



INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

# Auditoría de seguridad y Plan de Mitigación: Caso negocio en Facebook Marketplace

## ANÁLISIS DE CRIPTOGRAFÍA Y SEGURIDAD

Escuela de Ingeniería y Ciencias

Carrera: Ingeniería en Ciencia de Datos y Matemáticas

### SOCIO FORMADOR: TECNOGAM

Equipo 5:

Luis Ángel López Chávez | A01571000

Karla Andrea Palma Villanueva A01754270

Sarah Dorado Romo | A01540946

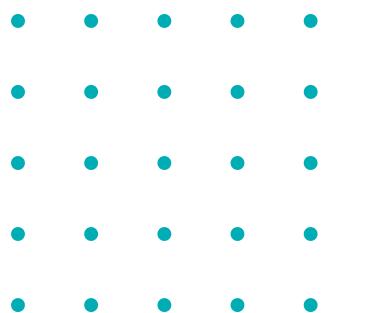
Adrián Pineda Sánchez | A00834710

Gerardo Juárez Hernández | A01732799

Salvador Vidal Torres | A01732983

• • • •  
• • • •  
• • • •  
• • • •  
• • • •

# CONTENIDO



Introducción



Levantamiento de inventario



Plan de evaluación



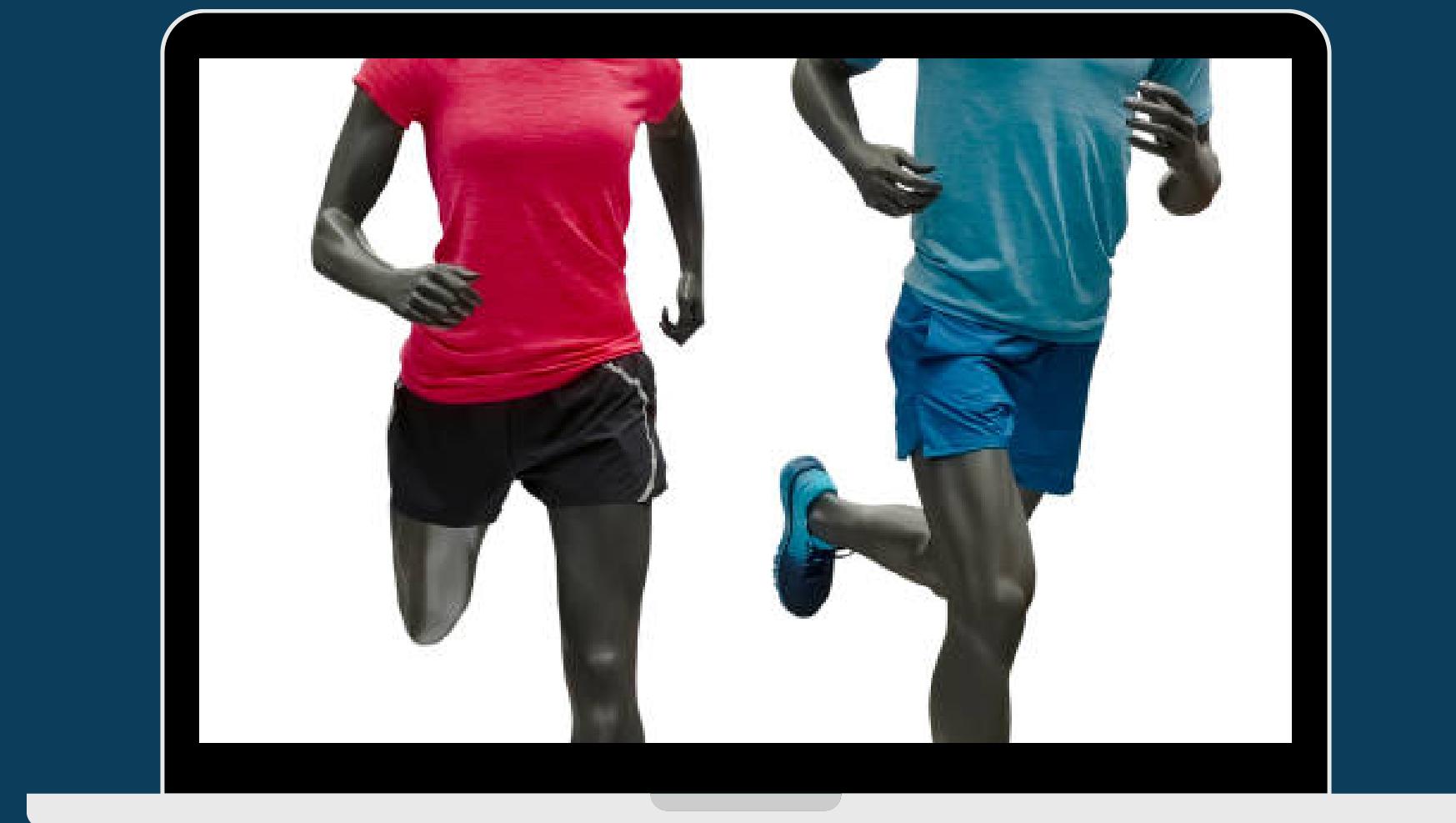
Plan de mitigación



Conclusiones



# INTRODUCCIÓN



## DISPOSICIÓN

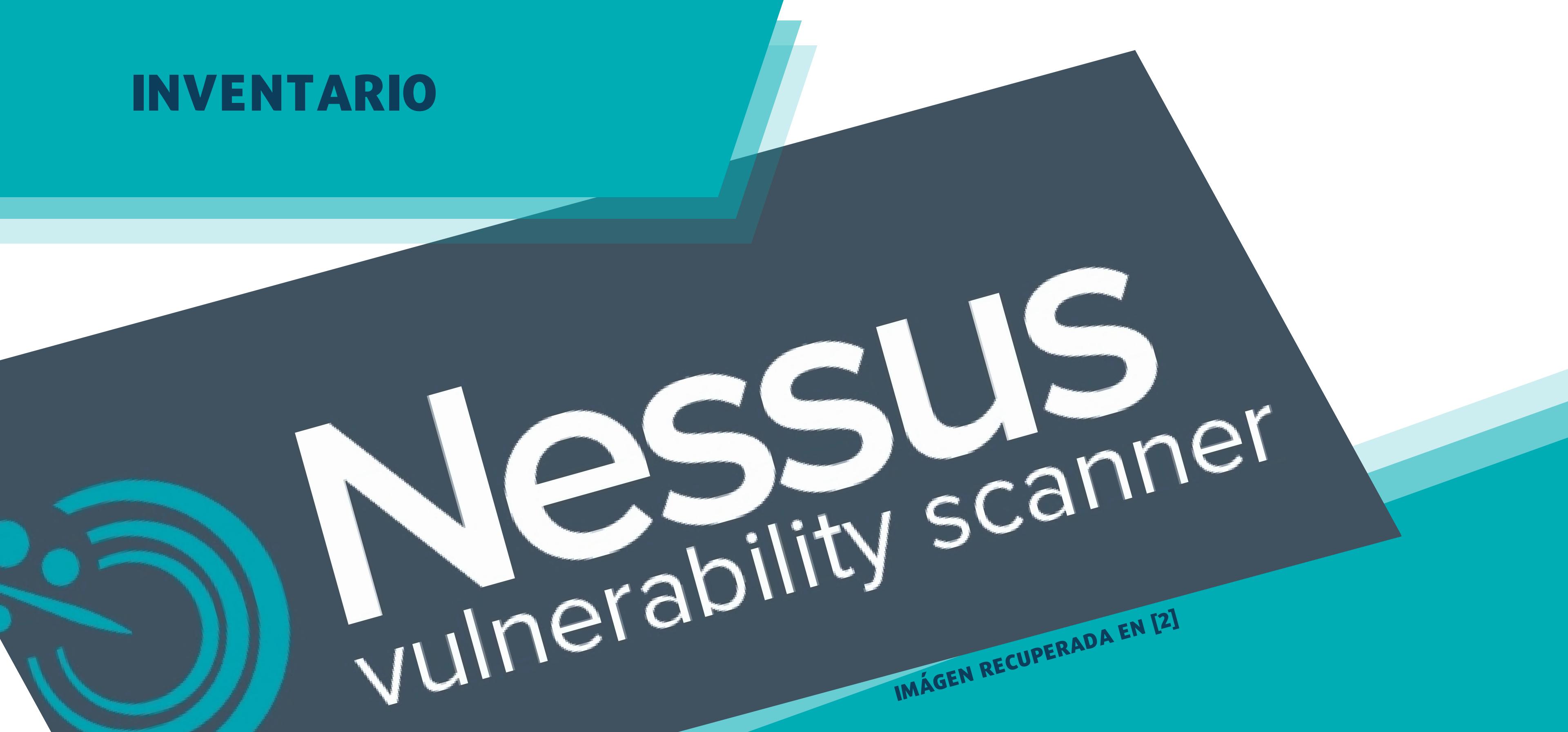
2800 MXN

AL AÑO



## ◆ HERRAMIENTAS UTILIZADAS

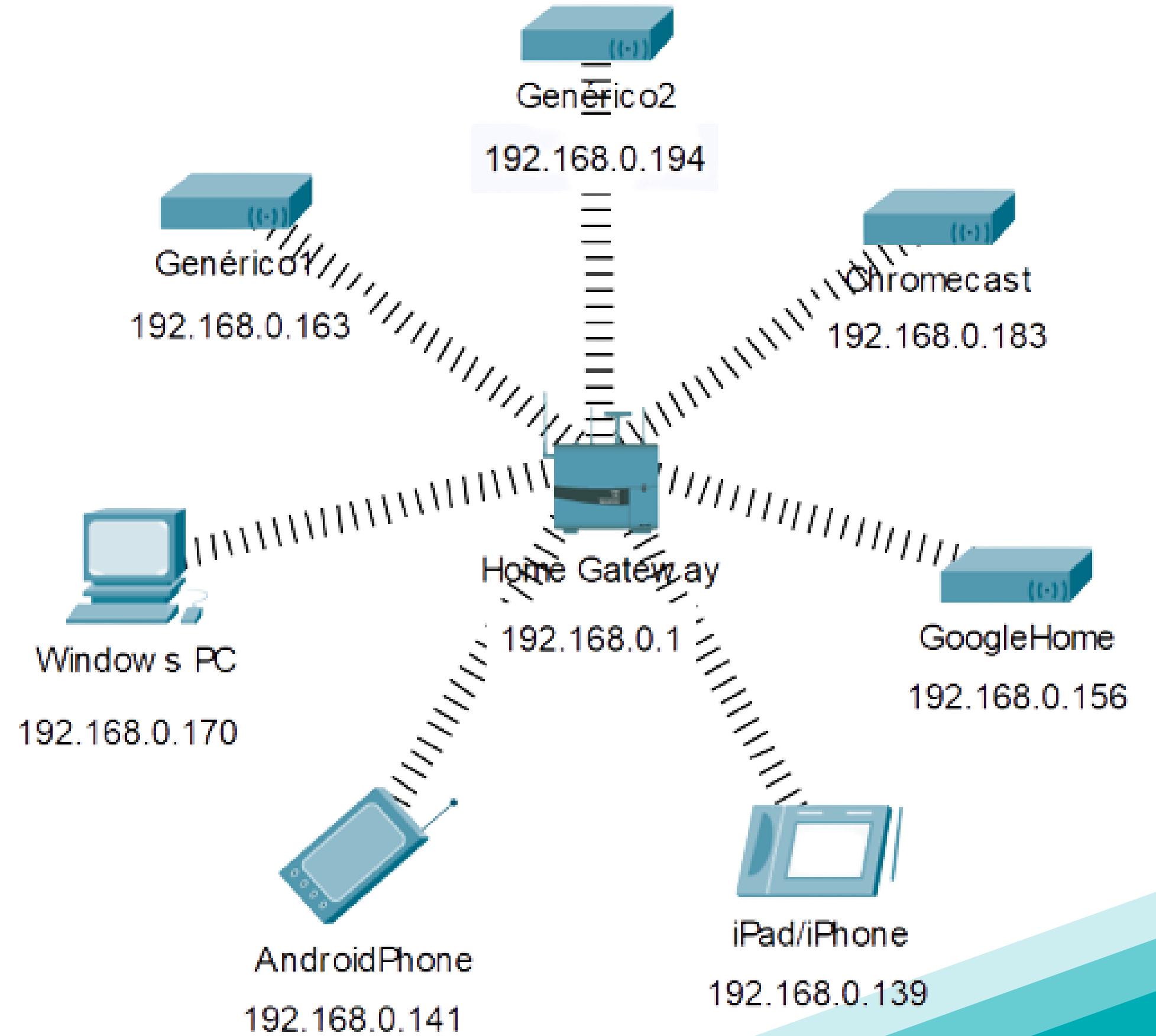
