Campos para ingresar el nombre de usuario y la contraseña.
- Botón de "Iniciar Sesión".

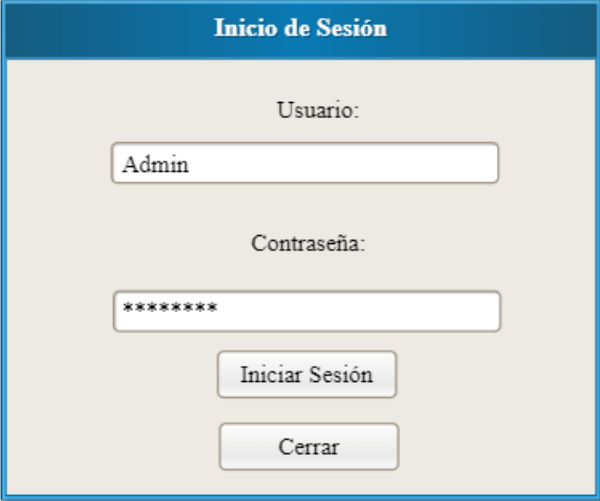


Ilustración de la interfaz de usuario para el inicio de sesión. La pantalla tiene un encabezado azul con el título "Inicio de Sesión". Debajo, hay un campo de texto para el "Usuario:" con el valor "Admin" ingresado. A continuación, hay un campo de texto para la "Contraseña:" con caracteres ocultos por asteriscos. En la parte inferior, hay dos botones: "Iniciar Sesión" y "Cerrar".

Ilustración 12 Maquetado-Inicio de sesión.

Panel de Control:

- Menú lateral con opciones como:
 - **Evaluación de Seguridad:** Inicia el proceso de selección del sistema a evaluar.
 - **Correcciones:** Visualización y aplicación de las correcciones sugeridas.
 - **Historial de Evaluaciones:** Listado de todas las evaluaciones realizadas, con filtros por fecha y nombre.
- Vista principal que muestra información resumida de las evaluaciones recientes, correcciones pendientes, y recomendaciones.

Selección de Sistema:

- Formulario para seleccionar un sistema o servicio específico para la evaluación.
- Botón de "Iniciar Evaluación" para ejecutar el proceso de acuerdo con los CIS Benchmarks.

Resultados de Evaluación:

- Vista detallada de los resultados con indicadores visuales de "Pasó", "Falló" o "No Aplica".
- Botón para "Aplicar Correcciones" en caso de resultados de fallo.
- Opción para iniciar una **Segunda Evaluación** después de aplicar las correcciones.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS XL

Conexión Remota a Servidor Windows

IP o Nombre de Host:

Usuario:

Contraseña:

Control	Valor Actual	Valor Esperado	Estatus
---------	--------------	----------------	---------

Reportes

ID	Nombre
----	--------

Ilustración 13 Maquetado - Sistema de evaluación.

Gestión de usuarios:

- **Visualización de usuarios:** Se muestra una tabla o lista para ver los usuarios registrados, con columnas como ID, Username y Password.
- **Formulario de ingreso:** A la derecha, se ven campos para ingresar datos como el nombre de usuario y contraseña.
- **Botones de acción:**
 - **Agregar Usuario:** Para registrar un nuevo usuario.
 - **Actualizar Usuario:** Para modificar los datos de un usuario existente.
 - **Eliminar Usuario:** Para eliminar un usuario del sistema.
 - **Cerrar:** Para salir de la aplicación.

The image shows a web application window titled "Administrador de Usuarios". Inside, there is a table with three columns: "ID", "Username", and "Password". The table is currently empty. To the right of the table, there are two input fields. The first is labeled "Username" and contains the text "Admin". The second is labeled "Password" and contains "*****". Below these input fields, there are four buttons arranged vertically: "Agregar Usuario", "Actualizar Usuario", "Eliminar Usuario", and "Cerrar".

Ilustración 14 Gestión de usuarios.

17.1 Tabla de requerimientos.

La tabla de requerimientos define las funcionalidades y características esenciales que debe cumplir el sistema de evaluación de seguridad en infraestructuras de TI. Estos requerimientos aseguran que el sistema no solo permite evaluar y corregir configuraciones de seguridad, sino que también proporciona herramientas de administración y gestión eficientes, facilitando el cumplimiento de estándares como los CIS Benchmarks. Cada requerimiento se clasifica según su prioridad para orientar el desarrollo y garantizar que las funciones críticas, como la autenticación, ejecución de evaluaciones y generación de reportes, sean implementadas y probadas en primer lugar. La tabla incluye tanto funcionalidades específicas del flujo de evaluación, como la aplicación de correcciones y la revalidación de resultados, como elementos de seguridad adicionales, tales como la automatización de procesos y la estandarización de normas. Esta estructura busca asegurar una solución robusta, alineada con las mejores prácticas de seguridad en TI.

ID	Requerimiento	Descripción	Prioridad
1	Autenticación de Usuario	El sistema debe permitir a los usuarios autenticarse ingresando credenciales	Alta

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES
CRÍTICOS XLII

ID	Requerimiento	Descripción	Prioridad
		válidas para iniciar sesión.	
2	Selección de Sistema a Evaluar	Permitir al usuario seleccionar un sistema o servicio que desea evaluar según los CIS Benchmarks.	Alta
3	Ejecución de Evaluación de Seguridad	Realizar la evaluación de seguridad del sistema seleccionado, mostrando los resultados en categorías "Pasó", "Falló", etc.	Alta
4	Visualización de Resultados	Mostrar los resultados detallados de la evaluación para que el usuario pueda analizar el estado de seguridad.	Alta
5	Aplicación de Correcciones	Permitir al usuario aplicar correcciones sugeridas por el sistema para mitigar los fallos identificados.	Media
6	Segunda Evaluación	Ejecutar una segunda evaluación después de aplicar las correcciones para verificar si los problemas fueron resueltos.	Media
7	Asignación de Nombre a la Evaluación	Permitir al usuario asignar un nombre específico a cada evaluación para	Media

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES
CRÍTICOS XLIII

ID	Requerimiento	Descripción	Prioridad
		facilitar su identificación y seguimiento.	
8	Generación de Reporte	Generar un reporte imprimible de la evaluación, incluyendo detalles de la primera y segunda evaluación (si aplica).	Alta
9	Gestión de Usuarios	Proveer opciones para gestionar las credenciales de acceso, asegurando la administración segura de las evaluaciones.	Alta
10	Visualización de Historial de Evaluaciones	Mostrar un historial de todas las evaluaciones realizadas con opción de filtrado por fecha y nombre de evaluación.	Media
11	Validación Continua de Actualizaciones y Parches	Verificar que los parches y actualizaciones aplicados no generen vulnerabilidades nuevas.	Alta
12	Implementación de Métricas de Seguridad	Desarrollar métricas de seguridad que permitan una evaluación continua del estado de seguridad de los sistemas.	Media
13	Gestión de Configuraciones y Políticas	Facilitar la gestión y actualización de políticas de	Media

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES
CRÍTICOS XLIV

ID	Requerimiento	Descripción	Prioridad
		seguridad para los sistemas evaluados.	
14	Comparación con Configuraciones de Seguridad Recomendadas	Comparar las configuraciones de los servidores con las recomendaciones de CIS Benchmarks para identificar áreas de mejora.	Alta

Tabla 1 Tabla de requerimientos.

CAPÍTULO 3. MARCO METODOLÓGICO

En el contexto del proyecto, la evolución tecnológica y el aumento en la complejidad de los ataques cibernéticos destacan la necesidad de fortalecer las configuraciones de seguridad en servidores críticos. A pesar de contar con herramientas como antivirus y firewalls, las deficiencias en estas configuraciones pueden dejar vulnerabilidades críticas sin protección. El objetivo de este proyecto es proporcionar un enfoque detallado para mejorar la seguridad en las organizaciones, identificando configuraciones clave y ofreciendo correcciones de manera rápida y confiable, a través de la metodología ágil Scrum.

Scrum es una metodología ágil que se adapta perfectamente a este proyecto, permitiendo iteraciones cortas y continuas mejoras basadas en retroalimentación constante. Durante las fases de desarrollo, se subrayará la importancia de aplicar políticas de seguridad adecuadas, especialmente ante ataques dirigidos que podrían explotar fallos en la fortificación de los servidores. La metodología Scrum facilita la organización y priorización de tareas, asegurando que cada sprint se enfoque en la implementación y validación de configuraciones de seguridad clave, así como en la aplicación de correcciones necesarias.

El desarrollo del software que simplifique la implementación de correcciones de seguridad, basado en las mejores prácticas regulativas como los CIS Benchmarks, se llevará a cabo en múltiples sprints. En cada sprint, se desarrollarán y probarán incrementos funcionales del software, permitiendo ajustes rápidos y eficientes en respuesta a la retroalimentación de los usuarios. No obstante, se recalca que este software no constituye una solución completa por sí solo, sino que debe combinarse con otras tecnologías de seguridad para garantizar una protección completa contra ataques cibernéticos.

Al concluir cada sprint, se espera que el proyecto aporte un nuevo enfoque en las correcciones de seguridad, enfatizando la importancia de mantener adecuadamente el robustecimiento de servidores. Más allá de simplemente depender de las últimas tecnologías o de realizar actualizaciones regulares del sistema operativo y las

aplicaciones, Scrum permitirá una adaptación ágil y continua del software, asegurando que las configuraciones de seguridad se mantengan al día y efectivas contra las amenazas cibernéticas emergentes.

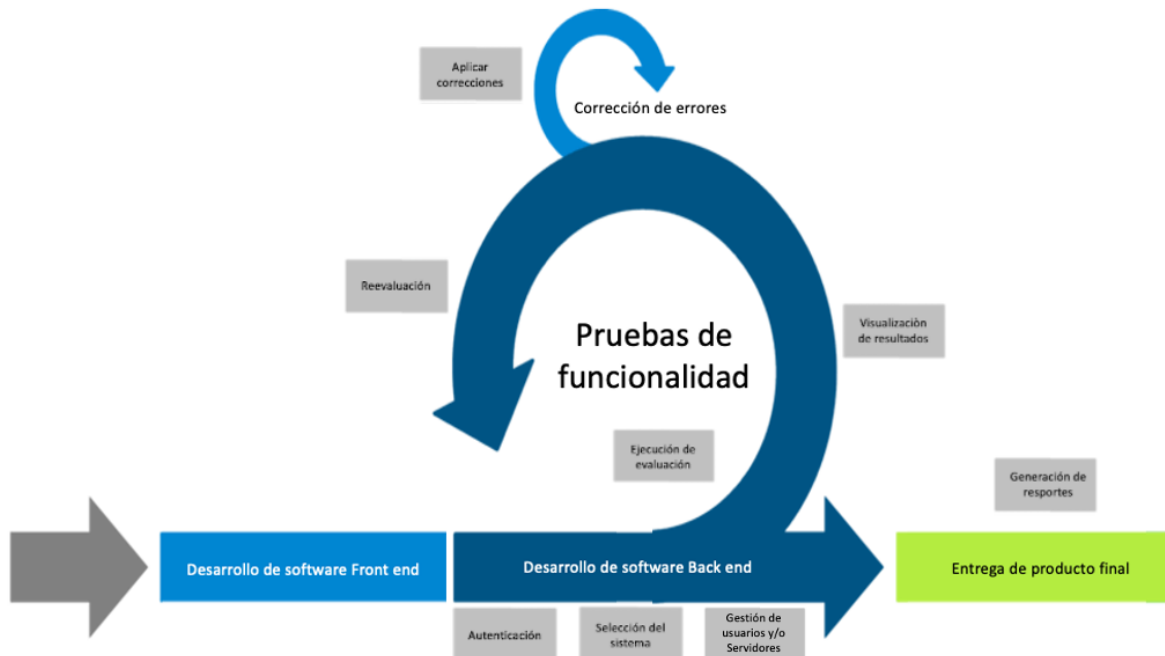


Ilustración 15 Diagrama de metodología.

