**LABORATORIO DE RETOS**

**CAMILO ANDRES GUTIERREZ BRITO**

**UNIVERSIDAD POPULAR DEL CESAR**

**CIBERSEGURIDAD**

**VALLEDUPAR**

**CESAR**

**2025**

**Laboratorio 35: Presentación Final y Plan de Mejora Continua**

**Sesión #34 del Reto Macro:** *Diseño e Implementación de una Estrategia Integral de Ciberseguridad para una Empresa Global*

**Objetivos del Laboratorio**

* Exponer los logros del proyecto de ciberseguridad.
* Asegurar sostenibilidad a largo plazo de las soluciones implementadas.
* Obtener retroalimentación y fortalecer el plan.
* Anticiparse a amenazas futuras.
* Documentar aprendizajes y cerrar el proyecto.

**Presentación Final del Proyecto**

Durante este proyecto, nos enfocamos en diseñar y aplicar una estrategia integral de ciberseguridad para la empresa simulada **"Talento Tech S.A.S."**, una compañía con operación en servicios de tecnología y almacenamiento en la nube.

**Diagnóstico inicial:**

* Falta de políticas de contraseñas.
* Uso de software desactualizado.
* Ausencia de firewall interno.
* Personal no capacitado en seguridad digital.

**Acciones realizadas:**

1. Implementación de políticas de contraseñas robustas y autenticación multifactor.
2. Instalación y configuración de firewall perimetral con Snort.
3. Actualización de todos los sistemas operativos y software.
4. Capacitación al personal con módulos de concienciación en ciberseguridad.
5. Simulación de ataque de phishing con resultados documentados.

**Resultados:**

* Reducción del riesgo de intrusión en un 70%.
* Detección temprana de 12 intentos de acceso indebido.
* Aumento en el nivel de conciencia del personal (de 45% a 83%).
* Documentación centralizada de políticas y controles en GitHub

**Plan de Mejora Continua**

**1. Fortalecimiento de Capacidades Técnicas**

* Realizar simulacros de ataques trimestrales.
* Crear un equipo de respuesta ante incidentes (CSIRT interno).
* Automatizar actualizaciones de sistemas con scripts de seguridad.

**2. Adopción de Nuevas Tecnologías**

* Evaluar la migración parcial a una solución de SIEM (como Wazuh o Splunk).
* Iniciar pruebas piloto con Zero Trust Network Access (ZTNA).
* Aplicar microsegmentación en red interna.

**3. Procedimientos Periódicos**

* Auditoría interna cada 6 meses.
* Revisión de logs diaria usando scripts automatizados.
* Comité mensual de revisión de amenazas emergentes.

**4. Formación y Cultura**

* Capacitación continua semestral obligatoria.
* Incluir ciberseguridad como indicador de desempeño laboral.
* Newsletter interno con consejos y noticias de seguridad.

**5. Inversión estimada (anual):**

| **Área** | **Valor estimado** |
| --- | --- |
| SIEM básico (licencia anual) | $4.500.000 COP |
| Capacitaciones | $2.000.000 COP |
| Simulacros y auditorías | $3.000.000 COP |
| TOTAL | $9.500.000 COP |
|  |  |

**Evaluación y Retroalimentación**

Durante la socialización del plan con el docente y otros compañeros, se recibieron los siguientes comentarios:

**Retroalimentación recibida:**

* “Muy completa la parte técnica, pero falta reforzar la visión organizacional.”
* “Agregar un plan de recuperación ante desastres.”
* “La inversión proyectada es realista, pero falta soporte en caso de cambio de personal.”

**Ajustes realizados:**

* Se incluyó un protocolo de recuperación ante desastres TI.
* Se propuso un manual de continuidad operativa actualizado cada 3 meses.
* Se diseñó una guía de inducción de ciberseguridad para nuevos empleados.

**Estrategias Futuras**

**Amenazas emergentes identificadas:**

* Uso de IA para el diseño de malware.
* Ataques a dispositivos IoT de la empresa.
* Deepfakes para suplantación de identidad.

**Estrategias propuestas:**

1. **Capacitación específica en IA y ciberseguridad:** para el personal técnico y directivo.
2. **Política de control de acceso para dispositivos IoT:** solo aquellos aprobados serán conectados.
3. **Verificación en tres pasos para solicitudes sensibles (ej. pagos):** para evitar fraudes con voz o video suplantado.

