UNIVERSIDAD NACIONAL DE GENERAL SARMIENTO

INSTITUTO DE INDUSTRIA

LICENCIATURA EN SISTEMAS

TRABAJO FINAL – SISTEMAS OPERATIVOS Y REDES 2

"DISEÑO DE UN SISTEMA DE BALANCEO DE CARGA PARA REDES HÍBRIDAS EN ENTORNOS CLOUD"

Alumno: **Alex Ramírez Torres**

Materia: **Sistemas Operativos y Redes 2**

Docente: **Prof. Juan Pérez**

Fecha de entrega: **30 de junio de 2025**

Buenos Aires, Argentina

1. Propósitos del Trabajo

El trabajo final integrador busca:

Aplicación práctica: Demostrar competencia técnica en diseño/implementación de soluciones relacionadas con Sistemas Operativos y Redes 2.

Puente investigativo: Sentar bases para proyectos de mayor alcance (ej: tesis de grado, publicaciones académicas).

2. Formato de Entrega

Formato de envío: TP[Numero de Tp]_[Materia]_[año y semestre]_[Apellido y Nombre del que subió el archivo]. Ejemplo: *TPFinal_SOR2_2025_1s_PérezLucas*

Contenido: Documento.pdf, Presentacion.pptx, Codigo/, Datasets/, etc.

3. Fecha de Entrega

Fecha Límite: 11 de junio de 2025

4. Criterios de Evaluación (100 puntos)

Componente	Puntaje	Detalle
Originalidad	25 pts	Solución innovadora vs. réplica de existentes
Profundidad Técnica	30 pts	Uso avanzado de herramientas, análisis crítico de datos
Documentación	20 pts	Estructura APA, redacción académica impecable
Presentación Oral (Excluyente)	25 pts	Dominio del tema, manejo de Q&A (7 min exposición + 3 min preguntas)

5. Estructura Obligatoria (15 páginas +)

5.1. Portada Formal

Título específico (ej: *"Diseño de un sistema de balanceo de carga para redes hibridas en entorno cloud")*

Logo institucional, nombre completo del estudiante, fecha y código de materia.

5.2. Resumen Ejecutivo (200-250 palabras)

Problema abordado, metodología empleada, resultados destacados y contribución al campo si es que tuviese.

5.3. Planteamiento del Problema

Contexto actual**:** Datos cuantitativos o casos reales (ej: *"Según Cisco (2023), el 68% de las redes empresariales sufren ataques DDoS no mitigados*").

Pregunta central (Opcional): Formulación precisa (ej*: ¿Cómo mejorar la detección de intrusiones en redes IoT usando técnicas de análisis de tráfico?*).

5.4. Objetivos

General *"Desarrollar un modelo predictivo para fallos en sistemas distribuidos"*
Específicos 1. *Implementar un monitor de recursos en Python para servidores Linux*
2. *Comparar 3 algoritmos de scheduling en Kubernetes*

5.5. Marco Teórico

Antecedentes: 5 referencias clave (2019-2024) con análisis crítico. (ej: *"Singh et al. (2022) demostraron que... pero omitieron..."*).

Glosario técnico (Opcional)

5.6. Metodología

Diseño: Experimental/cuantitativo, simulación numérica, estudio de caso.

Stack tecnológico: NS-3, Wireshark, nmap, C/Python, Raspberry Pi, servidores AWS EC2, etc

5.6.1. Integración de Marcos Técnicos (Obligatorio)

Todo Trabajo Final deberá fundamentarse en marcos teóricos y técnicos apropiados al enfoque del proyecto (Ver lineamientos al final).

En la presentación oral, también debe mostrarse con gráficos o ejemplos visuales.

5.7. Implementación

Incluir diagramas técnicos que muestre cómo se conectan los elementos de red y sistema operativo. Topología de red en draw.io, gráficos de secuencia UML, visio, etc.

5.8. Conclusiones

5.9. Referencias

Formato APA 7ª edición.