18.1 Desarrollo.

Fases Del Desarrollo.

Desarrollo De Software Front-End.

En esta fase se construye la interfaz gráfica del usuario, que será el medio de interacción entre el usuario final y el sistema. Se prioriza la usabilidad, accesibilidad y claridad de los elementos visuales. El diseño incluye menús, formularios, botones e indicadores que permiten iniciar auditorías, visualizar resultados, aplicar configuraciones y generar reportes.

Login.

El acceso a la plataforma está habilitado únicamente cuando el usuario conoce la contraseña predeterminada configurada de fábrica o, en su defecto, si dicha contraseña ya ha sido modificada previamente por una personalizada.

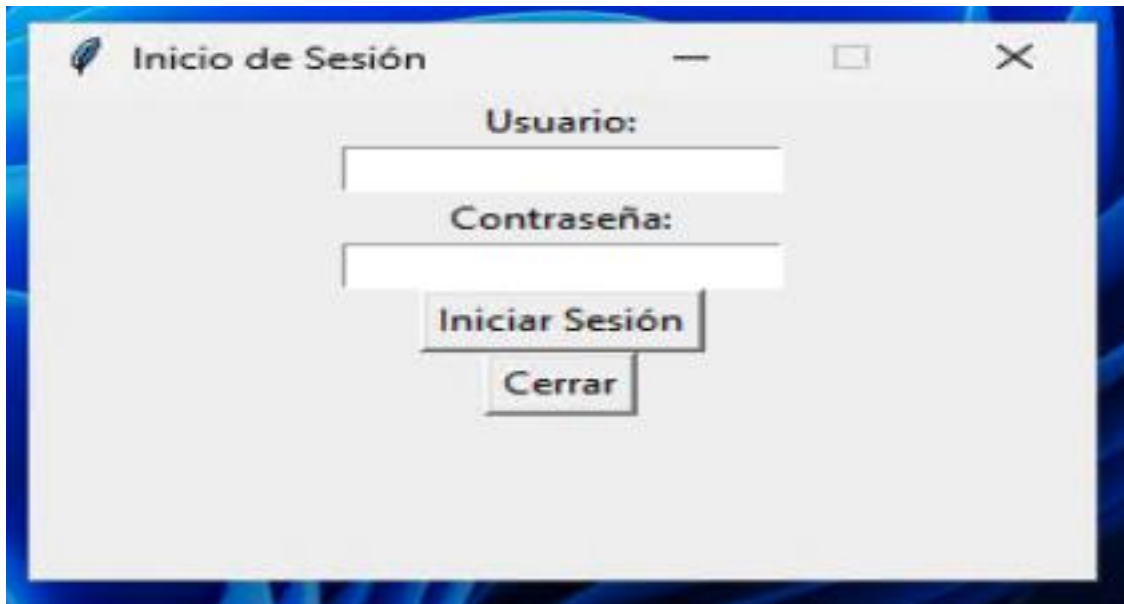


Ilustración 16 Login.

Interfaz principal.

La herramienta está diseñada para que cualquier usuario pueda seleccionar fácilmente el host que desea evaluar, especificar el sistema operativo que utiliza y definir el estándar de cumplimiento que se seguirá durante el análisis, CIS Benchmark.

Una vez elegido el servidor, la plataforma se conecta de forma remota y segura para realizar una evaluación completa, revisando tanto la configuración como el nivel de seguridad actual del sistema. Cuando termina la evaluación, también ofrece la opción de aplicar, de manera automática, las correcciones necesarias o las medidas de hardening recomendadas para asegurarse de que el servidor quede alineado con las mejores prácticas de seguridad y cumpla con los requisitos normativos establecidos.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS XLIX

Además, los resultados de la evaluación pueden exportarse en PDF, lo que facilita su revisión, documentación o auditoría. La información se muestra de forma clara y ordenada, con un resumen de todos los controles evaluados los llamados checks que incluye qué configuración o valor esperado, qué valor tiene actualmente el servidor y si cumple, no cumple.

Check	Valor Esperado	Valor Actual	Cumplimiento
El parámetro "Minimum Password Length" debe establecerse a 10 o un valor mayor.	≥ 10		
El parámetro "Maximum Password Age" debe configurarse a un valor no mayor a 60.	≤ 60		
El parámetro "Minimum Password Age" debe configurarse a un valor mayor a 0.	> 0		
El parámetro "Password must meet complexity requirements" debe estar habilitado.	Habilitado		
El parámetro "Enforce password history" debe configurarse a un valor de 24 o mayor.	≥ 24		
El parámetro "Store passwords using reversible encryption" debe estar deshabilitado.	Deshabilitado		
El parámetro "Account Lockout Threshold" debe configurarse en un valor no mayor a 5.	≤ 5		
El parámetro "Account Lockout Duration" debe configurarse a un valor igual o mayor de 60 minutos o "0" para que...	≥ 60 o 0		
El parámetro "Reset account lockout counter after" debe estar configurado a un valor mayor o igual a "30".	≥ 30		
El servicio "Application Layer Gateway (ALG)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Windows Audio (Audiosrv)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Wired AutoConfig (dot3svc)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Windows Installer (msiserver)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Help and Support Center Service (Helpsvc)" no debe estar en ejecución a menos que sea requerido.	Detenido		

Ilustración 17 Interfaz principal.

Gestión.

La administración de la plataforma permite gestionar servidores y usuarios, ofreciendo opciones para agregarlos, editarlos, actualizarlos o eliminarlos, así como cerrar la sesión.

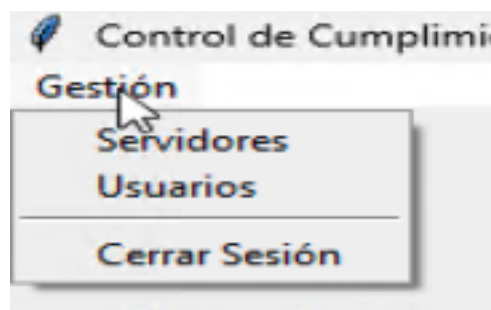
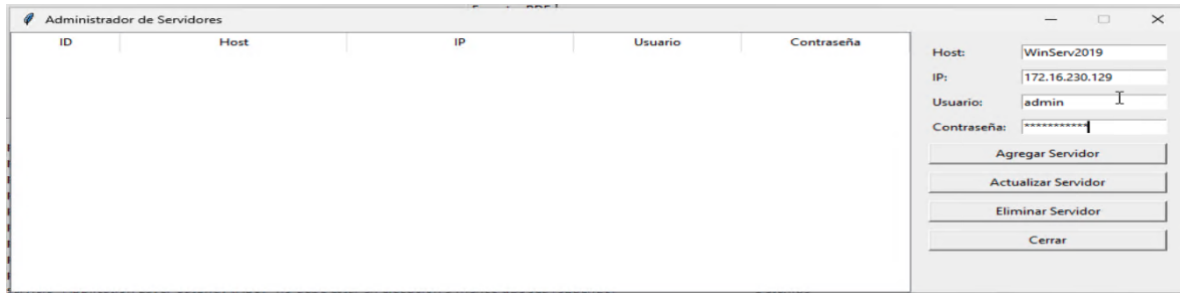


Ilustración 18 Gestión.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS L

Administración de servidores.

La gestión de servidores permite añadir nuevos equipos para su evaluación, siempre que sean compatibles con Windows Server 2019.



ID	Host	IP	Usuario	Contraseña
----	------	----	---------	------------

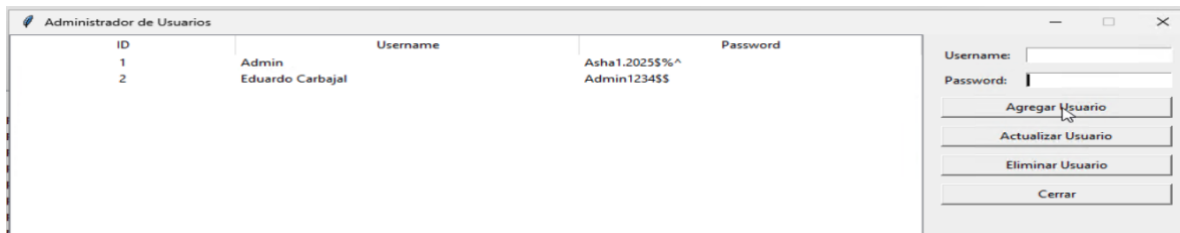
Host: WinServ2019
IP: 172.16.230.129
Usuario: admin
Contraseña: [masked]

Agregar Servidor
Actualizar Servidor
Eliminar Servidor
Cerrar

Ilustración 19 Adinistración de servidores.

Administración de usuarios.

La administración de usuarios facilita su gestión, permitiendo agregar nuevos usuarios, actualizar sus datos o eliminarlos cuando sea necesario.



ID	Username	Password
1	Admin	Asha1.20255%^
2	Eduardo Carbajal	Admin12345\$

Username: [input]
Password: [input]

Agregar Usuario
Actualizar Usuario
Eliminar Usuario
Cerrar

Ilustración 20 Administración de usuarios.

Desarrollo De Software Back-End.

Esta etapa se centra en la lógica del sistema y el manejo de datos, asegurando que las funcionalidades trabajen de forma coherente con la interfaz. Se divide en las siguientes subfases:

- **Autenticación:** Implementación de mecanismos de acceso seguro mediante credenciales para restringir el uso del sistema a personal autorizado.
- **Selección del sistema:** Programación de módulos que permiten al usuario seleccionar el servidor o equipo específico donde se realizará la auditoría o corrección, realazar la evaluación, aplicar correcciones y exportar los resultados.
- **Gestión de scripts:** Codificación de scripts encargados de ejecutar la verificación de configuraciones.

19.1 Pruebas de funcionamiento.

Las pruebas de funcionamiento tienen como finalidad asegurarse de que todas las funcionalidades implementadas en el sistema operen de manera adecuada y cumplan con los requisitos definidos en la etapa de diseño. Durante esta fase, se revisa tanto la interacción del usuario con la plataforma a través de la interfaz gráfica, como el desempeño de los procesos internos gestionados por los módulos de back-end.

Se verifica que la interfaz sea clara, intuitiva y accesible, permitiendo al usuario llevar a cabo tareas clave como iniciar sesión, elegir los servidores a auditar, ejecutar evaluaciones, aplicar configuraciones de hardening, administrar usuarios y servidores, y generar reportes. De igual manera, se comprueba que los procesos de autenticación, evaluación y selección de sistemas, aplicación de correcciones y exportación de resultados se ejecuten de forma segura y eficiente.

Estas pruebas aseguran que la interfaz visual y la lógica interna trabajen de manera conjunta, brindando al usuario final una experiencia consistente y confiable.

Acceso inicial.