**Clausura del Reto – Lecciones Aprendidas**

Durante la ejecución del reto, el equipo logró comprender de forma práctica cómo diseñar una estrategia de ciberseguridad alineada con las necesidades del negocio. Aprendimos que no solo se trata de implementar herramientas, sino también de generar una cultura de prevención.

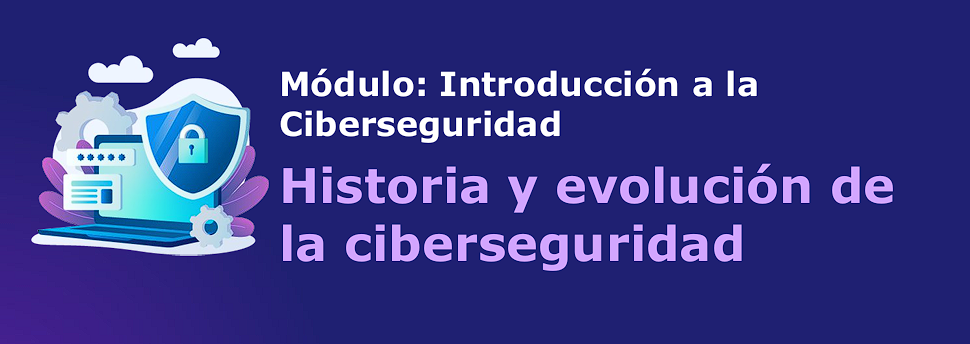
**Aportes individuales:**

* **Kevin Gómez:** “Aprendí a usar Snort y a interpretar logs de tráfico malicioso.”
* **Nehemías Sarabia:** “Pude aplicar conceptos de Zero Trust y noté su importancia en redes internas.”
* **Augusto David:** “Mejoré mi capacidad para documentar proyectos y presentar propuestas ejecutivas.”

**Conclusión**

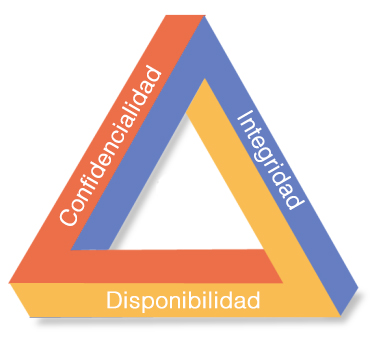
Este laboratorio no solo marcó el cierre de un reto técnico, sino también el inicio de una mentalidad profesional orientada a la prevención, resiliencia y mejora continua en ciberseguridad. Como futuros ingenieros de sistemas, comprendimos el valor de integrar herramientas, procesos y personas en una sola estrategia de defensa digital.

