Banco de Proyectos Finales de Semestre

SIS313: Infraestructura, Plataformas Tecnológicas y Redes

Lucio Marcelo Quispe Ortega

Semestre: 2/2025

Índice

I. Proyectos de Plataformas y Escalabilidad (T2, T4, T6)

1. Diseño e Implementación de un Sistema de Salas de Espera y Filas Virtuales (Virtual Queue)

Objetivo: Implementar un sistema de colas virtuales (similar a Virtual Queue) para manejar la sobrecarga de tráfico durante picos altos (ej., programación de asignaturas), redirigiendo a los usuarios a una sala de espera y permitiendo el acceso por cupos (ej., 100 alumnos por minuto) al sistema crítico (ej., SUNiver).

Justificación: Aborda directamente la falla de la **Continuidad Operacional (T1)** del sistema de inscripción, donde la saturación genera caídas. El proyecto requiere aplicar técnicas de **Balanceo de Carga (T3)**, **Optimización (T4)** y **Alta Disponibilidad (T2)** para crear una capa de protección (el sistema de filas) que evita el colapso.

Tecnologías/Software: Nginx/HAProxy (Proxy/Rate Limiting), **Redis/Memcached** (Gestión de Cola), **Node.js/Python** (Lógica de la Sala de Espera), **Prometheus/Grafana** (Monitoreo de tráfico en la cola).

2. Replicación de Base de Datos Maestro-Esclavo con Separación de Lectura/Escritura

Objetivo: Diseñar y configurar un clúster de Base de Datos con replicación, separando las operaciones de lectura (esclavo) y escritura (maestro) para optimizar el rendimiento y la tolerancia a fallos.

Justificación: Elimina el Single Point of Failure en la BD. Aplica los conceptos de **Alta Disponibilidad (T2)**, **Clúster (T1)**, **Backups (T6)** y mejora la capacidad de respuesta de aplicaciones con muchas consultas de lectura.

Tecnologías/Software: MariaDB/PostgreSQL (Replicación Asíncrona/Síncrona), **ProxySQL/pgPool-II** (Separación de Lectura/Escritura), **Keepalived** (Failover), **Bash/Ansible** (Automatización).

3. Servicio de Hosting PyMES con ISPConfig para Soporte a Emprendedores

Objetivo: Implementar un servicio de hosting multi-dominio (Web, Correo, DNS) utilizando ISPConfig para apoyar a emprendedores con servicios gratuitos limitados.

Justificación: Simula un entorno real de proveedor de servicios, integrando la gestión de **Servicios de Red (T4)** esenciales (DNS BIND, Postfix/Dovecot, Apache/Nginx) con la **Automatización (T6)** del provisionamiento. Demuestra administración de infraestructura completa.

Tecnologías/Software: ISPConfig/Virtualmin, **Postfix/Dovecot/ClamAV** (Correo), **BIND** (DNS), **PHP-FPM**, **Bash/Python** (Scripting de Automatización).

4. Plataforma de Almacenamiento y Colaboración Universitaria (Nextcloud/ownCloud)

Objetivo: Desplegar un servicio de almacenamiento en la nube privado (Nextcloud o similar) con acceso autenticado para la comunidad, permitiendo la sincronización en dispositivos móviles y PC.

Justificación: Ofrece una alternativa segura y soberana a servicios externos (Dropbox). Requiere configurar la **Capa de Almacenamiento (T2)** con redundancia (ej., LVM), **Hardening de Acceso (T5)** (SSL/TLS) y la integración de **Proxy/WAF (T5)**.

Tecnologías/Software: Nextcloud/ownCloud, **Apache/Nginx** (Servidor Web), **MariaDB/PostgreSQL** (BD), **LDAP/Active Directory** (Autenticación), **ModSecurity** (WAF).

II. Proyectos de Seguridad y Control de Red (T3, T5)

5. Portal Cautivo con Gestión de Consumo (GB/día) y Autenticación Universitaria

Objetivo: Configurar un Portal Cautivo para la red Wi-Fi que limite el consumo de datos por usuario, requiriendo autenticación centralizada.

Justificación: Permite una gestión equitativa del ancho de banda (**T3**), evitando la saturación por usuarios individuales. El proyecto integra **Networking (T3)** (DHCP, NAT), **Seguridad (T5)** (acceso controlado) y la gestión de **Servicios (T4)** (servidor Radius).