- **Contraseña predeterminada:** El software proporciona una clave de acceso por defecto para ingresar al sistema.
- **Actualización de contraseña:** Una vez utilizada la contraseña predeterminada, el sistema exige de manera inmediata su modificación para garantizar mayor seguridad.

Interfaz inicial.

- **Menús de navegación:** Se despliega la interfaz principal del software, la cual incluye menús y submenús para la administración de usuarios, gestión de escaneos, aplicación de correcciones y exportación de resultados.

Gestión de servidores.

- **Incorporación de servidores:** La plataforma permite añadir nuevos servidores a evaluar, considerando parámetros como dirección IP, nombre de host y credenciales administrativas.
- **Eliminación de servidores:** Es posible retirar servidores tanto de la interfaz como de la base de datos asociada.

Gestión de usuarios.

- **Creación de usuarios:** Se habilita la opción de registrar nuevos usuarios para que accedan al sistema y realicen las operaciones correspondientes.
- **Modificación de usuarios:** El software ofrece la posibilidad de actualizar los datos previamente registrados de un usuario.
- **Confirmación de eliminación:** Antes de eliminar a un usuario, se solicita una verificación que confirme dicha acción.
- **Eliminación definitiva:** Permite borrar de manera permanente a los usuarios seleccionados.

Comunicación.

- **Verificación de conexión:** Se valida la comunicación con el servidor seleccionado, diferenciando entre una conexión exitosa, una falla por problemas de red o la inactividad del propio servidor.

Evaluación.

- **Validación de configuraciones:** El sistema revisa los parámetros de configuración del servidor, clasificándolos como correctos, incorrectos o no aplicables.
- **Exportación de resultados:** Los reportes de evaluación pueden generarse en formato PDF como evidencia inicial del estado de las configuraciones.

Aplicación de correcciones.

- **Ejecución de correcciones:** El software aplica de forma automatizada los scripts necesarios para ajustar las configuraciones a los parámetros establecidos en la regulación CIS Benchmarks.
- **Evidencia de correcciones:** Tras la aplicación, los resultados pueden exportarse en formato PDF como constancia de los cambios realizados en el servidor.

CAPÍTULO 4. APLICACIÓN DE LA METODOLOGÍA Y DISCUSIÓN DE RESULTADOS

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LV

En esta sección se presenta la implementación práctica de la metodología propuesta para fortalecer la seguridad en servidores críticos, así como el análisis de los resultados obtenidos tras su aplicación. A lo largo del proyecto, se utilizó la metodología ágil Scrum para organizar el desarrollo de la plataforma, permitiendo iteraciones rápidas y mejoras continuas en función de la retroalimentación.

La aplicación de la metodología incluye tanto el desarrollo del software como su validación mediante pruebas funcionales, evaluando cada uno de los módulos: autenticación, gestión de usuarios y servidores, ejecución de evaluaciones, aplicación de correcciones y generación de reportes. También se describe el flujo completo de la interacción usuario-sistema, desde el acceso inicial hasta la exportación de evidencias.

Los resultados obtenidos en cada fase permiten comprobar la eficacia de la plataforma para identificar configuraciones inseguras, aplicar correcciones en línea con los CIS Benchmarks y dejar evidencia documentada de las evaluaciones realizadas. La discusión de los resultados resalta los logros alcanzados, las limitaciones identificadas y las recomendaciones para futuras mejoras, reafirmando la importancia de una gestión proactiva de la seguridad basada en metodologías ágiles y herramientas especializadas.

Acceso inicial.

Durante el proceso de acceso inicial, la plataforma solicita de manera obligatoria la actualización de la contraseña definida por defecto. Esta medida busca garantizar un nivel básico de seguridad desde el primer uso, evitando que la clave predeterminada se mantenga activa y pueda ser aprovechada como un punto de vulnerabilidad. Una vez modificado el password, el sistema confirma el cambio para que el usuario pueda continuar con las operaciones correspondientes bajo credenciales personalizadas y seguras.



Ilustración 21 Acceso inicial.

Durante el primer acceso, la plataforma solicita el uso de una contraseña predeterminada (default), la cual debe ser modificada obligatoriamente para garantizar la seguridad del sistema. Una vez ingresada, el software exige su actualización inmediata por una clave personalizada definida por el usuario y, posteriormente, confirma el cambio para futuros accesos. Este procedimiento evita el uso prolongado de contraseñas genéricas y reduce el riesgo de accesos no autorizados, fortaleciendo así la protección de la plataforma.

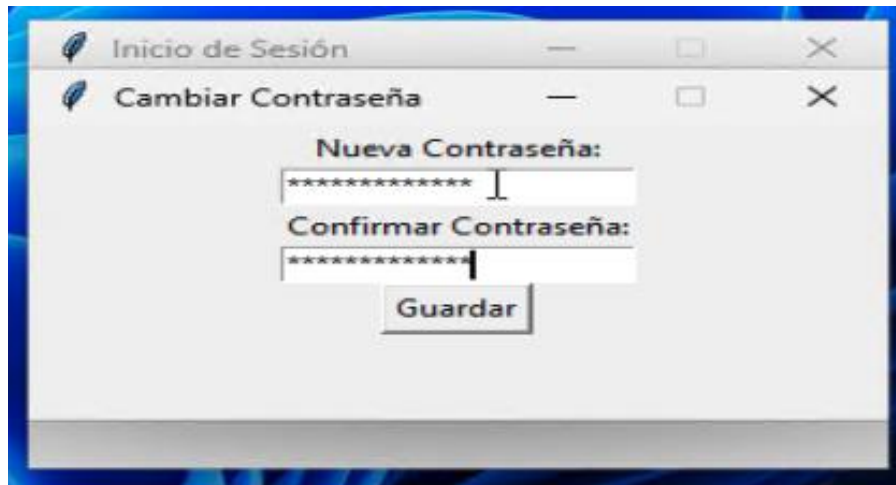


Ilustración 22 Cambio de password.

La actualización de la contraseña default asegura que el usuario disponga de credenciales únicas y seguras para acceder a la plataforma. Una vez realizada la modificación, el sistema confirma el cambio y registra la nueva clave como válida para futuros ingresos, garantizando con ello la protección frente a accesos no autorizados y reforzando las buenas prácticas de seguridad en el uso del software.

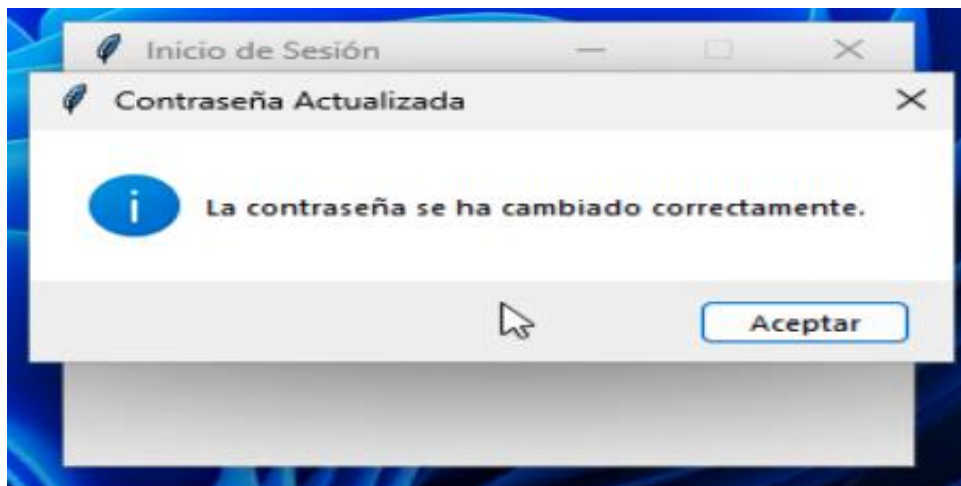


Ilustración 23 Confirmación de cambio.

Interfaz principal.

En esta etapa se verifica que todos los elementos de la interfaz gráfica de la plataforma se desplieguen correctamente. Esto incluye aspectos esenciales como menús principales y secundarios, etiquetas de texto, botones de acción, campos de ingreso de datos, listas desplegables y controles de validación. Una correcta visualización es fundamental para asegurar la usabilidad, reducir errores de interacción y garantizar que los usuarios cuenten con un entorno confiable para la gestión de configuraciones y evaluaciones.

- Menús
- Etiquetas y textos
- Botones
- Campos de texto
- Listas desplegables
- Controles o checks a evaluar

The screenshot shows the 'Control de Cumplimiento' application window. At the top, there's a 'Gestión' section with four dropdown menus: 'Host', 'Sistema Operativo' (set to 'Windows Server 2019'), 'Regulación' (set to 'CIS Benchmark Windows Server 2019'), and 'Aplicar Configuraciones'. To the right of these are buttons for 'Conectar', 'Evaluar', and 'Exportar PDF'. Below this is a table with four columns: 'Check', 'Valor Esperado', 'Valor Actual', and 'Cumplimiento'. The table lists 12 checks related to password policies and services. The 'Valor Actual' column shows the current status, and the 'Cumplimiento' column shows the result (e.g., 'Detenido' for services not running).

Check	Valor Esperado	Valor Actual	Cumplimiento
El parámetro "Minimum Password Length" debe establecerse a 10 o un valor mayor.	>= 10		
El parámetro "Maximum Password Age" debe configurarse a un valor no mayor a 60.	<= 60		
El parámetro "Minimum Password Age" debe configurarse a un valor mayor a 0.	> 0		
El parámetro "Password must meet complexity requirements" debe estar habilitado.	Habilitado		
El parámetro "Enforce password history" debe configurarse a un valor de 24 o mayor.	>= 24		
El parámetro "Store passwords using reversible encryption" debe estar deshabilitado.	Deshabilitado		
El parámetro "Account Lockout Threshold" debe configurarse en un valor no mayor a 5.	<= 5		
El parámetro "Account Lockout Duration" debe configurarse a un valor igual o mayor de 60 minutos o "0" para que no se bloquee.	>= 60 o 0		
El parámetro "Reset account lockout counter after" debe estar configurado a un valor mayor o igual a "30".	>= 30		
El servicio "Application Layer Gateway (ALG)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Windows Audio (Audiosrv)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Wired AutoConfig (dot3svc)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Windows Installer (msiserver)" no debe estar en ejecución a menos que sea requerido.	Detenido		
El servicio "Help and Support Center Service (Helpsvc)" no debe estar en ejecución a menos que sea requerido.	Detenido		

Ilustración 24 Visualización inicial.

Gestión de servidores.

La plataforma permite registrar una cantidad indefinida de servidores para su posterior análisis. Cada servidor se incorpora mediante el registro de datos clave como nombre de host, dirección IP, usuario y credenciales de acceso. Adicionalmente, es posible modificar la información previamente almacenada o bien eliminar servidores de la interfaz y de la base de datos en caso de que ya no sean necesarios en los procesos de evaluación y corrección. Este módulo asegura una administración flexible de los entornos que se desean auditar.