### INVENTARIO



**Nessus**  
vulnerability scanner

IMÁGEN RECUPERADA EN [2]

◆ CÓMO SE CONECTA LA RED  
**TOPOLOGÍA**



## VULNERABILIDADES [2]

### DISPOSITIVOS

HOME  
GATEWAY

Host: 192.168.0.1



IPAD O  
IPHONE

Host: 192.168.0.139



CELULAR  
ANDROID

Host: 192.168.0.141



GOOGLE  
HOME

Host: 1192.168.0.156



## VULNERABILIDADES [2]

# DISPOSITIVOS

**GENÉRICO 1**

Host: 192.168.0.163



**WINDOW'S  
PC**

Host: 192.168.0.170



**CHROMECAST**

Host: 192.168.0.183



**GENÉRICO 2**

Host: 192.168.0.194



# PLAN DE EVALUACIÓN



# ROUTER/MÓDEM

192.168.0.1

VULNERABILIDAD (Clave CVE, Nessus Plugin ID) [2]	CALIFICACIÓN CVSS	DESCRIPCIÓN [2]
20007	9.8	<b>Versión de SSL vulnerable a fallas de criptoseguridad.</b>
CVE-2016-7406 CVE-2016-7407 CVE-2016-7408 CVE-2016-7409	9.8	<b>Versión de Dropbear SSH anterior a ver. 2016.72 el cual es vulnerable a ataques</b>
CVE-2013-4421 CVE-2013-4434	5.0	<b>Versión de Dropbear SSH anterior a ver. 2013.59 el cual es vulnerable a ataques conocidos con los CVE anteriores</b>