Tecnologías/Software: pfSense/OPNsense/MikroTik (Firewall/Portal), **FreeRADIUS** (Autenticación y Acct.), **MariaDB** (Almacenamiento de Cuentas/Consumo), **VLANs (T3)**.

6. Defensa Perimetral de Aplicaciones: WAF y Bloqueo de Intrusiones (Fail2ban)

Objetivo: Implementar un Web Application Firewall (WAF) y configurar Fail2ban para escanear logs y bloquear automáticamente IPs con comportamiento malicioso (fuerza bruta, escaneo de vulnerabilidades).

Justificación: El proyecto integra dos capas de defensa, aplicando directamente las técnicas de **Seguridad y Hardening (T5)**. El WAF protege contra ataques de aplicación (SQLi, XSS) y Fail2ban automatiza el **Hardening de Servicios (T5)** contra

ataques de diccionario.

Tecnologías/Software: ModSecurity/NAXSI (WAF), **Fail2ban**, **Nginx/Apache** (Proxy Inverso), **Linux Firewall (iptables/UFW)** (Bloqueo de IPs).

7. Implementación y Análisis de Tráfico de Red en Tiempo Real con Ntopng

Objetivo: Desplegar y configurar **ntopng** para monitorear el tráfico de red, identificar el uso de protocolos, el consumo de ancho de banda por host y detectar anomalías en tiempo real.

Justificación: Permite una gestión proactiva y forense de la red. El proyecto se centra en la auditoría de la **Infraestructura de Networking (T3)**, la captura y el análisis de paquetes (T3), y es una herramienta clave para la **Gestión de Incidentes (T1)**.

Tecnologías/Software: Ntopng, **Prometheus/Grafana** (Visualización de Métricas de Ntopng), **Switch/Router** con capacidad de Port Mirroring o **TAP** (Hardware/Virtual).

8. Diseño y Despliegue de una VPN Segura para Acceso Remoto (WireGuard)

Objetivo: Implementar una Red Privada Virtual (VPN) de acceso remoto para estudiantes y docentes, utilizando el protocolo moderno y eficiente **WireGuard**.

Justificación: Provee un canal de comunicación cifrado (**T5**) y seguro para acceder a recursos internos (servidores, repositorios) desde fuera del campus. Se enfoca en la **Seguridad de Red (T3, T5)** y la configuración de túneles VPN.

Tecnologías/Software: WireGuard, **UFW/iptables** (Reglas de Enrutamiento y NAT), **Bash/Ansible** (Generación automatizada de claves públicas/privadas).

III. Proyectos de Automatización y Gestión (T6)

9. Diseño e Implementación de Plan de Backups Automatizado (Incremental y DRP)

Objetivo: Diseñar e implementar un sistema de **Backups Automáticos (T6)** que use una estrategia incremental, gestione la retención (GFS: Grandfather-Father-Son) y documente el Plan de Recuperación ante Desastres (DRP).

Justificación: Los backups son el último recurso para la **Continuidad Operacional (T1)**. El proyecto se enfoca en la eficiencia del almacenamiento (incrementales) y la **Automatización (T6)** del proceso de restauración, vital para la resiliencia del sistema.

Tecnologías/Software: Bacula/Duplicity/Restic, **Cron/Systemd** (Planificación), **LVM Snapshots** (Consistencia de la BD), **Ansible** (Automatización de la Restauración).

10. Repositorio de Proyectos GIT Exclusivo para la Comunidad Universitaria (GitLab)

Objetivo: Desplegar una instancia dedicada de **GitLab** que provea un repositorio central para que estudiantes y docentes puedan versionar sus proyectos.

Justificación: Introduce la metodología de **Control de Versiones (T6)** y la integración continua/entrega continua (CI/CD). Requiere la configuración de un **Proxy Inverso (T4)**, la aplicación de **Hardening (T5)** y la gestión de grandes volúmenes de datos.

Tecnologías/Software: GitLab Community Edition, **Nginx/Apache** (Proxy Inverso), **LDAP/OAuth** (Integración de Autenticación), **Prometheus** (Monitoreo de Servicios).

IV. Proyectos de Servicios Críticos y Plataformas (T4, T2)

11. Implementación de Correo Corporativo de Alta Disponibilidad

Objetivo: Desplegar y configurar una plataforma de correo electrónico empresarial (utilizando una suite como iRedMail) con mecanismos de **Alta Disponibilidad (T2)**, gestión de buzones, listas de distribución, y un robusto sistema **Anti-Spam/Anti-Virus (T5)**.