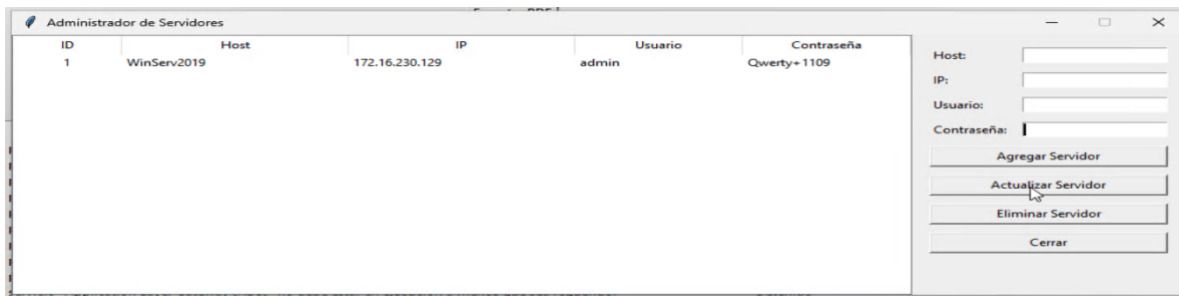


Ilustración 25 Agregando servidor 1.

La plataforma permite registrar un segundo servidor ingresando parámetros esenciales como el nombre del host, la dirección IP, el usuario autorizado y su respectiva contraseña. Esta información es necesaria para que el sistema pueda establecer comunicación con el servidor y realizar las evaluaciones correspondientes de manera segura y confiable.

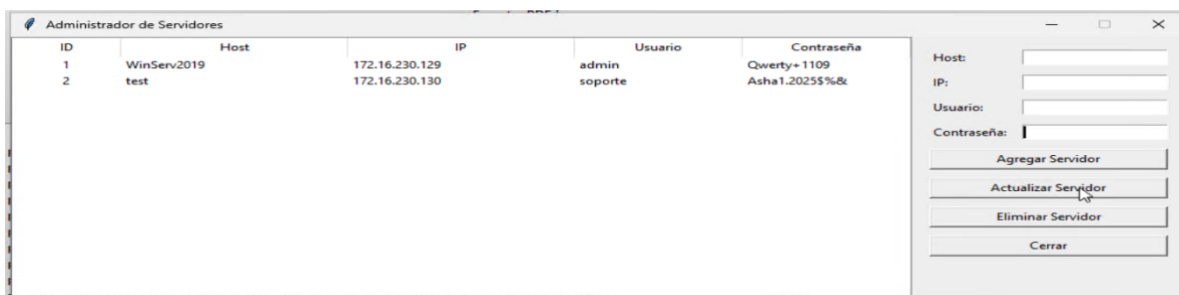


Ilustración 26 Agregando servidor 2.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LX

Cuando un servidor ya no es necesario dentro del proceso de evaluación, la plataforma brinda la opción de eliminarlo tanto de la interfaz de usuario como de la base de datos. Esta acción asegura que únicamente permanezcan activos los servidores relevantes, optimizando la gestión de recursos y reduciendo riesgos de exposición innecesaria.

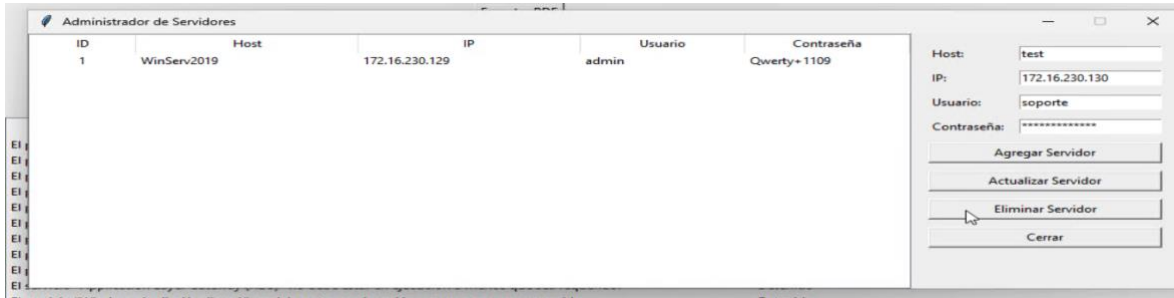


Ilustración 27 Eliminar servidor 2.

Gestión de usuarios.

De manera similar a los servidores, la plataforma ofrece la opción de crear múltiples usuarios con diferentes niveles de acceso. Los administradores pueden añadir nuevos registros, actualizar la información de usuarios existentes o eliminarlos de forma definitiva. Para prevenir acciones accidentales, el sistema solicita una confirmación previa antes de proceder con la eliminación. Esta funcionalidad permite una gestión adecuada de los perfiles, asegurando que únicamente personal autorizado tenga acceso a la ejecución de evaluaciones, correcciones o exportación de resultados.

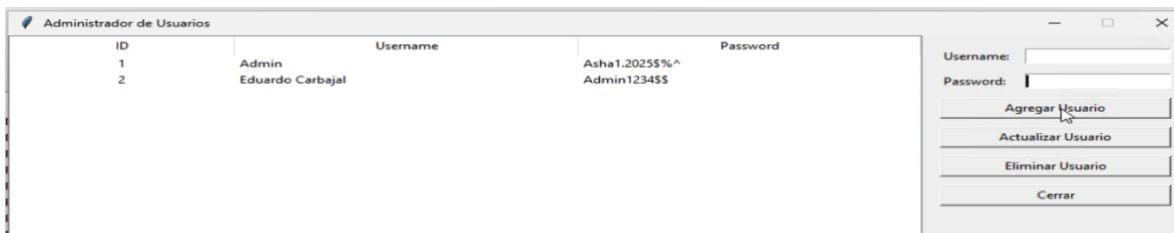


Ilustración 28 Agregar usuarios.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXI

El sistema permite modificar los datos previamente registrados de los usuarios, tales como nombre, credenciales o permisos de acceso. Esta funcionalidad asegura que la información se mantenga vigente y que los usuarios cuenten con los niveles de acceso adecuados según sus funciones dentro de la plataforma.

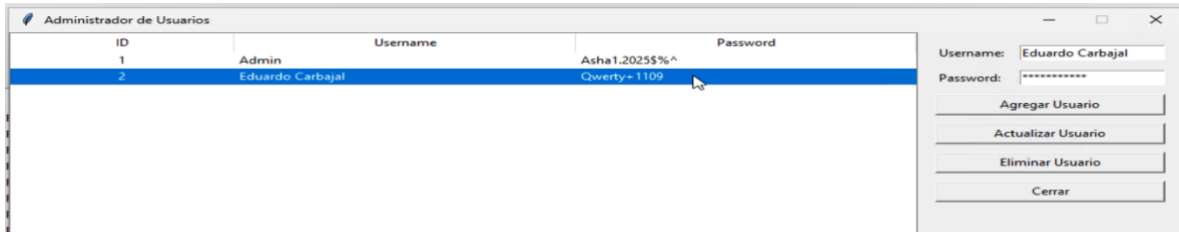


Ilustración 29 Actualizar usuarios.

Antes de eliminar un usuario registrado, el sistema solicita una confirmación de la acción, con el fin de evitar eliminaciones accidentales. Esta medida preventiva refuerza la seguridad en la administración de perfiles y protege la integridad de la información registrada.

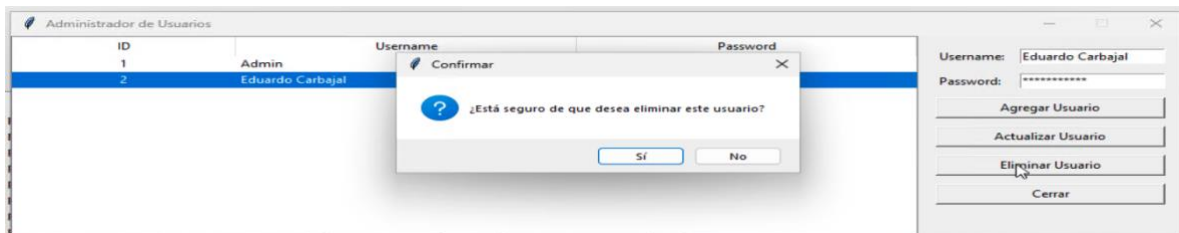


Ilustración 30 Confirmación - Eliminar usuarios.

Una vez confirmada la acción, la plataforma procede a la eliminación definitiva de los usuarios seleccionados. Esto garantiza que dichas cuentas no puedan volver a acceder al sistema, preservando así la seguridad y control de acceso en el entorno.

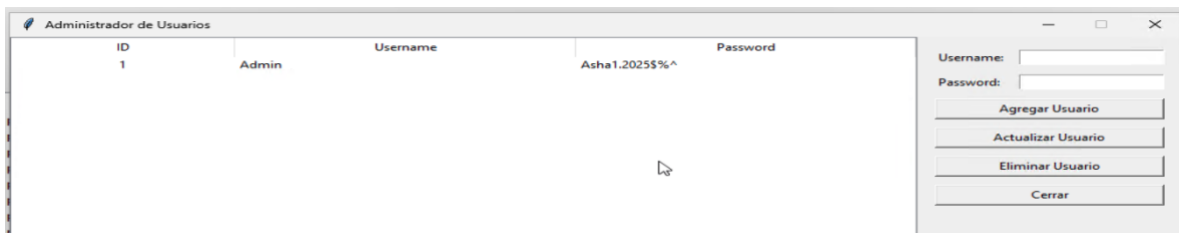


Ilustración 31 Eliminar usuarios.

Comunicación.

Una vez definidos los servidores y usuarios, el siguiente paso consiste en establecer la comunicación con el servidor objetivo. Durante esta validación, la plataforma comprueba que el servidor esté activo, que sea alcanzable a través de la red y que las credenciales registradas sean correctas. Este proceso es crítico, pues determina la viabilidad de ejecutar las evaluaciones posteriores y garantiza que los datos obtenidos correspondan al sistema real y operativo.

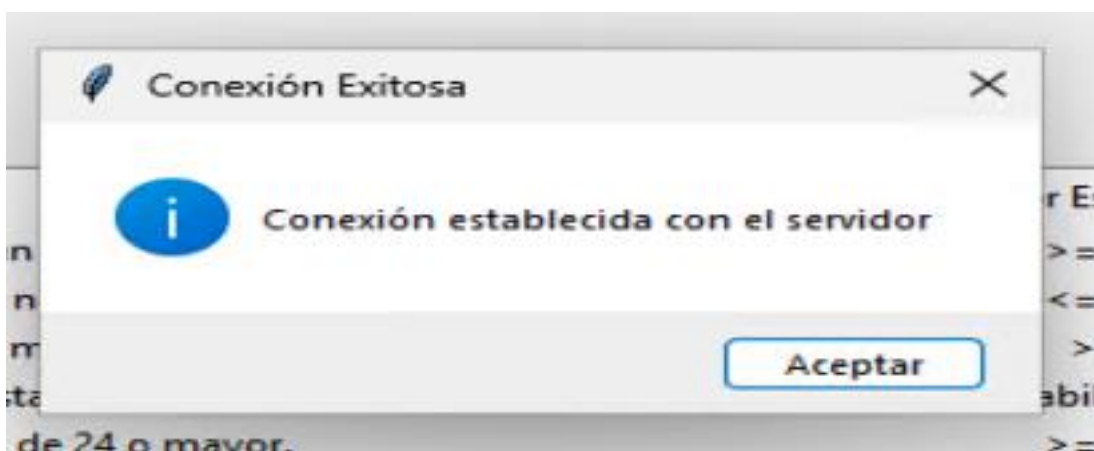


Ilustración 32 Conexión exitosa.

Evaluación.