CVE-2016-2183	7.5	<b>Uso de cifrados SSL de mediano nivel de encriptación</b>
51192	6.5	<b>No se puede confiar en el certificado SSL</b>



VERSIONES  
ANTICUADAS



# ROUTER/MÓDEM

192.168.0.1

VULNERABILIDAD (Clave CVE, Nessus Plugin ID) [2]	CALIFICACIÓN CVSS [2]	DESCRIPCIÓN [2]
<b>CVE-2013-2566</b> <b>CVE-2015-2808</b>	<b>5.9</b>	<b>Versión de SSL soporta el sistema de cifrado RC4 el cual tiene fallas en la generación de bytes pseudo-aleatorios.</b>
<b>12217</b>	<b>5.3</b>	<b>El servidor de DNS vulnera el caché haciendo que fisgones puedan averiguar cuando se visita una página web.</b>
<b>104743</b>	<b>6.5</b>	<b>Protocolo TLS 1.0 el cual antigua con vulnerabilidades</b>
<b>157288</b>	<b>6.5</b>	<b>Soporta el protocolo TLS 1.1 el cual carece de sistemas de cifrado recomendados.</b>
<b>153953</b>	<b>3.7</b>	<b>El servidor SSH permite uso de algoritmos de intercambio de llaves de encriptación débiles</b>