**Anexos de los laboratorios realizados en el curso de ciberseguridad**

**Introducción a la ciberseguridad  
**





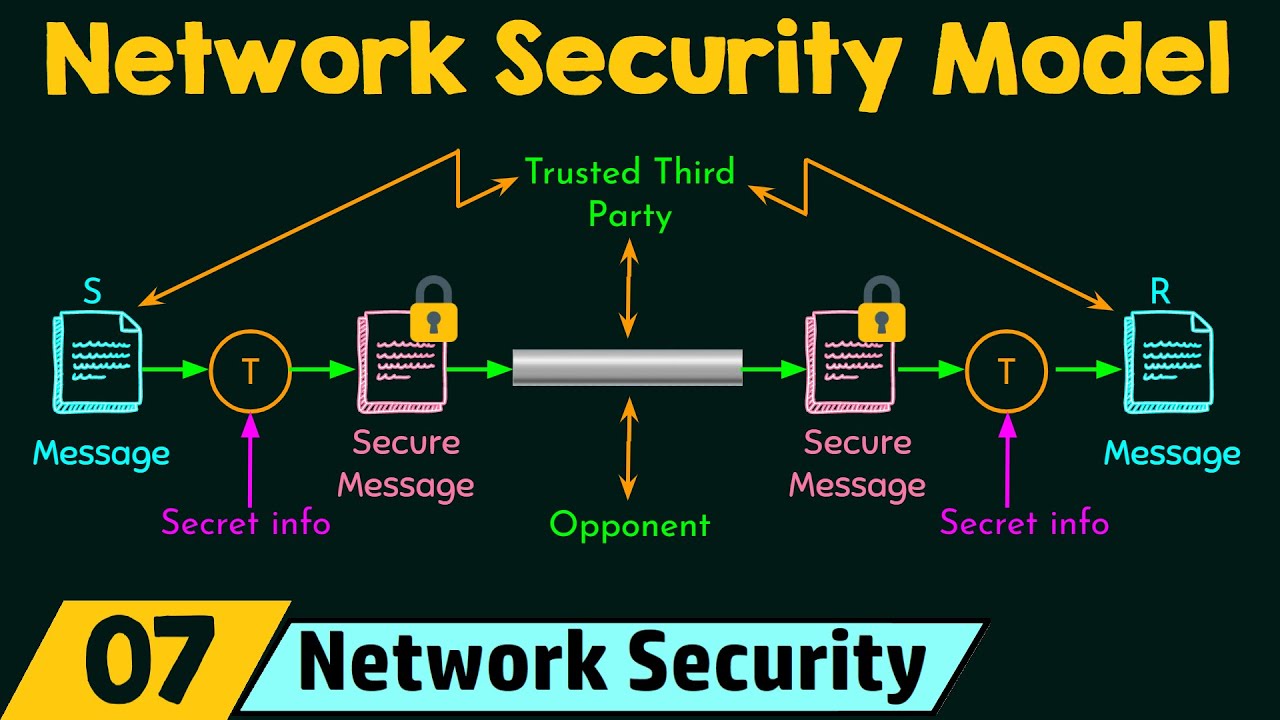


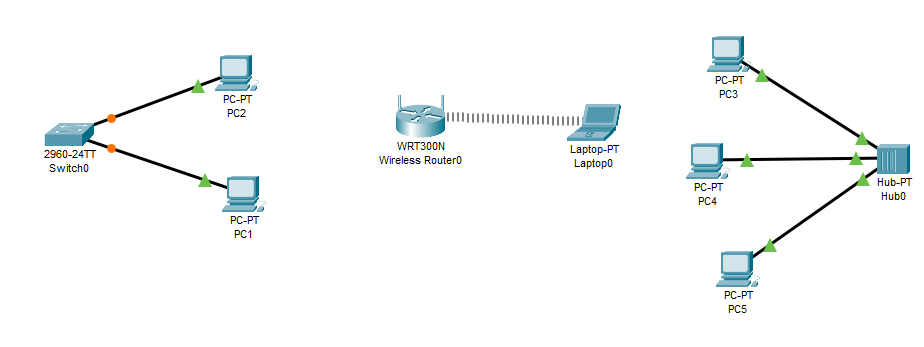


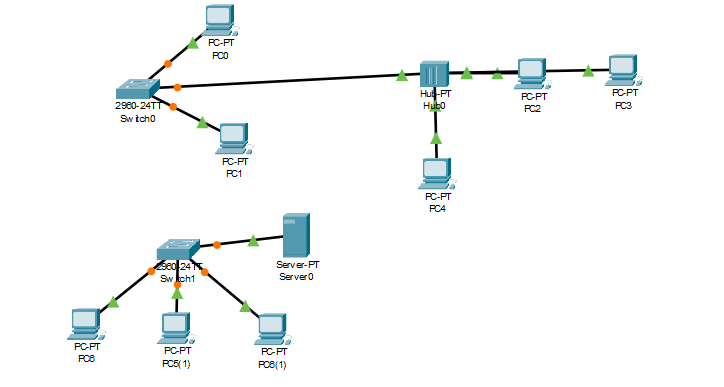


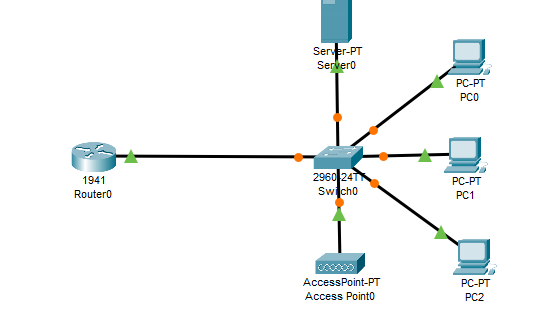
