Tecnológico de Monterrey

Inteligencia artificial avanzada para la ciencia de datos II (Gpo 101)

Profesor: Félix Ricardo Botello Urrutia

# Actividad 4

# CIS Benchmarks


| | |
|---|---|
| Sofía Cantú Talamantes | A01571120 |
| Ozner Leyva | A01742377 |
| Nallely Serna | A00833111 |
| Fernanda Perez | A01742102 |


Octubre 2024

# *Informe de Cumplimiento de Seguridad en Windows 10 Enterprise*

## *1. Resumen sobre los Benchmarks que ofrece CIS*

El Center for Internet Security (CIS) proporciona Benchmarks las cuales son guías de configuración de seguridad recomendadas para diversas plataformas, estan incluidos sistemas operativos, bases de datos y aplicaciones. Estas guías se desarrollan en conjunto y unanimidad con personas expertas de la industria y se enfocan en la reducción de vulnerabilidades mediante el ajuste de configuraciones predeterminadas.

Para Windows 10 Enterprise, el Benchmark v3.0.0 incluye recomendaciones para mejorar la seguridad en diversas áreas como lo son: contraseñas, políticas de bloqueo de cuentas, control de acceso, auditoría, firewall, y administración de servicios de red. Estas configuraciones son de gran ayuda para prevenir el acceso no autorizado, mejorar la visibilidad de los eventos del sistema y proteger la integridad de los datos.

## *2. Informe de cumplimiento*

El sistema Operativo Analizado es Windows 10 Enterprise. Utiliza las siguientes herramientas para la auditoría:

- SecPol.msc para revisar políticas de seguridad locales.
- Gpedit.msc para editar políticas de grupo.
- Windows Defender y Firewall para evaluar configuraciones de red.
- Comandos en PowerShell para auditar configuraciones específicas del sistema.

<u>Configuraciones de seguridad analizadas</u>

- Política de contraseñas
    - Benchmark: La política recomendada establece que la longitud mínima de contraseñas es de 14 caracteres y debe contar con la habilitación de requisitos de complejidad.
    - Configuración del sistema: La configuración actual del sistema utiliza una contraseña con longitud de 10 caracteres, y no todos los requisitos de complejidad están habilitados.
    - Recomendación: Es recomendado aumentar la longitud mínima de las contraseñas a 14 caracteres y habilitar la complejidad o sea, incluir letras mayúsculas, minúsculas, números y símbolos).
- Política de bloqueo de cuentas
    - Benchmark: Se recomienda que las cuentas se bloqueen después de 5 intentos fallidos de inicio de sesión y que el bloqueo dure al menos 15 minutos.

    - Configuración del sistema: El sistema no cuenta con un límite configurado para los intentos fallidos de inicio de sesión.
    - Recomendación: Configurar el bloqueo de cuentas tras 5 intentos fallidos para poder evitar ataques de fuerza bruta.
- Auditoría de eventos de seguridad
    - Benchmark: Se recomienda habilitar la auditoría de eventos críticos como la validación de credenciales.
    - Configuración del sistema: La auditoría de eventos de inicio de sesión y validación de credenciales no está habilitada.
    - Recomendación: Habilitar la auditoría para los eventos de validación de credenciales y sesiones de usuario para mejorar la capacidad de monitoreo de incidentes de seguridad.
- Configuración del firewall
    - Benchmark: El firewall tiene que estar habilitado en todos los perfiles (dominio, privado y público) y bloquear todas las conexiones entrantes no solicitadas.
    - Configuración del sistema: El firewall está habilitado, pero no bloquea todas las conexiones entrantes no solicitadas.
    - Recomendación: Será necesario ajustar las reglas del firewall para bloquear todas las conexiones entrantes no solicitadas y mejorar la seguridad de la red.

## *3. Hallazgos y Conclusiones*

Después de comparar las configuraciones actuales del equipo con las políticas de hardening recomendadas por el Benchmark de CIS para Windows 10 Enterprise, identificamos las siguientes brechas de seguridad:

- Políticas de contraseñas insuficientes: La longitud y complejidad de las contraseñas no cumplen con los estándares recomendados, lo cual representa una vulnerabilidad frente a ataques de diccionario o fuerza bruta.
- Falta de bloqueo de cuentas: Al no haber una política de bloqueo de cuentas hay más riesgo de intentos de inicio de sesión no autorizados por medio de ataques de fuerza bruta.
- Auditoría limitada: No se están auditando eventos clave, lo que reduce la visibilidad sobre actividades sospechosas en el sistema.
- Firewall no configurado para bloquear conexiones entrantes: Aunque el firewall está habilitado, no se están bloqueando adecuadamente las conexiones entrantes, lo que deja expuesto el sistema a amenazas externas.

Recomendaciones generales

- Ajustar las políticas de contraseñas y bloqueo de cuentas de acuerdo a lo recomendado por el Benchmark para mejorar la seguridad de autenticación.
- Habilitar la auditoría para eventos de inicio de sesión y credenciales, para incrementar la capacidad de detectar posibles intrusiones.
- Configurar el firewall para bloquear conexiones entrantes no solicitadas y reducir la exposición a ataques desde la red.

Estas recomendaciones son prácticas y sencillas y pueden implementarse con las herramientas que ya están disponibles en el sistema operativo Windows 10, sin necesidad de grandes inversiones adicionales en recursos.

# *Referencias*

Center for Internet Security. *CIS Microsoft Windows 10 Enterprise Benchmark*. 22 Feb. 2024. v3.0.0 - 02-22-2024. https://drive.google.com/file/d/15s4CMkxq3K09bzjoBfub1PIyN4RCEQ3H/view?usp=sharing