# GOOGLE HOME

192.168.0.156

VULNERABILIDAD (Clave CVE, Nessus Plugin ID) [2]	CALIFICACIÓN CVSS	DESCRIPCIÓN [2]
<b>CVE-2016-2183</b>	7.5	<b>Soporta cifrados de SSL con un mediano nivel de encriptación</b>
<b>51192</b>	6.5	<b>No se puede confiar en el certificado SSL</b>
<b>57582</b>	6.5	<b>El certificado SSL no fue reconocida por una autoridad</b>
<b>104743</b>	6.5	<b>Protocolo TLS 1.0 el cual ya es antigua y conocida por tener vulnerabilidades de ataques conocidos.</b>
<b>157288</b>	6.5	<b>Soporta el protocolo TLS 1.1 el cual carece de sistemas de cifrado recomendados.</b>

# GENÉRICO 1

192.168.0.163

VULNERABILIDAD (Clave CVE, Nessus Plugin ID )	CALIFICACIÓN CVSS	DESCRIPCIÓN [2]
<b>CVE-2016-2183</b>	<b>7.5</b>	<b>SSL soporta cifrados de nivel medio y vulnerable a ataques conocidos.</b>
<b>51192</b>	<b>6.5</b>	<b>No se puede confiar en el certificado SSL</b>
<b>57582</b>	<b>6.5</b>	<b>El certificado SSL no fue reconocida por una autoridad</b>
<b>42263</b>	<b>6.5</b>	<b>Se usa protocolo Telnet sobre un canal sin encriptar</b>
<b>CVE-2020-11022</b> <b>CVE-2020-11023</b>	<b>6.1</b>	<b>Versión de librería JQuery vulnerable a ataques de script mediante sitios web</b>
<b>104743</b> <b>157288</b>	<b>6.5</b>	<b>Protocolo TLS 1.0 y 1.1 los cuales son antiguas con vulnerabilidades</b>



# PC WINDOWS

192.168.0.170

VULNERABILIDAD (Clave CVE, Nessus Plugin ID )	CALIFICACION CVSS	DESCRIPCIÓN [2]
57608	5.3	<b>No es necesario firmar en el servidor SMB remoto.</b>



# GOOGLE CHROMECAST

192.168.0.183

VULNERABILIDAD (Clave CVE, Nessus Plugin ID )	Calificación CVSS	DESCRIPCIÓN [2]
CVE-2004-2761	7.5	<b>Facilita que los atacantes dependientes del contexto realicen ataques de suplantación de identidad</b>
CVE-2016-2183	7.5	<b>Facilita que los atacantes remotos obtengan datos de texto claro</b>
51192	6.5	<b>No se puede confiar en el certificado SSL para este servicio.</b>
57582	6.5	<b>La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.</b>
104743	6.5	<b>El servicio remoto encripta el tráfico utilizando una versión anterior de TLS.</b>

