



# AUDITORÍA DE SEGURIDAD

FERNANDO SOTO  
BRAULIO MARTÍNEZ  
ANTONIO NOEMI  
CHRISTOPH FREITER  
MAX SUASTEGUI



Empresa dedicada a la venta de  
zapatos al mayoreo con más de 20  
años de experiencia.

# Objetivos



Identificar y priorizar vulnerabilidades en los activos tecnológicos identificados.



Evaluar y fortalecer la seguridad de la infraestructura tecnológica para protegerla contra amenazas.



Garantizar la continuidad de las operaciones comerciales y la integridad y confidencialidad de la información crítica y sensible.





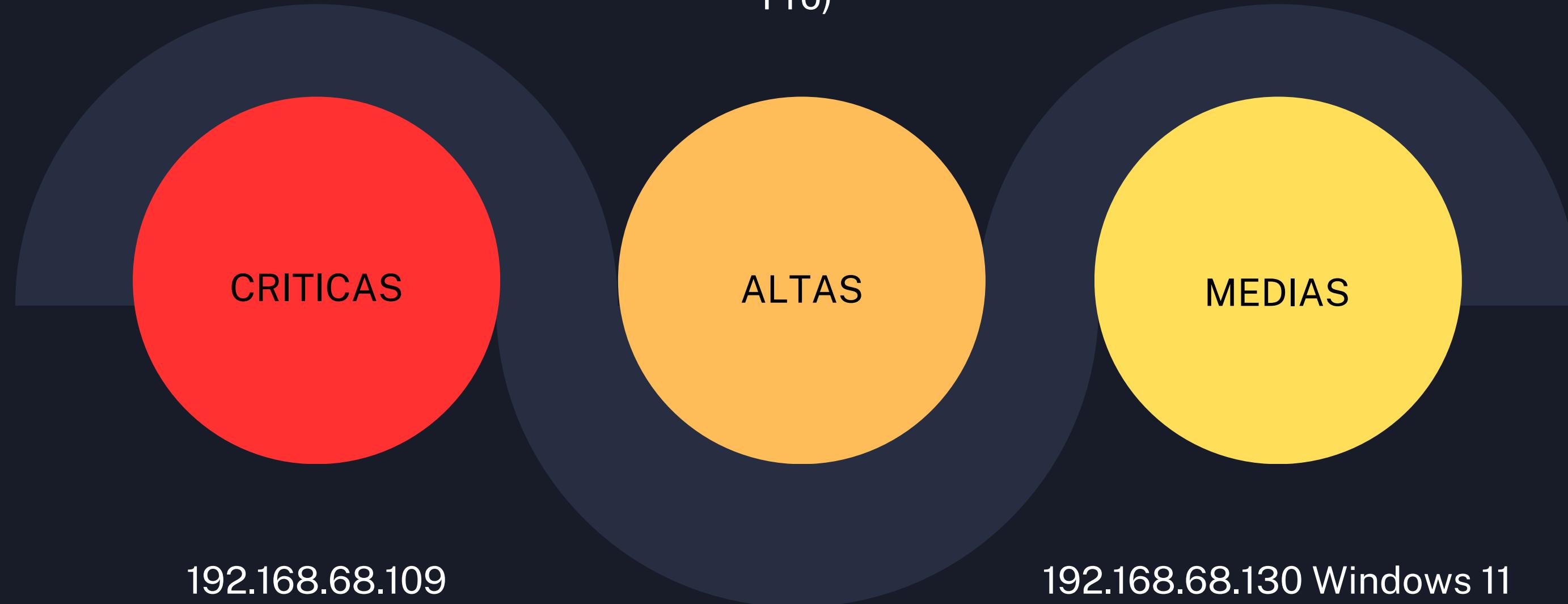
Nessus®  
vulnerability scanner

# Metodología

- 1 Identificación de vulnerabilidades
- 2 Evaluación de vulnerabilidades
- 3 Análisis y reporte de vulnerabilidades
- 4 Mitigación

# Vulnerabilidades

192.168.68.129  
(Microsoft  
Windows 8.1  
Pro)



192.168.68.109  
(Microsoft  
Windows 7  
Ultimate)

192.168.68.130 Windows 11

# SOLUCIONES

## CRITICAS

- Actualizar a una versión compatible y compatible con parches de seguridad

## ALTAS

- Aplicar el parche de seguridad MS17-010 y deshabilitar SMBv1 si no es necesario.