Justificación: El correo sigue siendo el servicio de comunicación formal más crítico en cualquier institución. Este proyecto busca asegurar la **Continuidad Operacional (T1)** del servicio mediante redundancia (MTA) y el **Hardening de Protocolos (T5)** (SSL/TLS, DMARC/SPF/DKIM). Exige el dominio de la configuración de servicios complejos (**T4**) como SMTP, IMAP y POP3 en un entorno multi-tenant o corporativo.

Tecnologías/Software: iRedMail/Mailcow (Suite), **Postfix/Dovecot** (MTA/MDA), **MariaDB/PostgreSQL** (BD de Cuentas), **ClamAV/SpamAssassin** (Seguridad), **Nginx/Apache** (Webmail), **Keepalived** (HA para Failover de servicios).

12. Plataforma de Mensajería Instantánea Segura orientada a la Comunidad Universitaria

Objetivo: Desplegar una solución de mensajería empresarial (ej., Mattermost o Rocket.Chat) que soporte mensajes privados, grupos, y el envío de archivos, configurada para ser **Escalable (T2)** y con acceso autenticado para estudiantes y docentes.

Justificación: Ofrece un canal de comunicación en tiempo real que es privado y está bajo control de la universidad, superando las limitaciones de seguridad y privacidad de plataformas externas (WhatsApp/Telegram). El proyecto integra **Servicios Web (T4)**, **Bases de Datos (T2)** y la optimización de **Networking (T3)** para latencia.

Tecnologías/Software: Mattermost/Rocket.Chat, **Nginx/Apache** (Proxy Inverso con WebSockets), **PostgreSQL/MongoDB** (Base de Datos), **Prometheus** (Monitoreo de conexiones concurrentes).

13. Optimización de Rendimiento del LMS Moodle mediante Sistemas de Caché

Objetivo: Analizar el rendimiento de un sistema LMS (Moodle) e implementar soluciones de **Caché (T4)** para reducir la carga de la Base de Datos durante picos de tráfico.

Justificación: Aborda directamente el problema de rendimiento en entornos de alto tráfico. Demuestra la habilidad de diagnosticar **Infraestructura de Hardware (T2)** y aplicar técnicas de **Optimización de Servicios (T4)** para mejorar la escalabilidad y la experiencia del usuario.

Tecnologías/Software: Moodle, **Redis/Memcached** (Caché de Objetos), **Nginx/Varnish** (Caché HTTP), **Prometheus/Grafana** (Medición de Latencia y Aciertos de Caché).

14. Implementación de un Servicio de Streaming de Video Conferencia (Jitsi Meet / BigBlueButton)

Objetivo: Desplegar una plataforma de videoconferencia robusta (Jitsi Meet o similar) para la comunidad universitaria, optimizando los recursos de red y configurando el servicio para manejar un alto volumen de sesiones concurrentes.

Justificación: Proporciona una alternativa libre y soberana a servicios comerciales (Zoom), esencial para la **Continuidad Operacional (T1)** de la docencia cuando no es posible la presencialidad. Exige un profundo conocimiento de **Networking (T3)** para gestionar el tráfico UDP/TCP en tiempo real y la configuración de **Servicios Web (T4)** y media servers dedicados para el transcoding.

Tecnologías/Software: Jitsi Meet/BigBlueButton, **STUN/TURN Servers** (Gestión de NAT/Firewalls), **Nginx/Apache** (Proxy Inverso), **IPTables/UFW** (Gestión del tráfico UDP - **T5**), **Prometheus/Grafana** (Monitoreo de CPU y Latencia).

V. Proyectos de Seguridad Perimetral y Control (T3, T5)

15. Implementación de Proxy Caching Transparente para Control de Contenido y Ancho de Banda

Objetivo: Configurar un Proxy Caching Transparente (ej., Squid) para auditar el tráfico HTTP/S, implementar políticas de bloqueo por categoría o horario, y optimizar el uso de ancho de banda mediante caché.

Justificación: Permite cumplir normativas de uso, mejorar la **Seguridad (T5)** y la **Eficiencia de Red (T3)** al servir contenido popular desde la caché local. Se enfoca en la **Seguridad Perimetral (T5)** y el control de tráfico a nivel de aplicación.

