✅ Evaluación Práctica: Diseño de Red Segura para Laboratorio 2 - UTU

Puntaje total: 20 puntos
Criterios de evaluación: completitud, claridad, seguridad y solución técnica viable.

---

❶ Enunciado General

Diseñar una red para brindar servicio de **servidor web** y **base de datos**. Los servidores deben estar **virtualizados en un solo host con Proxmox**, ubicados en el **Laboratorio 2 de la UTU**, y deben:

- Estar en una **DMZ** segura, **detrás de un firewall**.
- Tener definidos: **NOMBRE**, **IP**, **GW**, **MAC** (simulada), y **puertos de escucha**.
- Convivir con las redes **Ceibal** y de **la UTU**, sin interferencias.
- Implementar servicios de **DNS** y **DHCP** internos.
- Definir **VLANs** para separar:
    - Tráfico de servidores (admin).
    - Estudiantes (vlan_students).
    - Docentes (vlan_staff).
    - WiFi general.

  La red de **estudiantes** proviene de la red de **aulas** de la UTU. Se debe considerar esta restricción como parte del diseño lógico y de seguridad.

Se debe entregar:

- Diagrama **topológico** lógico.
- Diagrama **físico** de cableado y ubicación de equipos:
    - Rack: los estudiantes deberán realizar un **inventario** del equipamiento actual y cargar las **especificaciones físicas reales** del mismo.
    - Detallar tipo de cableado, conexiones con patchera, switch, terminal jack, y rack frame (si existe).

---

❷ Componentes de la Red

Servidores Virtuales en Proxmox (DMZ)

Servicio	Nombre	IP	GW	MAC	Puertos
Web Server	`web-lab2`	192.168.100.10	192.168.100.1	02:00:00:00:01	80, 443
DB Server	`db-lab2`	192.168.100.20	192.168.100.1	02:00:00:00:02	3306
DNS/DHCP	`dns-lab2`	192.168.100.2	192.168.100.1	02:00:00:00:03	53, 67

> Todos los servicios deben estar contenidos dentro de contenedores LXC o VMs dentro de Proxmox, en VLAN 100 (DMZ).

---

❸ VLANs Sugeridas

Nombre VLAN	ID	Uso
VLAN_DMZ	100	Servidores virtualizados
VLAN_STUDENTS	110	Acceso estudiantes (red aulas UTU)
VLAN_STAFF	120	Acceso docentes
VLAN_WIFI_GUEST	130	Invitados / pública WiFi

---

❹ Consideraciones de Seguridad

- Firewall entre WAN/UTU y VLAN_DMZ.
- Políticas:
  - Solo permitir puertos específicos en DMZ (80, 443, 3306, 53, 67).
  - Bloquear acceso desde STUDENTS a DMZ.
  - Permitir STAFF acceso limitado a DMZ.
  - Separar todo tráfico WiFi en VLAN 130, sin acceso a servidores.
- Monitoreo con SNMP o herramienta tipo Zabbix sugerido.

---

❺ Diagrama Topológico (Lógico)

> Reutilizar el estilo del práctico anterior, incluyendo:

- Proxmox host como nodo central.
- Enlaces etiquetados por VLAN.
- Switch gestionable.
- Firewall conectado a Ceibal/UTU.

---

❻ Diagrama Físico - Cableado y Rack

El detalle del equipamiento físico debe ser **levantado y documentado por el estudiante**:

- Realizar un **inventario** del rack actual en el Laboratorio 2.
- Detallar ubicación del rack en el espacio físico.
- Identificar:
    - Cantidad de unidades (U) ocupadas.
    - Tipo de patchera.
    - Switch utilizado.
    - Tipos de cables (Cat5e, Cat6, fibra, etc.).
    - Tomas murales (jack hembra) y canaletas.
    - Organización del cableado.

---

❼ Integración con redes existentes

- Conexión del switch principal hacia:
    - **Router UTU**: acceso a Internet y direcciones oficiales.
    - **Router Ceibal**: segmentado, sin routing hacia DMZ.
- Tráfico gestionado con ACLs y tagging de VLAN en puertos troncales.
- Estudiantes deben considerar la coexistencia sin conflicto ni exposición de la red DMZ.

✅ Criterios de Evaluación (20 puntos)

Criterio	Puntaje
Topología lógica clara y completa	5
Diagrama físico con detalles de rack/cable	5
Configuración coherente de red/DNS/DHCP	4
Separación de tráfico con VLAN y seguridad	4

Consideraciones con Ceibal y UTU	2

Total: **20 puntos**

✨ Se espera una propuesta profesional, funcional, documentada y basada en la realidad técnica del Laboratorio 2.