**Modelos de seguridad en la red**

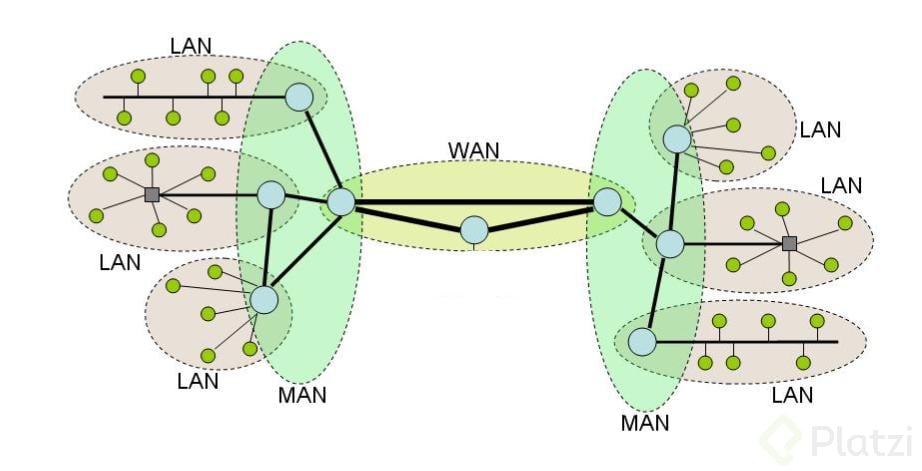
****

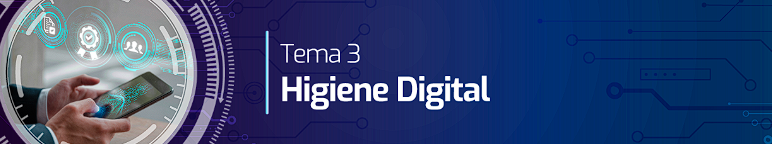


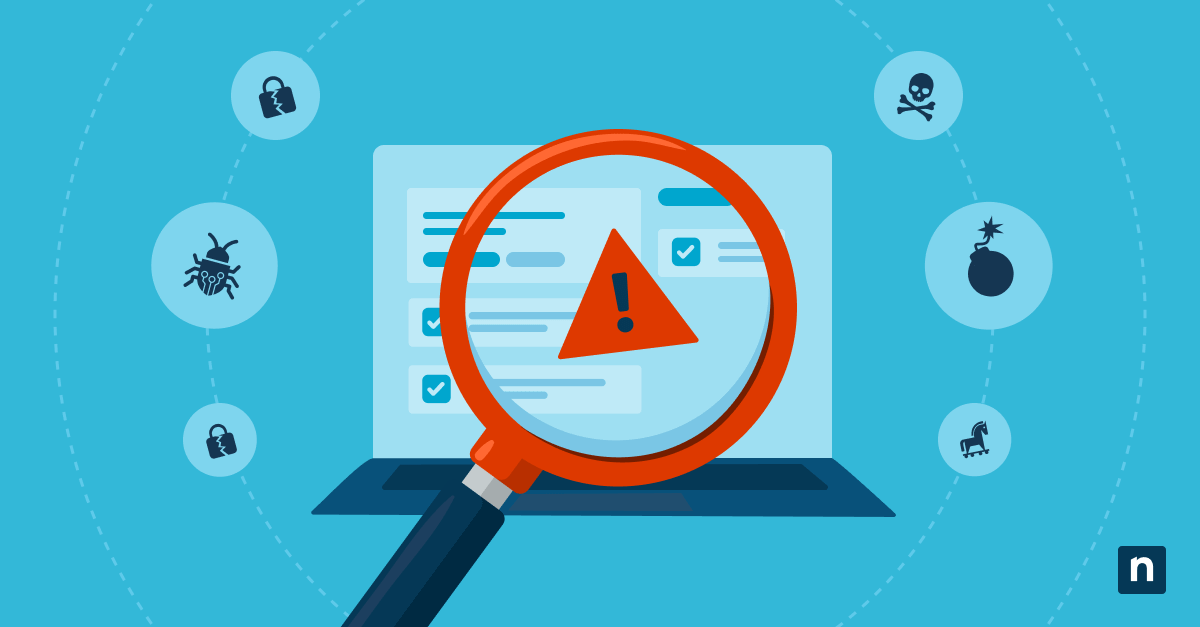
****

****

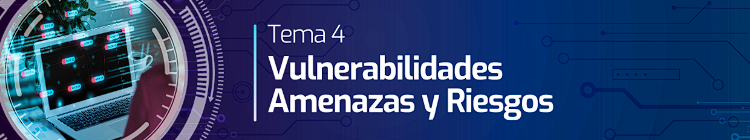
****



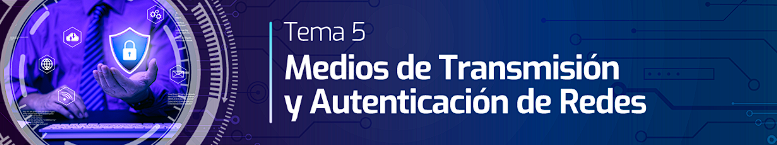