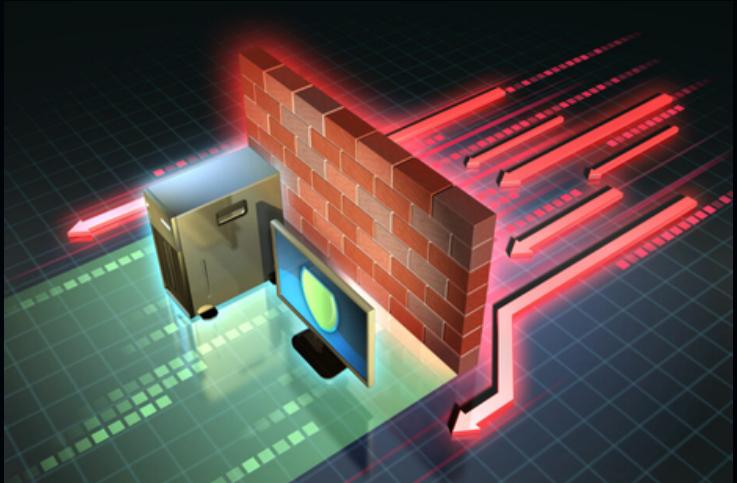
## MEDIAS

- Verificar la validez del certificado SSL y corregir la cadena de certificados según sea necesario

# PLAN MITIGACIÓN

## Firewalls

Configurar firewalls para restringir el acceso no autorizado a los servicios y recursos de red.



## Políticas de acceso

Crear políticas de acceso para limitar los privilegios de usuario y restringir el acceso a recursos e información sensibles.



# PLAN MANTENIMIENTO

GESTIÓN DE  
PARCHES

FORMACIÓN Y  
CONCIENTIZACIÓN

PLAN DE  
RESPUESTA A  
INCIDENTES

ACTUALIZACIÓN  
DE POLÍTICAS  
DE SEGURIDAD

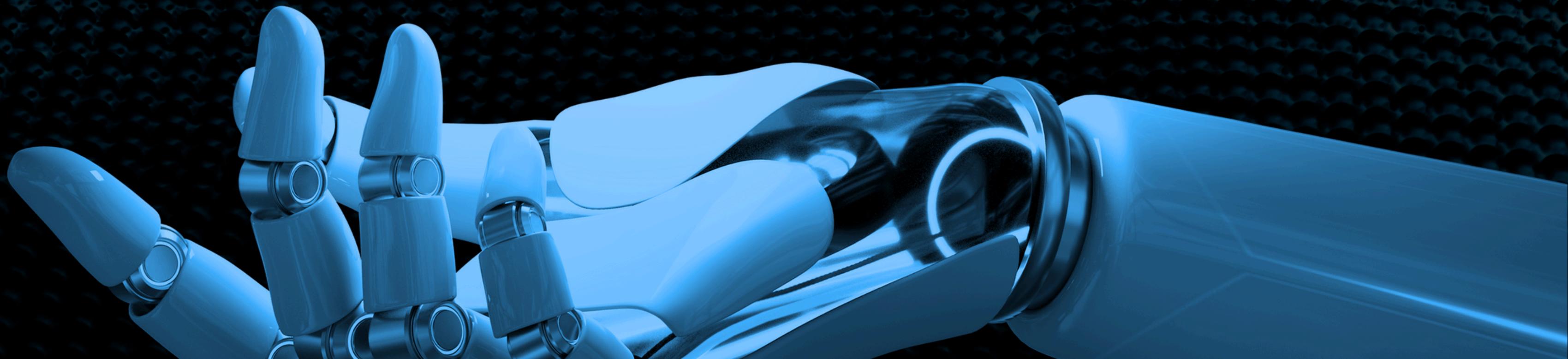
# EVALUACIÓN FINAL

**Nessus a veces muestra falsos errores en el tipo de vulnerabilidad Unsupported Windows OS (remote).**

Como fue en este caso de los host 192.168.68.109 (Microsoft Windows 7 Ultimate), 192.168.68.129 (Microsoft Windows 8.1 Pro) y 192.168.68.123 (Microsoft Windows 8.1 Pro) que supuestamente compartían la misma vulnerabilidad (Windows 10 ya había sido instalado)

**Las siguientes vulnerabilidades ya fueron solucionadas con windows 10:**

- S17-010: Security update for Microsoft Windows
- SMB server
- SMB Signing not required
- MS16-047



# CONCLUSIONES

Se identificaron varias vulnerabilidades que ya habían sido abordadas de manera indirecta, esto con actualizaciones automáticas de los propios equipos.

Las vulnerabilidades relacionadas con los certificados SSL no requerían de atención inmediata

Próximos pasos:

- Monitorear y evaluar continuamente la seguridad de la red.
- Actualizar las políticas y procedimientos de seguridad según sea necesario.
- Invertir en capacitación y educación continua en ciberseguridad para los empleados.