Tecnologías/Software: Squid (Proxy Caching), **SquidGuard/DansGuardian** (Filtro de Contenido), **iptables** (Redirección Transparente de tráfico puerto 80/443), **SSL Bumping** (Proxy HTTPS).

16. Sistema de Monitoreo Proactivo de Infraestructura con Zabbix o Nagios

Objetivo: Instalar, configurar y desplegar un sistema de monitoreo (Zabbix o Nagios) para supervisar el estado de servidores (hardware/SO) y equipos de red (SNMP), con alertas automatizadas.

Justificación: La gestión proactiva es fundamental para la **Continuidad Operacional (T1)**. Este proyecto integra la gestión de **Plataformas de Servicios (T4)** y la supervisión de la **Infraestructura de Networking (T3)**, garantizando la detección temprana de fallos.

Tecnologías/Software: Zabbix/Nagios, **SNMP** (Monitoreo de Switches/Routers), **Agentes Zabbix/NRPE** (Monitoreo de Servidores), **MariaDB/PostgreSQL** (BD de Monitoreo).

17. Hardening Automatizado de Servidores Linux Usando Ansible y Estándares CIS

Objetivo: Diseñar Playbooks de **Ansible (T6)** que automaticen la aplicación de políticas de seguridad (ej., **CIS Benchmarks**) en un servidor base, validando el cumplimiento del hardening.

Justificación: La aplicación manual de seguridad (**Hardening - T5**) es ineficiente y no escalable. Este proyecto demuestra el uso de la **Automatización (T6)** como herramienta de seguridad fundamental para la gestión de la infraestructura.

Tecnologías/Software: Ansible, **YAML** (Definición de Playbooks), **Linux Security Modules (SELinux/AppArmor)**, **CIS-CAT/Lynis** (Herramientas de Audi-

toría).

VI. Proyectos de Repositorios y Automatización (T6, T4)

18. Repositorio Digital Universitario para Tesis, Artículos y Contenido Académico (DSpace/EPrints)

Objetivo: Implementar un repositorio digital que permita a la comunidad universitaria subir, organizar y compartir material académico (tesis, artículos, publicaciones), asegurando su persistencia y fácil acceso.

Justificación: Crea un activo digital de la universidad para preservar la producción científica y académica. Requiere la configuración de una plataforma web (a menudo **Java/PHP - T4**), un diseño de **Almacenamiento (T2)** de gran capacidad y alta disponibilidad, y la implementación de políticas de **Acceso Controlado (T5)** y metadatos para la catalogación.

Tecnologías/Software: DSpace/EPrints, **Apache Tomcat/Jetty** (Servidor de Aplicaciones), **PostgreSQL/Oracle** (BD), **LVM/RAID** (Gestión de Almacenamiento - **T2**), **Nginx/Apache** (Proxy de Acceso).

19. Implementación de Servicio de Wiki Universitario con MediaWiki y Optimización de Rendimiento

Objetivo: Desplegar un servicio de Wiki (MediaWiki) configurado con **Caché (T4)** y optimización de la Base de Datos para asegurar la disponibilidad del conocimiento.

Justificación: Una Wiki es una herramienta de documentación colaborativa. El proyecto requiere configurar un clúster web-DB básico y centrarse en el Hardening (T5) y la **Optimización de Plataformas (T4)** para manejar el tráfico concurrente de edición y lectura.

Tecnologías/Software: MediaWiki, **PHP-FPM**, **Nginx/Apache** (Servidor Web), **MariaDB/PostgreSQL** (BD), **Redis/Memcached** (Caché de MediaWiki).

20. Implementación de Servidor de Medios Centralizado (Emby/Plex Media Server)

Objetivo: Implementar un servicio de streaming de contenido multimedia (video/audio) con acceso autenticado para una organización o comunidad universitaria.

Justificación: Simula un servicio de biblioteca de recursos didácticos o entretenimiento interno. Requiere un diseño de **Almacenamiento (T2)** de gran capacidad y alta velocidad, gestión de ancho de banda (**T3**) y **Hardening (T5)** del acceso para proteger el contenido.

Tecnologías/Software: Emby/Plex Media Server, **LVM/RAID 5/6** (Almacenamiento), **Nginx/Apache** (Proxy Inverso con SSL), **Docker/Podman** (Contenedores para despliegue).