****

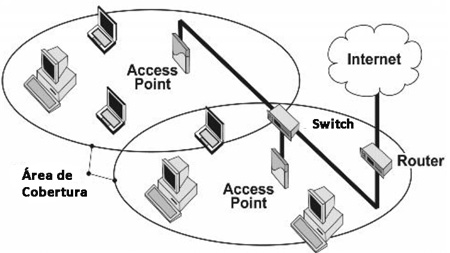


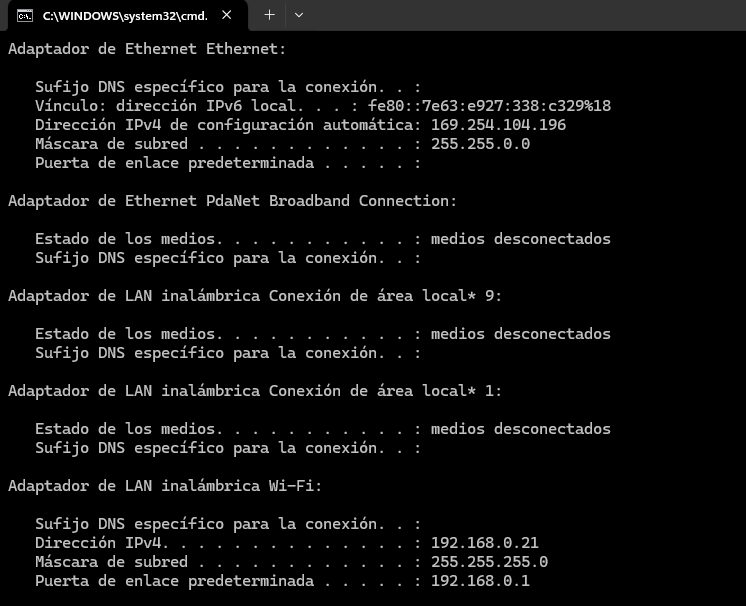
**Parcheo de software**

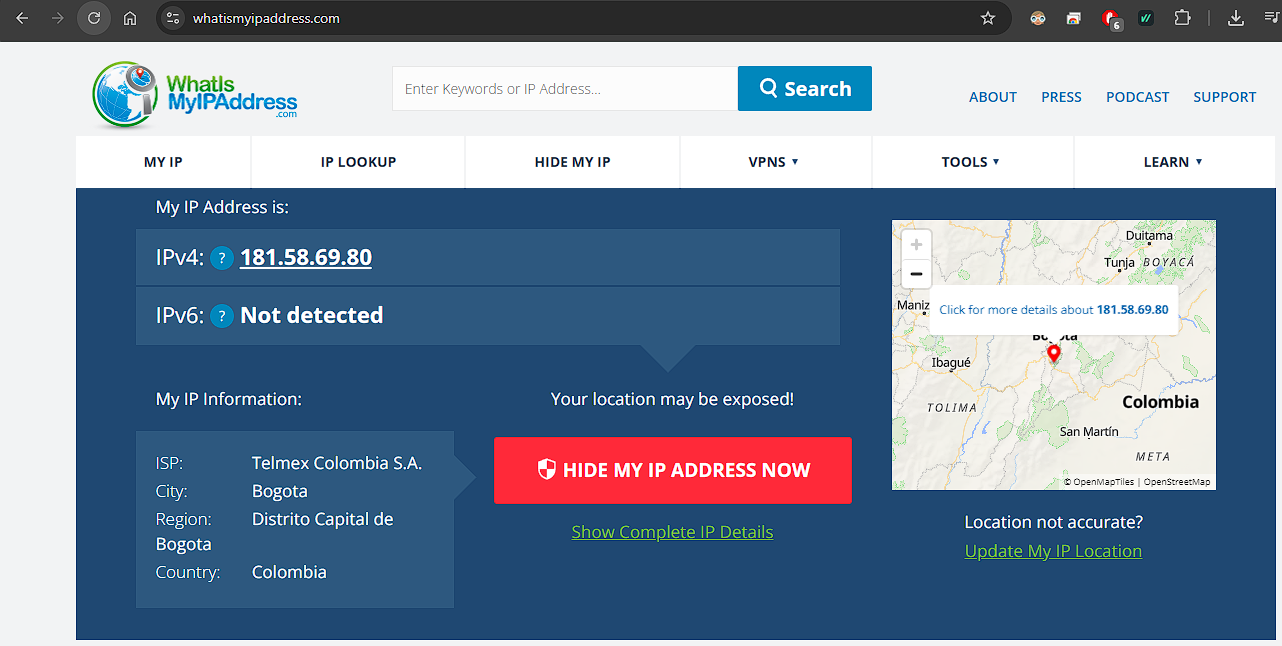
****

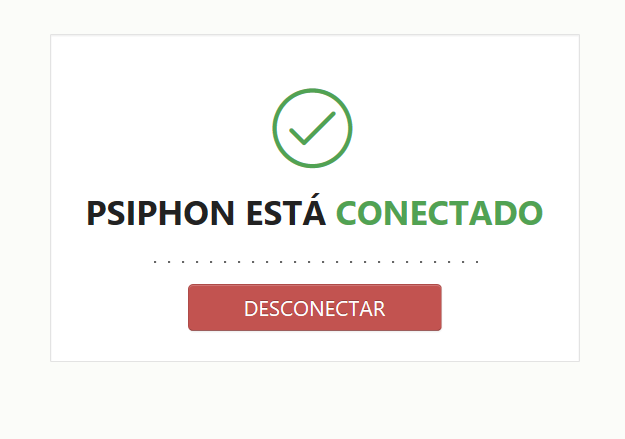


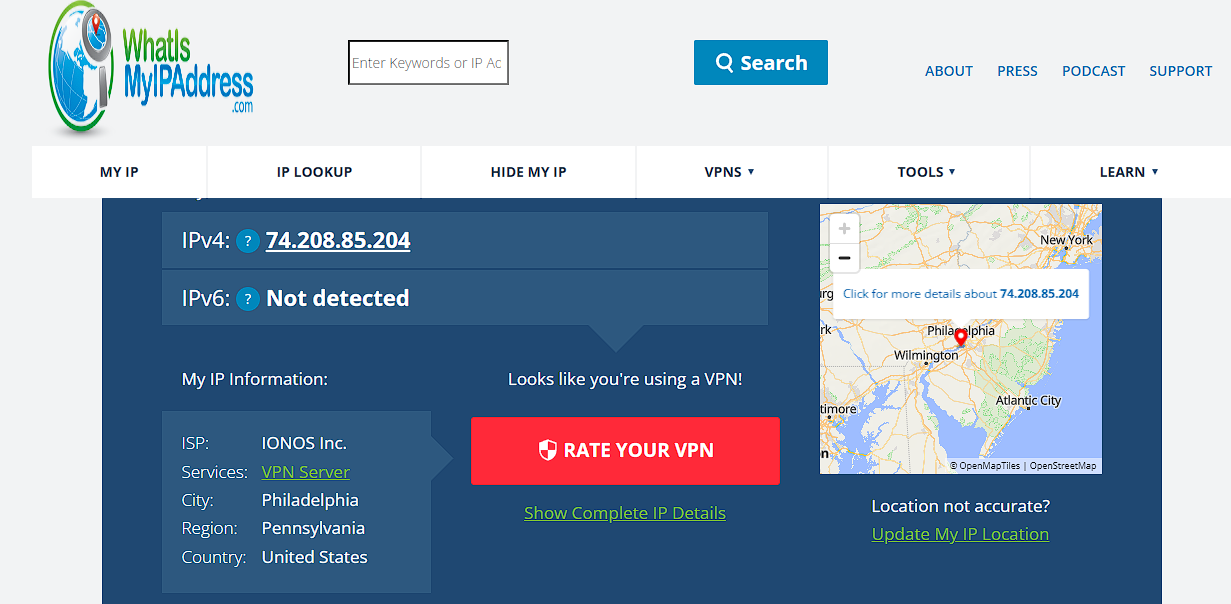
****











**Creación de reglas de Firewall con UFW e IPTABLES**

**# 1. Activar UFW**

sudo ufw enable

**# 2. Ver estado y reglas activas**

sudo ufw status verbose

**# 3. Permitir tráfico SSH (muy importante para no bloquearte)**

sudo ufw allow ssh

**# 4. Reglas de entrada**

sudo ufw allow http # Permitir tráfico HTTP (puerto 80)