En este módulo se ejecuta una revisión de las configuraciones del servidor con base en parámetros definidos por la herramienta. Los resultados se clasifican en tres categorías principales:

- **Incorrecto:** Configuraciones que presentan desviaciones respecto al estándar de seguridad y que requieren corrección inmediata.
- **OK:** Configuraciones implementadas correctamente, alineadas a las buenas prácticas y estándares definidos.
- **N/A:** Configuraciones que no aplican al servidor evaluado debido a la ausencia de servicios, rutas o llaves de registro correspondientes.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES
CRÍTICOS LXIII

La evaluación inicial constituye un diagnóstico que refleja el estado real del servidor en términos de cumplimiento con las configuraciones esperadas.

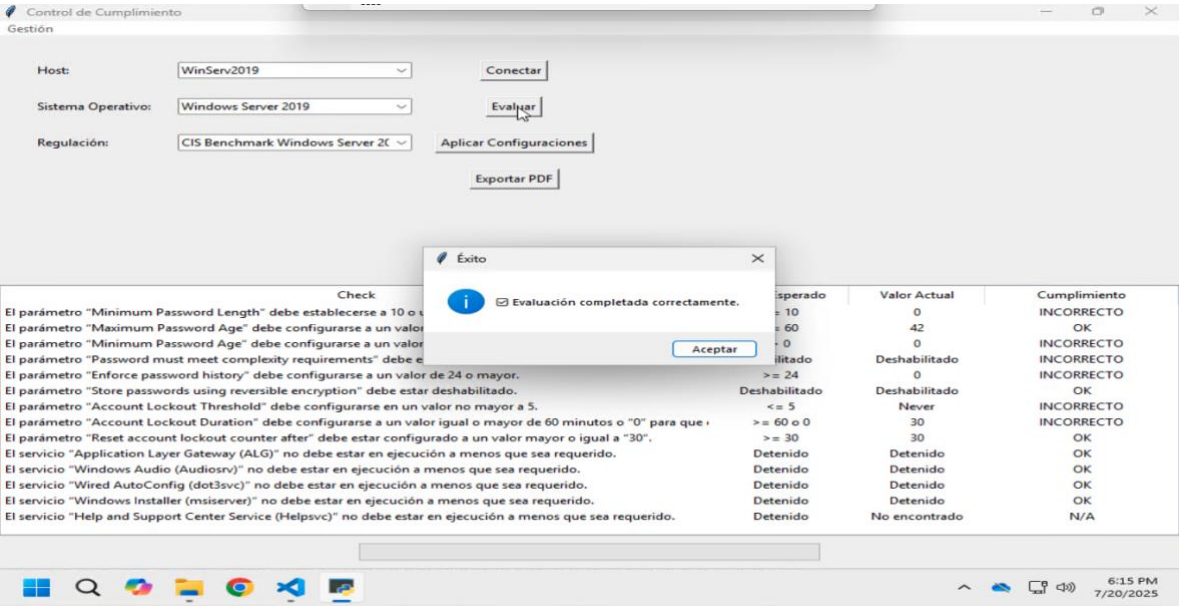


Ilustración 33 Evaluación inicial.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXIV

Los resultados obtenidos pueden exportarse en formato PDF como evidencia formal del estado de las configuraciones antes de realizar cualquier ajuste. Este documento funciona como un respaldo que permite comparar el estado inicial con los resultados obtenidos tras la aplicación de correcciones. La evidencia almacenada contribuye al cumplimiento de auditorías y procesos de aseguramiento de la información.

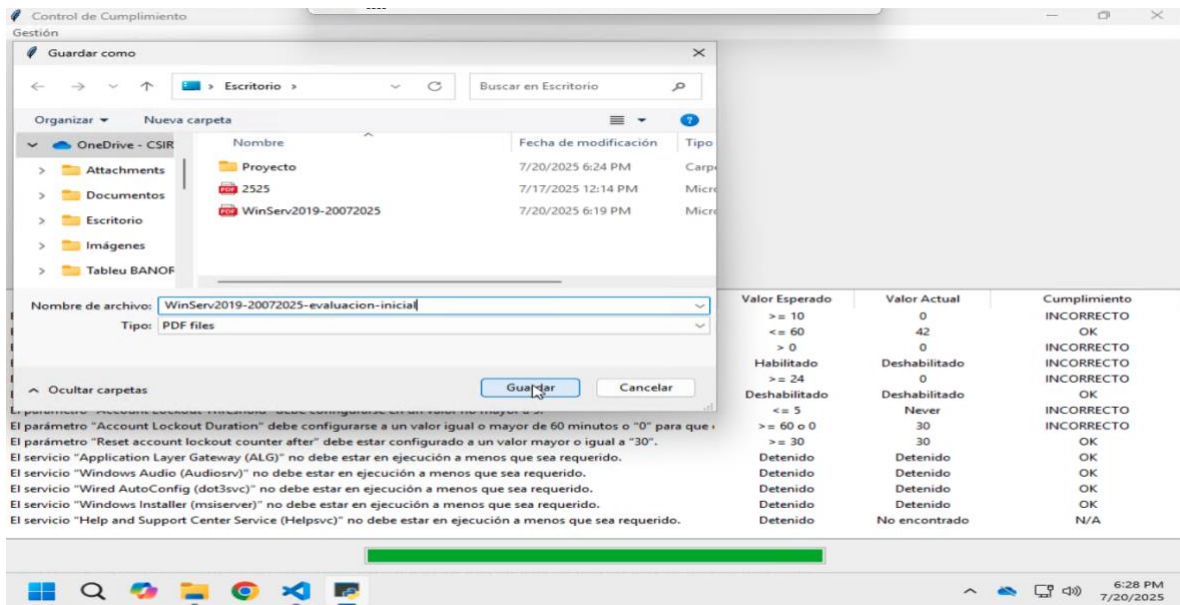


Ilustración 34 Exportar evaluación inicial.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXV

La herramienta indica de manera explícita la ruta de almacenamiento del archivo PDF generado como resultado de la primera evaluación, lo que facilita la trazabilidad y posterior consulta de la evidencia registrada.

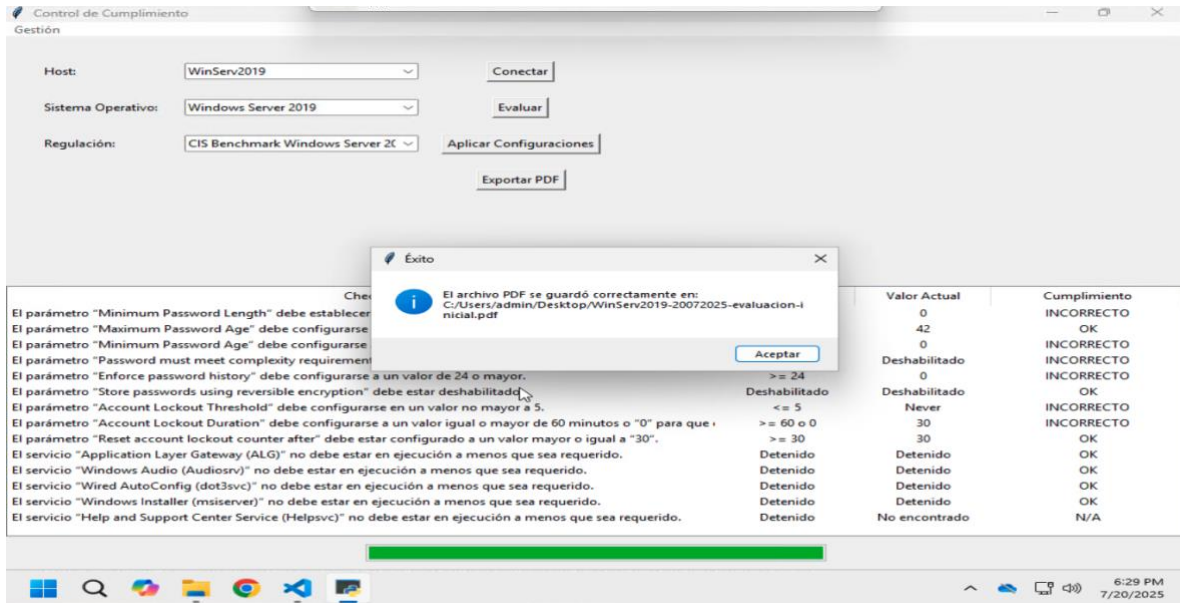


Ilustración 35 Exportado.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXVI

El PDF exportado refleja el estado de las configuraciones del servidor tras la primera evaluación, mostrando las configuraciones correctas, incorrectas o no aplicables, y constituyendo la evidencia documental del diagnóstico inicial.

Check	Valor Esperado	Valor Actual	Cumplimiento
El parámetro "Minimum Password Length" d	>= 10	0	INCORRECTO
El parámetro "Maximum Password Age" debe	<= 60	42	OK
El parámetro "Minimum Password Age" debe	> 0	0	INCORRECTO
El parámetro "Password must meet complex	Habilitado	Deshabilitado	INCORRECTO
El parámetro "Enforce password history"	>= 24	0	INCORRECTO
El parámetro "Store passwords using reve	Deshabilitado	Deshabilitado	OK
El parámetro "Account Lockout Threshold"	<= 5	Never	INCORRECTO
El parámetro "Account Lockout Duratig"	>= 60 o 0	30	INCORRECTO
El parámetro "Reset account lockout caku	>= 30	30	OK
El servicio "Application Layer Gateway (	Detenido	Detenido	OK
El servicio "Windows Audio (Audiosrv)" n	Detenido	Detenido	OK
El servicio "Wired AutoConfig (dot3svc)"	Detenido	Detenido	OK
El servicio "Windows Installer (msiserve	Detenido	Detenido	OK
El servicio "Help and Support Center Ser	Detenido	No encontrado	N/A
El servicio "IIS Admin" no debe estar en	Detenido	No encontrado	N/A
El servicio "Network Connections (Netman	Detenido	Detenido	OK
El servicio "Spooler" no debe estar en e	Detenido	Ejecutándose	INCORRECTO
El servicio "Portable Device Enumerator"	Detenido	Ejecutándose	INCORRECTO
El servicio "Routing and Remote Access"	Detenido	Detenido	OK
El servicio "Background Intelligent Tran	Detenido	Detenido	OK
El servicio "POP3SVC" no debe estar en e	Detenido	No encontrado	N/A
El servicio "Remote Access Connection Ma	Detenido	Detenido	OK
El servicio "Remote Access Auto Connect	Detenido	Detenido	OK
El servicio "Remote Administration (Svc.	Detenido	Ejecutándose	INCORRECTO
El servicio "Remote Desktop (TermService	Detenido	Detenido	OK

Ilustración 36 Resultados primera evaluación.

Aplicación de correcciones.

La plataforma automatiza la aplicación de correcciones mediante la ejecución de scripts diseñados para alinear las configuraciones del servidor con las recomendaciones del CIS Benchmark. Esta funcionalidad reduce el esfuerzo manual y asegura un cumplimiento homogéneo con los estándares de seguridad. Una vez aplicadas las correcciones, se generan evidencias que demuestran los cambios efectuados en el sistema, fortaleciendo la trazabilidad del proceso.