5.10. Anexos (Opcional)

Código: Scripts, archivos de configuración.

Multimedia: Videos demostrativos, logs de servidores.

Lineamientos para la Integración de Marcos Técnicos según el Tipo de Proyecto

1. Proyectos Enfocados en Redes

Incluir una sección titulada: **"Análisis según Modelo OSI".** Debe contener:

- Capa(s) involucradas: descripción técnica de en qué capa(s) del Modelo OSI se sitúa el problema o solución.
- Protocolos asociados: mención clara de los protocolos involucrados y su capa correspondiente.
- Mecanismos de seguridad aplicados: descripción de amenazas específicas y medidas de mitigación implementadas.

Ejemplo: *Ataque Man-in-the-Middle (MitM) en una red LAN corporative*

Capas involucradas: Capa 2 (Enlace de Datos) mediante ARP Spoofing, Capa 6 y 7 si hay manipulación de tráfico cifrado (TLS/HTTPS).

Protocolos**:** ARP (Capa 2), TLS (Capa 6), HTTPS (Capa 7).

Seguridad aplicada**:** Capa 2: Prevención con *arpwatch* y tablas ARP estáticas. Capa 4: Protección contra SYN Floods con *iptables*. Capa 7: Prevención de phishing con autenticación OAuth 2.0.

Opcional: También pueden utilizar marcos complementarios como: Zero Trust**,** NIST Cybersecurity Framework**,** MITRE ATT&CK**,** Modelo TCP/IP**.**

2. Proyectos Enfocados en Sistemas Operativos

Incluir una sección titulada: **"Análisis según Modelo de Capas del Sistema Operativo"**. Debe contener:

- Capas involucradas del sistema operativo, con una breve descripción de su rol en el proyecto.
- Mecanismos de seguridad y control utilizados en cada capa.
- Procesos o funciones clave del sistema operativo relacionados.

Ejemplo**:** *Aislamiento de Contenedores Docker en Linux*

Capas involucradas**:**

- *Capa 1 (Hardware)*: Compartición de CPU, RAM, disco entre contenedores.
- *Capa 2 (Kernel)*: Aislamiento de procesos con *namespaces* y control de recursos con *cgroups*. Seguridad con *AppArmor* o *SELinux*.
- *Capa 3 (Servicios del sistema)*: Uso de *OverlayFS* y drivers de red virtual.
- *Capa 4 (Aplicaciones)*: Servidores web o bases de datos ejecutándose en contenedores.

Seguridad aplicada**:**

- Aislamiento reforzado con políticas en el kernel.
- Archivos de solo lectura para prevenir modificaciones maliciosas.
- Limitación de puertos y ejecución controlada.

Opcional: Se pueden integrar marcos como: POSIX**,** Modelos Cliente-Servidor o Microkernel**,** Ciclo de vida del proceso**.**

3. Proyectos Combinados (Redes + Sistemas Operativos)

Incluir una sección titulada: **"Integración del Modelo OSI y Capas del Sistema Operativo"**. Debe contener:

- Identificación clara de las capas involucradas en ambos modelos.
- Justificación técnica de cómo se articula la solución desde ambos puntos de vista.
- Descripción de herramientas, protocolos y funciones del sistema utilizadas.

Ejemplo: *Desarrollo de un IDS embebido en Linux para una red empresarial*

Capas OSI involucradas**:**

- Capa 3 (Red): Monitoreo de tráfico IP.
- Capa 4 (Transporte): Análisis de tráfico TCP/UDP.

Sistema Operativo**:**

- Captura de paquetes en el espacio del kernel (p. ej., con *nfqueue*).
- Procesamiento y alertas desde el espacio de usuario.
- Registro de eventos en archivos logs.
- Posible uso de contenedores para aislamiento del IDS.

Protocolos**:** IP, TCP, herramientas como *Snort* o *Suricata*.

Seguridad aplicada**:**

- Cifrado de logs.
- Políticas de red con *iptables*.
- Contención de procesos con Docker.