# SIN VULNERABILIDADES

## GENÉRICO 2

◆ 192.168.0.193

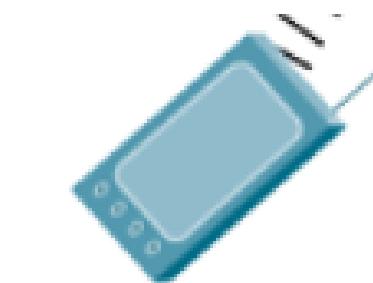


Genérico2

192.168.0.194

## CELULAR ANDROID

◆ 192.168.0.141

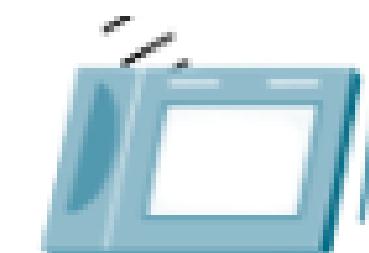


AndroidPhone

192.168.0.141

## IPAD/ IPHONE

◆ 192.168.0.139



iPad/iPhone

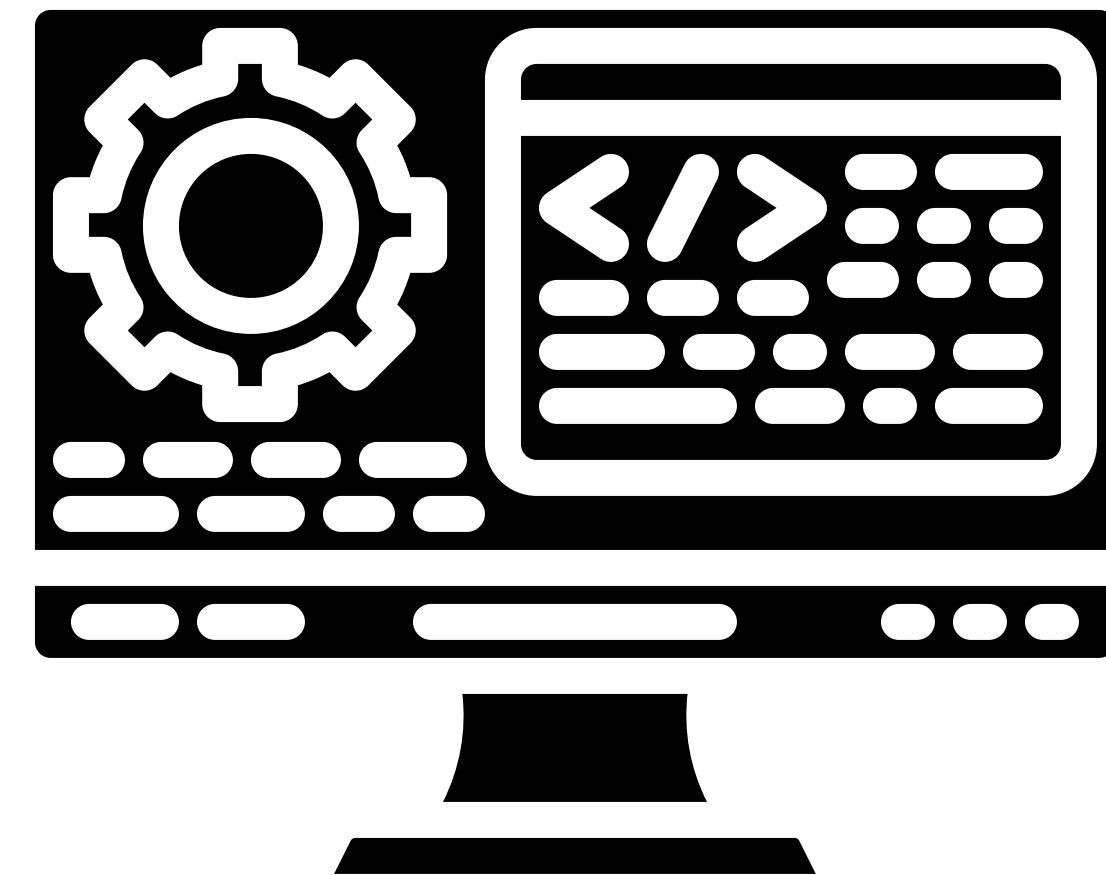
192.168.0.139



# ANALISIS DE RIESGOS Y ATAQUES



**FISGÓN**  
(MAN IN THE MIDDLE) [2]



**INYECCIÓN DE CÓDIGO**  
CROSS-SITE SCRIPTING (XSS) [2]



# PLAN DE MITIGACION

---



PUNTOS DEL PLAN



ENFOQUE



COSTOS

# PUNTOS DEL PLAN DE MITIGACION

1

MODIFICAR  
REGISTRO DE  
WINDOWS

2

USO DE VPN

3

CONFIGURACIÓN  
DE ACCESS LIST

4

DESACTIVAR EL  
USO DE  
PROTOCOLO  
TELNET

5

HABILITAR USO  
DE SSH

6

FIRMA DE  
SEGURIDAD DE  
WINDOWS

7

ACTUALIZACIÓN  
DE TODOS LOS  
DISPOSITIVOS EN  
LA RED

7

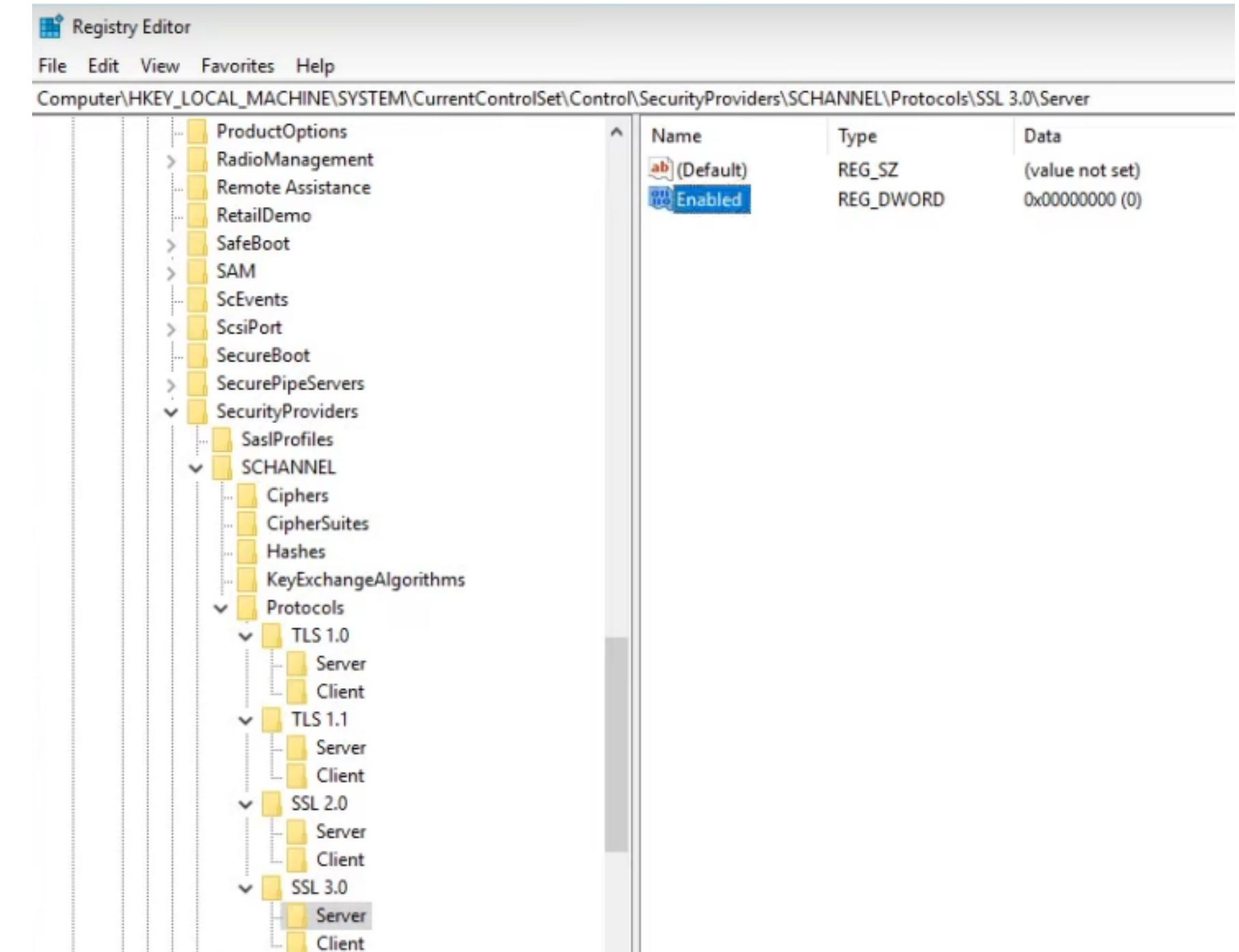
AUTENTICACION  
MEDIANTE SMB



PUNTOS

# REGRISTRO DE WINDOWS [9]

- Desactivar el uso de protocolos obsoletos en aplicación Editor de Registro en Windows



Ejemplo de cambio de registros [9]

## ◆ PUNTOS

# USO DE VPN [8]

---

- Transmite los datos hacia redes públicas de forma segura y anónima, se ocultan las IP de los usuarios, cifra los datos para que solamente sean recibidos y descifrados por el dispositivo con autorización.

• • • • •  
• • • • •  
• • • • •  
• • • • •  
• • • • •



◆ PUNTOS

## USO DE ACCESS LIST[9]

---

- Barrera de seguridad entre la red interna y el internet que inspecciona el tráfico de red y utiliza blacklists y whitelists para indicar las IP autorizadas para acceder a la red.

• • • • •  
• • • • •  
• • • • •  
• • • • •  
• • • • •





PUNTOS

## DEACTIVAR PROTOCOLO

### TELNET[10]

- El protocolo Telnet se utiliza comúnmente para el acceso remoto a un servidor o dispositivo, y permite al usuario conectarse y utilizar los servicios o aplicaciones del servidor como si estuviera físicamente presente en el mismo lugar que el servidor.