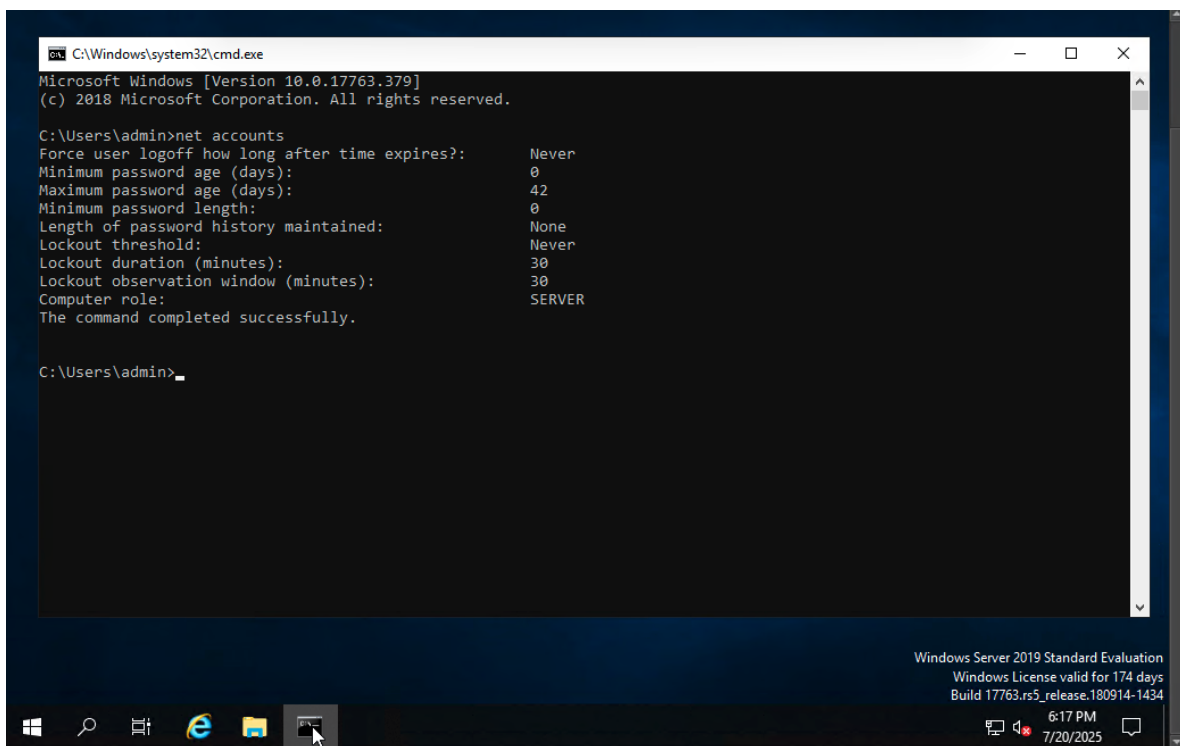


Ilustración 37 Evidencia inicial.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXVIII

La plataforma ejecuta automáticamente los scripts necesarios para ajustar las configuraciones del servidor a los parámetros recomendados por los lineamientos de seguridad establecidos en el CIS Benchmark. Este proceso asegura la estandarización y cumplimiento de buenas prácticas de seguridad.

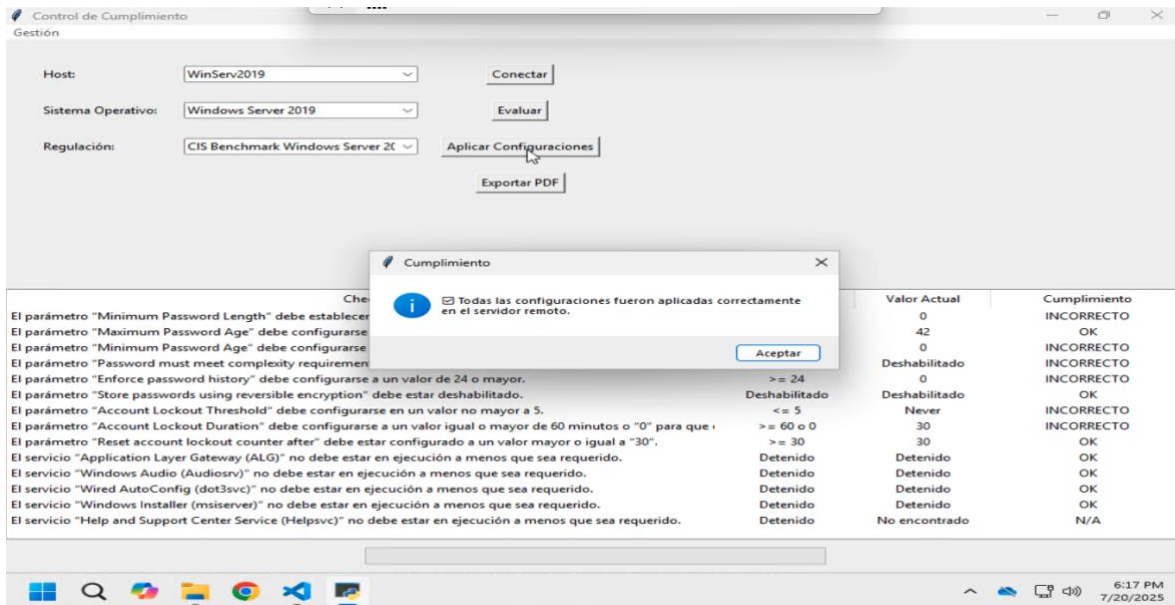
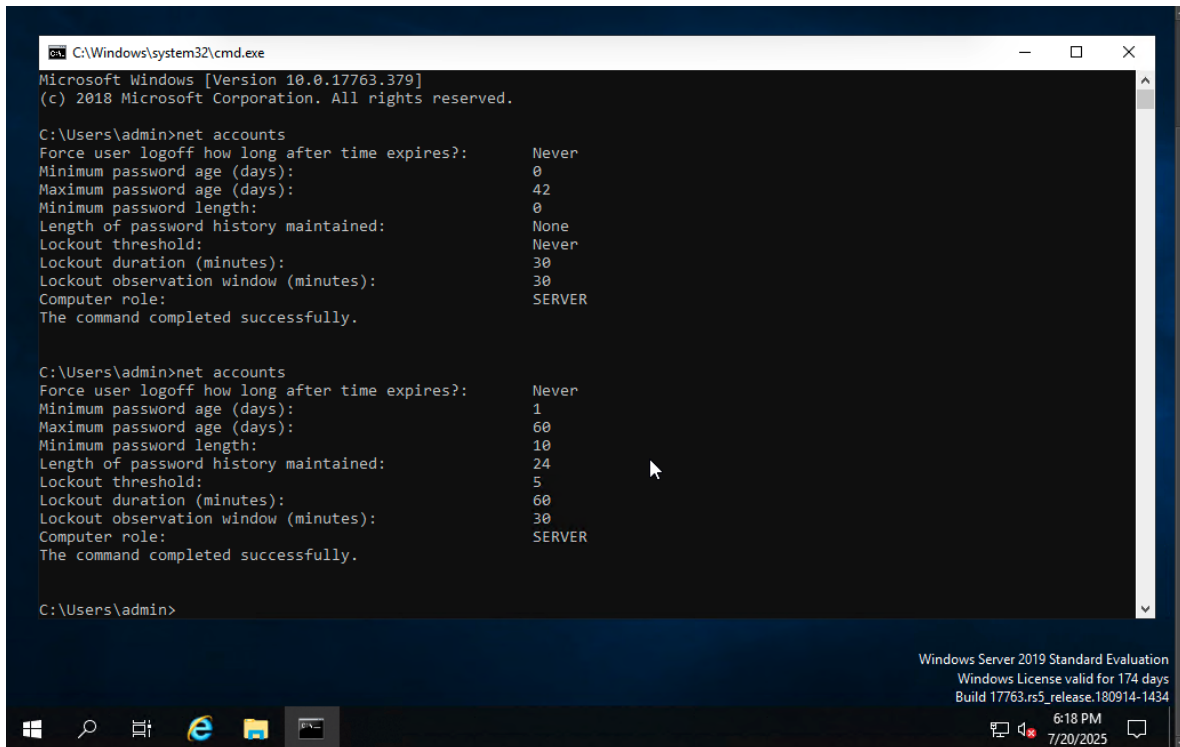


Ilustración 38 Aplicación de correcciones.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXIX

Tras aplicar las correcciones, el sistema genera un reporte que documenta los cambios realizados, funcionando como respaldo de que las configuraciones fueron modificadas correctamente en el servidor evaluado.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\admin>net accounts
Force user logoff how long after time expires?:      Never
Minimum password age (days):                        0
Maximum password age (days):                        42
Minimum password length:                             0
Length of password history maintained:               None
Lockout threshold:                                   Never
Lockout duration (minutes):                          30
Lockout observation window (minutes):                 30
Computer role:                                       SERVER
The command completed successfully.

C:\Users\admin>net accounts
Force user logoff how long after time expires?:      Never
Minimum password age (days):                        1
Maximum password age (days):                        60
Minimum password length:                             10
Length of password history maintained:               24
Lockout threshold:                                   5
Lockout duration (minutes):                          60
Lockout observation window (minutes):                 30
Computer role:                                       SERVER
The command completed successfully.