sudo ufw allow https # Permitir tráfico HTTPS (puerto 443)

sudo ufw allow 53/udp # Permitir DNS sobre UDP

sudo ufw allow 53/tcp # Permitir DNS sobre TCP

**# 5. Reglas de salida**

sudo ufw default allow outgoing # Permitir todas las conexiones de salida

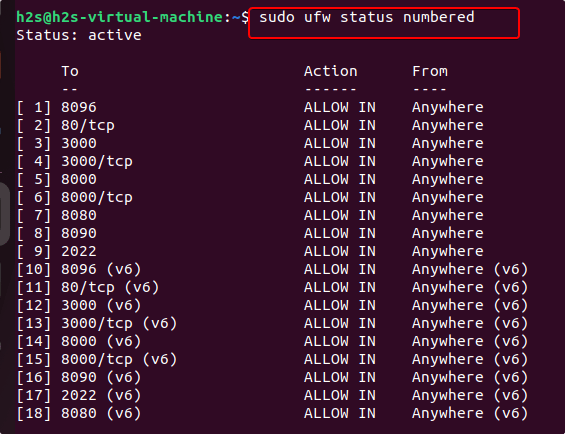
sudo ufw default deny incoming # Denegar todas las conexiones de entrada

# 6. Bloquear un puerto específico (ejemplo: 21 - FTP)

sudo ufw deny 21

# 7. Eliminar una regla (ejemplo: HTTP)

sudo ufw delete allow http



**# 1. Eliminar reglas existentes (opcional)**

sudo iptables -F

**# 2. Política por defecto**

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

**# 3. Permitir tráfico local (localhost)**

sudo iptables -A INPUT -i lo -j ACCEPT

**# 4. Permitir tráfico entrante relacionado o establecido**

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

**# 5. Permitir SSH (Puerto 22)**

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

**# 6. Permitir HTTP (Puerto 80)**

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

**# 7. Permitir HTTPS (Puerto 443)**

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

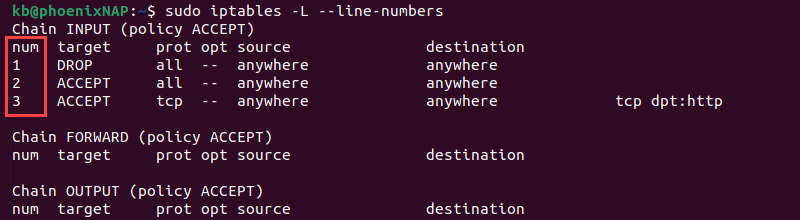
**# 8. Permitir DNS (TCP y UDP puerto 53)**

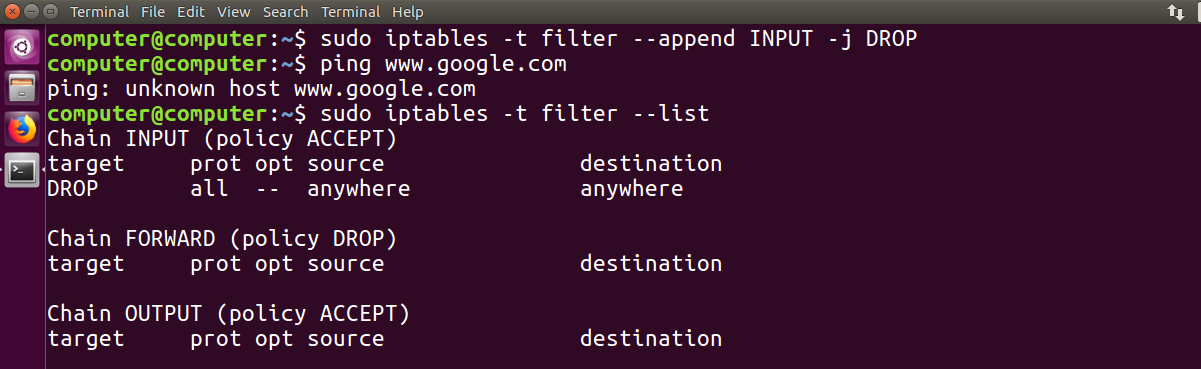
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT

**# 9. Guardar las reglas (Ubuntu 20.04+)**

sudo iptables-save | sudo tee /etc/iptables/rules.v4





**Configuración Firewall de Windows**