• • • •  
• • • •  
• • • •

## ◆ PUNTOS

# HABILITAR USO DE SSH [11]

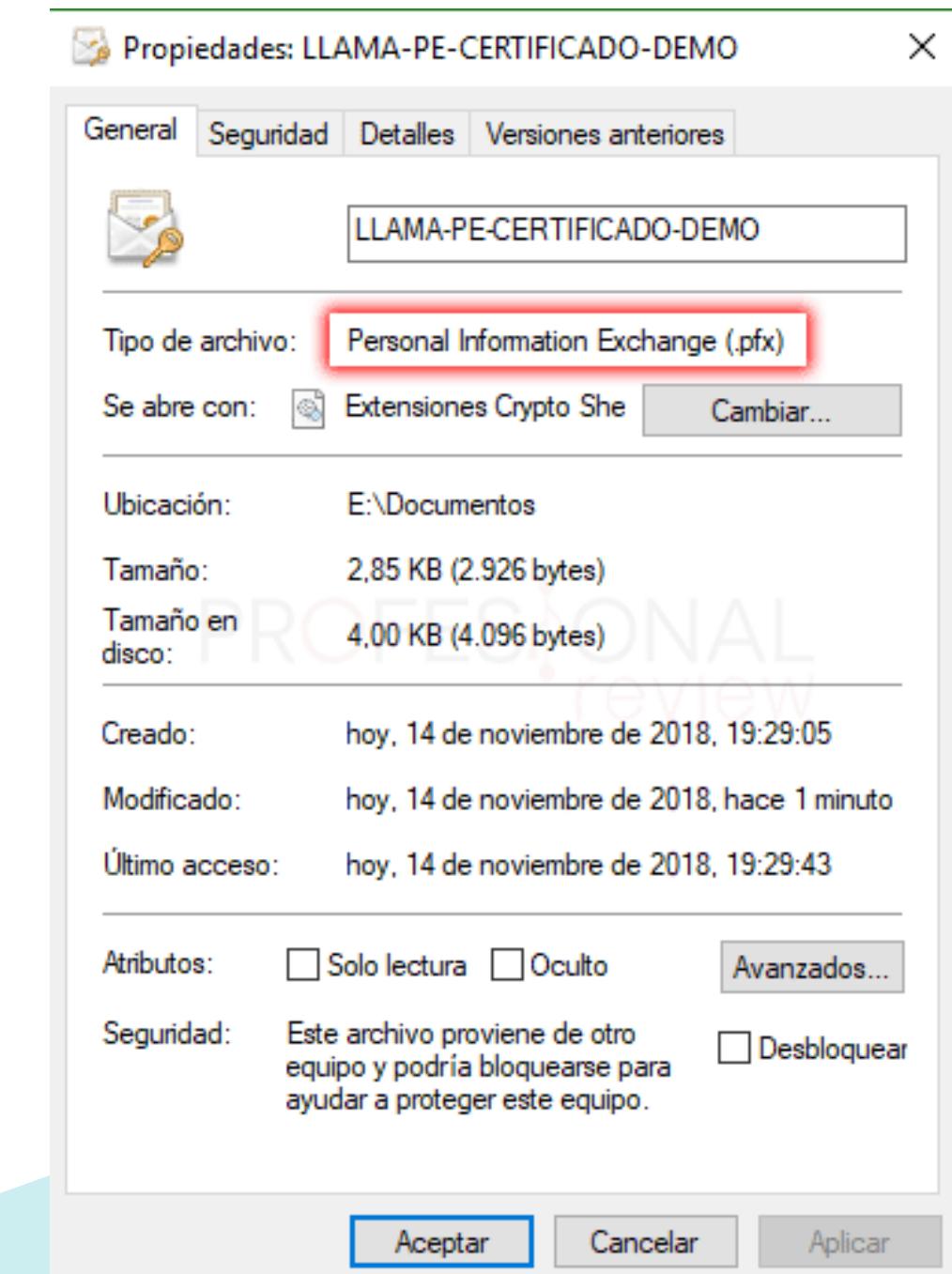
- El soporte del protocolo Telnet también conocido por no contar con ninguna encriptación en el momento de enviar los paquetes, por lo que deshabilitar esta opción y, en cambio, habilitar el protocolo SSH sería la solución.



## ◆ PUNTOS

# FIRMA DE SEGURIDAD DE WINDOWS[12]

- La firma de seguridad es una firma digital que se aplica a los archivos de software para garantizar que el archivo no ha sido modificado o alterado desde que fue firmado digitalmente por el desarrollador del software.





## PUNTOS

# ACTUALIZACIÓN DE TODOS LOS DISPOSITIVOS EN LA RED [4]

- La actualización de los protocolos a sus versiones más recientes, previene vulnerabilidades relacionadas con la antigüedad y el hallazgo de las mismas que ya fueron corregidas por los proveedores de servicios.