C:\Users\admin>
```

Windows Server 2019 Standard Evaluation
Windows License valid for 174 days
Build 17763.rs5_release.180914-1434
6:18 PM
7/20/2025

Ilustración 39 Resultados.

Tras la aplicación de correcciones, se realiza una segunda evaluación para validar que los cambios hayan sido implementados de manera adecuada. Este nuevo diagnóstico permite comparar los resultados frente a la evaluación inicial, identificando mejoras en las configuraciones del servidor. Al igual que en la etapa inicial, los resultados se exportan en formato PDF, proporcionando una evidencia

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXX

formal del cumplimiento alcanzado después de la aplicación de las medidas correctivas.

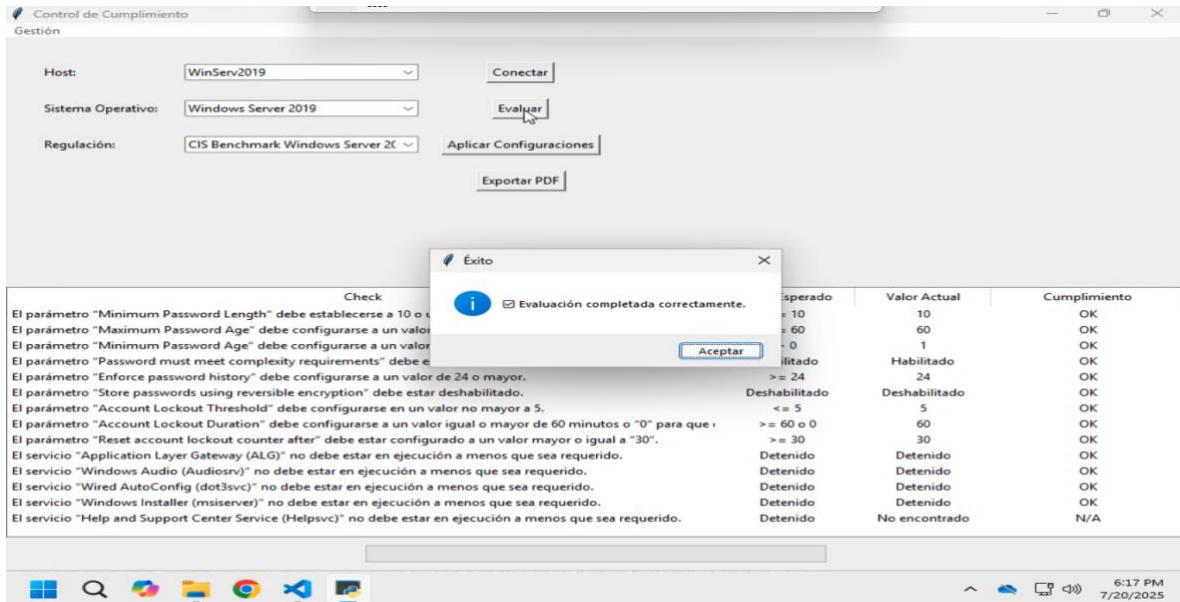


Ilustración 40 Segunda evaluación.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXXI

Los resultados obtenidos pueden exportarse en formato PDF como evidencia formal del estado de las configuraciones antes de realizar cualquier ajuste. Este documento funciona como un respaldo que permite comparar el estado inicial con los resultados obtenidos tras la aplicación de correcciones. La evidencia almacenada contribuye al cumplimiento de auditorías y procesos de aseguramiento de la información.

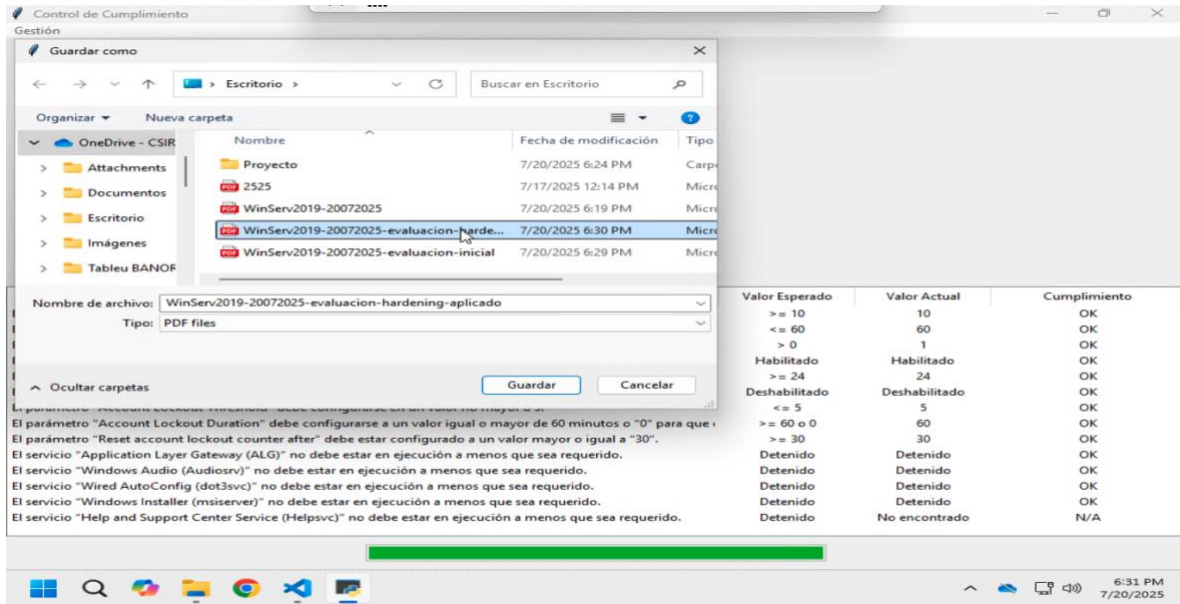


Ilustración 41 Exportar segunda evaluación.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXXII

De igual manera que en la primera fase, la plataforma registra y muestra la ruta donde se guarda la evidencia generada por la segunda evaluación, asegurando la disponibilidad de la información para auditorías o revisiones posteriores.

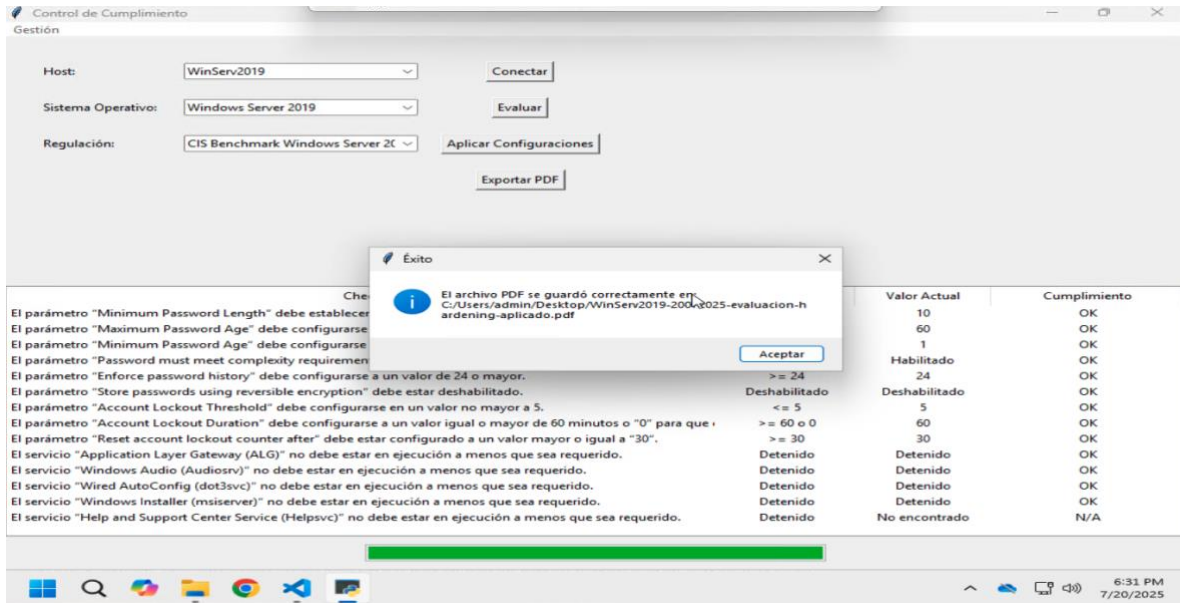
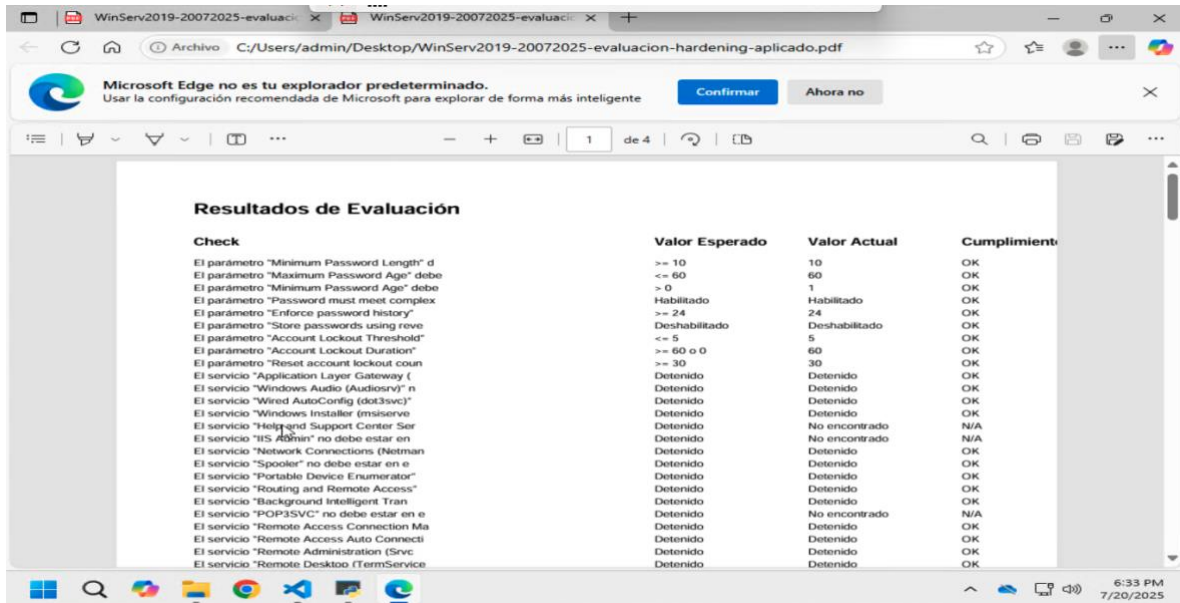


Ilustración 42 Exportado 2.

DISEÑO DE APLICACIÓN AUTOMATIZADA DE HARDENING EN SERVIDORES CRÍTICOS LXXIII

Se muestra el contenido del PDF como resultado de la evaluación final. El documento en formato PDF refleja el estado del servidor después de la aplicación de las correcciones, permitiendo contrastar los resultados con la evaluación inicial y evidenciar las mejoras implementadas en materia de seguridad.



Check	Valor Esperado	Valor Actual	Cumplimiento
El parámetro "Minimum Password Length" d	>= 10	10	OK
El parámetro "Maximum Password Age" debe	<= 60	60	OK
El parámetro "Minimum Password Age" debe	> 0	1	OK
El parámetro "Password must meet complex	Habilitado	Habilitado	OK
El parámetro "Enforce password history"	>= 24	24	OK
El parámetro "Store passwords using reve	Deshabilitado	Deshabilitado	OK
El parámetro "Account Lockout Threshold"	<= 5	5	OK
El parámetro "Account Lockout Duration"	>= 60 o 0	60	OK
El parámetro "Reset account lockout coun	>= 30	30	OK
El servicio "Application Layer Gateway (	Detenido	Detenido	OK
El servicio "Windows Audio (Audiosrv)" n	Detenido	Detenido	OK
El servicio "Wireless AutoConfig (dot3svc)	Detenido	Detenido	OK
El servicio "Windows Installer (msiserve	Detenido	Detenido	OK
El servicio "Help and Support Center Ser	Detenido	No encontrado	N/A
El servicio "IIS Admin" no debe estar en	Detenido	No encontrado	N/A
El servicio "Network Connections (Netman	Detenido	Detenido	OK
El servicio "Spooler" no debe estar en e	Detenido	Detenido	OK
El servicio "Portable Device Enumerator"	Detenido	Detenido	OK
El servicio "Routing and Remote Access"	Detenido	Detenido	OK
El servicio "Background Intelligent Tran	Detenido	Detenido	OK
El servicio "PDQ35VC" no debe estar en e	Detenido	No encontrado	N/A
El servicio "Remote Access Connection Ma	Detenido	Detenido	OK
El servicio "Remote Access Auto Connect	Detenido	Detenido	OK
El servicio "Remote Administration (Svc	Detenido	Detenido	OK
El servicio "Remote Desktop (TermService	Detenido	Detenido	OK

Ilustración 43 Resultados segunda evaluación.

20.1 Validación y verificación.

En esta sección se detallan las actividades realizadas para validar y verificar el correcto funcionamiento de la plataforma desarrollada, asegurando que cumpla con los requisitos establecidos durante la etapa de diseño y desarrollo. La verificación se enfocó en comprobar que cada módulo y funcionalidad implementada opere de acuerdo con las especificaciones técnicas, mientras que la validación evaluó si la plataforma satisface las necesidades del usuario final y responde adecuadamente a los objetivos planteados.

Las pruebas incluyeron la revisión de la interfaz gráfica, la autenticación de usuarios, la gestión de servidores y usuarios, la ejecución de auditorías, la aplicación de medidas de seguridad conforme a los CIS Benchmarks, así como la generación y

exportación de reportes. Se evaluaron escenarios reales y casos de uso para garantizar que el sistema sea robusto, fiable y fácil de utilizar.

Los resultados de esta fase permiten confirmar que la plataforma no solo es técnicamente correcta, sino también útil y alineada con las expectativas de quienes la emplearán para fortalecer la seguridad de los servidores.

21.1 Discusión de resultados.

La futura implementación del software propuesto se proyecta como una herramienta clave para la automatización de la verificación y corrección de configuraciones de seguridad en servidores críticos, siguiendo los lineamientos de los CIS Benchmarks. Con base en el diseño, los objetivos y las pruebas preliminares, se anticipan los siguientes beneficios:

- **Automatización efectiva de auditorías de seguridad**
El sistema será capaz de escanear configuraciones clave del sistema operativo, identificar desviaciones y generar reportes alineados con los estándares CIS. Se espera mantener una tasa de detección de configuraciones erróneas superior al 70% en entornos reales.
- **Reducción significativa en tiempos de evaluación y corrección**
Se proyecta una disminución de hasta un 60% en el tiempo destinado a auditorías manuales, lo que permitirá a los equipos de ciberseguridad enfocarse en tareas estratégicas y mejorar su eficiencia operativa. Además, las pruebas iniciales demostraron que la aplicación de las correcciones ya no requiere horas ni días de trabajo manual, sino que puede completarse en cuestión de minutos gracias a la automatización, optimizando así los procesos y reduciendo los tiempos de indisponibilidad de los servicios.
- **Interfaz intuitiva y visualización clara de resultados**
La plataforma proporcionará a los usuarios una experiencia sencilla para interpretar hallazgos de seguridad, facilitando decisiones rápidas y fundamentadas ante desviaciones en la configuración.

- **Alta aceptación por parte de usuarios técnicos**
Se prevé que el 85% de los profesionales en ciberseguridad valoren positivamente la automatización del proceso, y que el 75% priorice su alineación con los CIS Benchmarks, fortaleciendo su adopción institucional.
- **Cumplimiento normativo y trazabilidad fortalecida**
Los reportes automáticos en formatos técnicos y ejecutivos permitirán mantener evidencia clara de cumplimiento regulatorio, facilitando auditorías internas y externas con mayor control y transparencia.

Desde una perspectiva a futuro, los resultados esperados posicionan esta solución como una herramienta integral para mejorar la postura de seguridad en organizaciones que manejan infraestructuras críticas. Su aplicación no solo representará un avance técnico, sino también un cambio en la cultura organizacional hacia la prevención proactiva y el cumplimiento estructurado de estándares de seguridad.

La automatización de las auditorías con base en los CIS Benchmarks permitirá cerrar la brecha existente entre el conocimiento normativo y su ejecución técnica. Aunque muchas organizaciones cuentan con herramientas como firewalls o antivirus, este desarrollo busca resolver una de las debilidades menos abordadas: la correcta configuración de los servidores.

Se espera que el software se convierta en un habilitador de capacidades en ciberseguridad, especialmente en organizaciones con recursos limitados, al reducir la dependencia de personal altamente especializado. No obstante, también se proyecta que esta herramienta se complemente con otras tecnologías como SIEM, gestión de vulnerabilidades y soluciones de monitoreo continuo, formando parte de una estrategia de seguridad en capas.

En términos de escalabilidad, se anticipa que el sistema podrá adaptarse a diferentes entornos, incluyendo infraestructuras híbridas y en la nube. Futuras versiones podrían integrar inteligencia artificial para sugerir correcciones basadas

en patrones históricos y contexto de amenaza, así como dashboards en tiempo real con indicadores clave de riesgo.

Finalmente, el uso de la metodología Scrum permitirá que el software continúe evolucionando mediante ciclos iterativos de mejora, ajustándose a los cambios en el entorno tecnológico y a las necesidades emergentes de los usuarios. Este enfoque garantiza que la herramienta no solo sea funcional al momento de su entrega, sino que mantenga su vigencia y efectividad a lo largo del tiempo.

CAPÍTULO 5. CONCLUSIONES Y PERSPECTIVAS PARA TRABAJO FUTURO

A partir del análisis realizado, se concluye que la automatización en la verificación y corrección de configuraciones de seguridad en servidores críticos representa una necesidad urgente ante el crecimiento exponencial de los ataques cibernéticos y la sofisticación de sus métodos. La solución propuesta, basada en el diseño de un software guiado por los lineamientos de los CIS Benchmarks, tiene el potencial de convertirse en una herramienta clave para la gestión proactiva de la ciberseguridad en entornos organizacionales.

Se proyecta que su implementación no solo permitirá mejorar la eficiencia operativa al reducir los tiempos de auditoría y remediación, sino también fortalecerá la cultura de cumplimiento normativo y prevención de riesgos. Además, brindará soporte técnico a equipos con recursos limitados, minimizando la necesidad de conocimientos especializados para aplicar buenas prácticas de hardening.

La automatización de procesos críticos como la evaluación de configuraciones y la generación de reportes técnicos aumentará significativamente la visibilidad sobre el estado de los sistemas, facilitando la toma de decisiones informadas y anticipadas. A medida que evolucione, el sistema podría integrarse con soluciones como SIEM, análisis de vulnerabilidades e inteligencia artificial, posicionándose como parte esencial de una estrategia de seguridad en capas.

En un escenario futuro, esta herramienta podrá escalar hacia entornos más complejos como infraestructuras en la nube o híbridas, adaptándose a nuevos desafíos tecnológicos y operativos. El uso de metodologías ágiles como Scrum asegurará una evolución continua y orientada a las necesidades reales de los usuarios.

En definitiva, este trabajo sienta las bases para un enfoque más automatizado, eficiente y normativamente alineado en la protección de activos críticos, destacando que el fortalecimiento de servidores no debe depender únicamente de tecnologías de seguridad tradicionales, sino de procesos estructurados, visibilidad constante y adaptabilidad futura.

REFERENCIAS

- Charles P. Pfleeger, S. L. (2003). *Google Libros*. Obtenido de https://google.com.mx/books/edition/Security_in_Computing/O3VB-zspJo4C?hl=es-419&gbpv=0
- ALBAN, Y. A. (2020). *Diseño e implementacion de una metodología de hardening para los servidores, estaciones de trabajo y directorio activo del ministerio de hacienda y crédito publico*. Obtenido de Google Académico: <http://repository.unipiloto.edu.co/handle/20.500.12277/8206>
- Anderson, R. (22 de Diciembre de 2020). Obtenido de https://www.google.com.mx/books/edition/Security_Engineering/GNIHEAAAQBAJ?hl=es-419&gbpv=0
- Dafydd Stuttard, M. P. (2011). *Google Libros*. Obtenido de https://www.google.com.mx/books/edition/The_Web_Application_Hacker_s_Handbook/YJKbVzeabJYC?hl=es-419&gbpv=0
- Erickson, J. (Febrero de 2008). *Google Libros*. Obtenido de [https://www.google.com.mx/books/edition/Hacking_The_art_Of_Exploitation/6JJPDwAAQBAJ?hl=es-419&gbpv=1&dq=Erickson,+J.+\(2008\).+Hacking:+The+Art+of+Exploitation.&printsec=frontcover](https://www.google.com.mx/books/edition/Hacking_The_art_Of_Exploitation/6JJPDwAAQBAJ?hl=es-419&gbpv=1&dq=Erickson,+J.+(2008).+Hacking:+The+Art+of+Exploitation.&printsec=frontcover)
- Internet, C. f. (2024). Obtenido de <https://www.cisecurity.org/>
- Iza Sanhueza, L. J. (2020). *Propuesta Metodológica para evaluar la seguridad del entorno informático de la Caja Central de cooperativas mediante procesos de Hardening*. Obtenido de Google Académico: <https://repositorio.espe.edu.ec/bitstream/21000/24845/1/T-ESPE-044544.pdf>
- Merlos, B. (2021). *Bastionado de servidores. Desarrollo de herramienta de auditoria*. Obtenido de Google Académico: <http://repositorio.ual.es/handle/10835/13520>
- Schneier, B. (2015 de Octubre de 2015). *Gooble Libros*. Obtenido de https://www.google.com.mx/books/edition/Applied_Cryptography/01vfjgEACAAJ?hl=es-419
- Stallings, W. (28 de Julio de 2016). *Google Libros*. Obtenido de https://www.google.com.mx/books/edition/Network_Security_Essentials/HEWwDAEACAAJ?hl=es-419
- Szor, P. (2005 de Febrero de 2005). *Google Libros*. Obtenido de https://www.google.com.mx/books/edition/The_Art_of_Computer_Virus_Research_and_D/XE-ddYF6uhYC?hl=es-419&gbpv=0

ANEXOS

Configuraciones

Para permitir la administración remota de un servidor Windows mediante el protocolo Windows Remote Management, es necesario habilitar el servicio correspondiente y configurar el puerto estándar (5985) para recibir conexiones HTTP. Esta configuración facilita la ejecución remota de evaluaciones, auditorías y la aplicación de configuraciones de seguridad desde la herramienta desarrollada.

A continuación, se presentan los comandos utilizados:

- winrm quickconfig:
 - Inicializa y configura WinRM con los valores predeterminados recomendados.
- Set-Item -Path WSMan:\localhost\Service\Auth\Basic -Value \$true
 - Habilita la autenticación básica para las conexiones remotas.
- Set-Item -Path WSMan:\localhost\Service\AllowUnencrypted -Value \$true
 - Permite conexiones sin cifrado en escenarios controlados o de prueba.
- netsh advfirewall firewall add rule name="WinRM HTTP" protocol=TCP dir=in localport=5985 action=allow
 - Crea una regla en el firewall de Windows para permitir tráfico entrante a través del puerto TCP 5985.
- winrm set winrm/config/service/auth '@{Basic="true"}'
 - Establece explícitamente la autenticación básica en la configuración del servicio WinRM.
- winrm set winrm/config/service '@{AllowUnencrypted="true"}'
 - Configura el servicio para aceptar conexiones no cifradas.
- winrm set winrm/config/client '@{AllowUnencrypted="true"}'
 - Configura el cliente WinRM para permitir conexiones no cifradas al comunicarse con servidores.

- net localgroup "Remote Management Users" TuUsuario /add
 - Agrega el usuario especificado al grupo local *Remote Management Users*, otorgándole permisos para administrar el servidor de forma remota.
- Usuario administrador
 - Es fundamental configurar una cuenta de usuario que disponga de los permisos y privilegios adecuados para llevar a cabo una evaluación completa del servidor. Este usuario debe tener acceso suficiente no solo para revisar todas las configuraciones y políticas de seguridad, sino también para aplicar los cambios o ajustes necesarios conforme a las recomendaciones. Contar con los privilegios correctos garantiza que el proceso de auditoría y endurecimiento se realice de manera efectiva y sin limitaciones técnicas.

Estas configuraciones son esenciales para habilitar la conectividad remota requerida por la plataforma de evaluación y endurecimiento desarrollada, asegurando que el servidor objetivo sea accesible y gestionable desde la red. Se recomienda realizar estas configuraciones en entornos seguros o de prueba, ya que habilitar la autenticación básica y permitir conexiones sin cifrado puede implicar riesgos de seguridad en ambientes productivos.