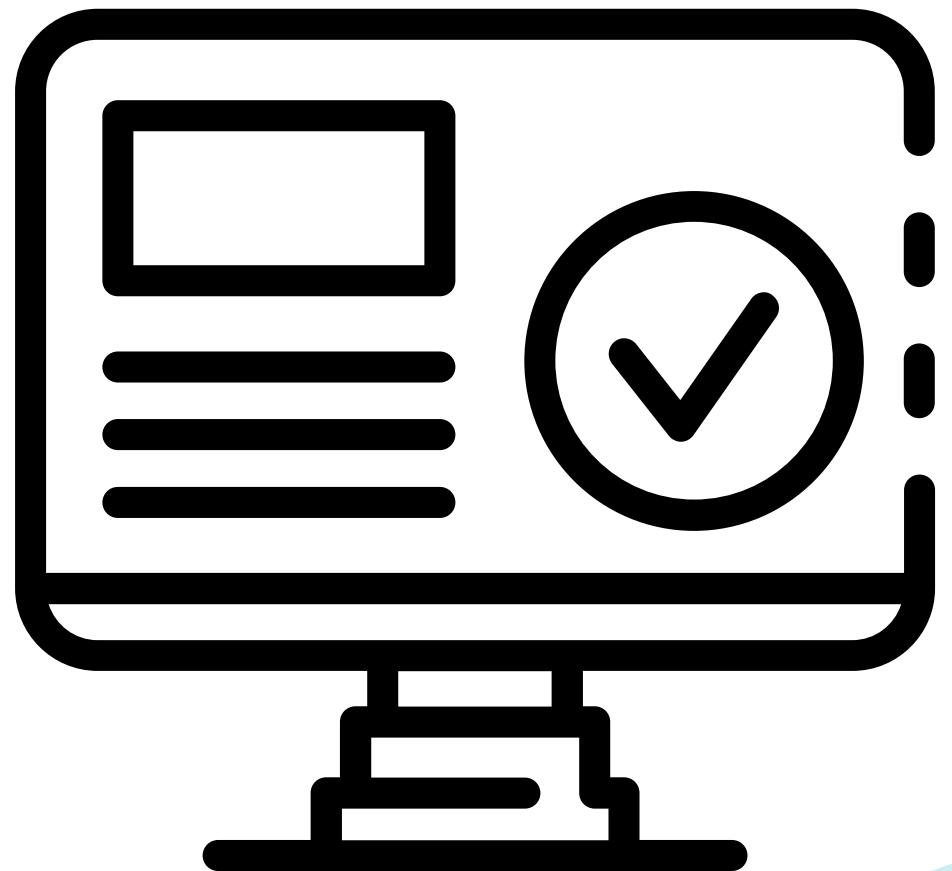


• • • • •  
• • • • •  
• • • • •  
• • • • •  
• • • • •

## ◆ PUNTOS

# AUTENTICACION POR SMB [4]

- SMB (Server Message Block) Proporciona seguridad y control en cuestión del acceso autorizado a la información y recursos compartidos.
- Esencial para la seguridad entre cliente y servidor.



• • • • •  
• • • • •  
• • • • •  
• • • • •  
• • • • •  
• • • • •

# ENFOQUE

La prioridad al analizar las vulnerabilidades encontradas es mantener todos los dispositivos y software actualizados. Esto evita las siguientes amenazas:

Uso de algoritmos de cifrado e implantacion anticuados

Fallas en el protocolo SSL susceptibles a ataques comunes.

Ataques tipo "man in the middle" para interceptar y desencriptar informacion



# COSTOS

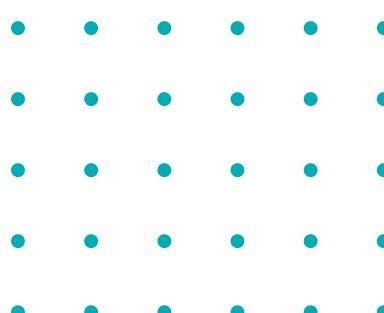
Servicio	Duración de la suscripción	Costo
VPN	Dos años	\$1,000 mxn
Antivirus (50 dispositivos)	Tres años	\$2,300 mxn
Windows Server Essentials (opcional en caso de ser requerido)	Única compra	\$7,500mxn



# RESULTADOS

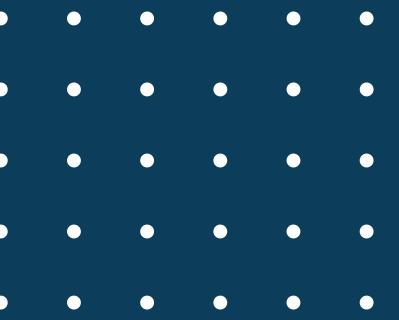
27/28

VULNERABILIDADES  
RESUELTA



# REFERENCIAS

1. Lizarazo, C. (30 de enero de 2023) Las PyMEs en México: Retos e importancia. Conekta. Recuperado el 23 de febrero de 2023, de: <https://www.conekta.com/blog/las-pymes-en-mexico-retos-e-importancia>
2. Tenable Network Security, Inc. (s.f.). Nessus [Software] <https://www.tenable.com/products/nessus>
3. Canva Pty Ltd (s.f.). Canva [Software] <https://www.canva.com/>
4. Microsoft. (2022, September 21). Información general sobre el protocolo SMB y el protocolo CIFS de Microsoft - Win32 apps. Microsoft.com. <https://learn.microsoft.com/es-es/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview>
5. Microsoft. (s.f.). Manage Windows Server Essentials. Learn. Recuperado el 9 de marzo de 2023, de: <https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-windows-server-essentials>
6. Kemmerer, C. (s.f.) Desactive SSL 3.0 y TLS 1.0 en su navegador- SSL.com. Recuperado el 8 de marzo de 2023, de: <https://www.ssl.com/es/c%C3%B3mo/apague-ssl-3-0-y-tls-1-0-en-su-navegador/>
7. [InfoSec Governance] (febrero de 2016). How to disable SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 in Windows 10. [Video]. YouTube. Recuperado el 8 de marzo de 2023, de: <https://www.youtube.com/watch?v=oh2gfGYoytw>



# REFERENCIAS

- 8 Cisco Systems, Inc. (s.f.). What is a VPN? Cisco. Recuperado el 9 de marzo de 2023, de:  
<https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>
- 9 [InfoSec Governance] (febrero de 2016). How to disable SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 in Windows 10. [Video]. YouTube. Recuperado el 8 de marzo de 2023, de: <https://www.youtube.com/watch?v=oh2gfGYoytw>
- 10 McAfee. (15 de mayo de 2020). ¿Qué es un firewall?. Recuperado el 9 de Marzo de 2023, de  
<https://www.mcafee.com/es-mx/antivirus/firewall.html>
- 11 Eleventa (s.f.) Pruebas de conexión Telnet en windows. Recuperado el 11 de marzo de 2023, de:  
<https://eleventa.com/aprender/conexion-telnet>
- 12 Johnston, M. (14 de noviembre de 2022) Dropbear SSH. Recuperado el 11 de marzo de 2023, de:  
<https://matt.ucc.asn.au/dropbear/dropbear.html>

• • • • •  
• • • • •  
• • • • •  
• • • • •  
• • • • •

