Gestión Operativa y Seguridad en Redes
Ordenanza 1877

Datos administrativos de la asignatura			
Departamento:	Ingeniería en Sistemas de Información	Carrera	Ingeniería en Sistemas de Información
Asignatura:	Gestión Operativa y Seguridad en Redes		
Nivel de la carrera	5º nivel	Duración	Cuatrimestral
Bloque curricular:	Tecnologías Aplicadas		
Carga horaria presencial semanal:	4,5 hs. Reloj / 6 hs. catedra	Carga Horaria total:	72 hs. Reloj / 96 hs. cátedra
Profesor/es Titular/Asociado/Adjunto:	Osvaldo Falabella	Dedicación:	Simple
JTP:	Lautaro Bifano	Dedicación:	Simple ad honorem
Ayudante de primera	Rafael Caceres Petkowicz	Dedicación:	Simple ad honorem

Propósito

Aplicar las redes de datos como soporte y gestión para los sistemas de información, en base al estudio de las topologías, protocolos, seguridad informática y arquitecturas de las mismas.

Objetivos establecidos en el DC

-Gestionar las arquitecturas de redes de datos como soporte de un sistema de información.
-Analizar los componentes necesarios que conforman una red de datos garantizando la calidad de servicio.
-Evaluar los conceptos de seguridad informática en una red de datos.
-Determinar las políticas para compartir recursos y su implementación.
-Monitorear los recursos de la red.
-Analizar y tomar decisiones en la implementación de servicios y aplicaciones para Internet.
-Fomentar la lectura de documentación técnica en inglés, dado que la mayor parte de la información actualizada, y a la que el alumno deberá recurrir en un entorno laboral, se encuentran en ese idioma.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Resultados de aprendizaje
• **RA1:** Configura routers para asegurar la correcta gestión y optimización del enrutamiento de datos en la red, utilizando configuración básica, avanzada, y el uso de herramientas de gestión. • **RA2**: Diseña redes virtuales para optimizar recursos y mejorar la flexibilidad de la infraestructura de red, utilizando tecnologías como VLAN, VXLAN, así como configuraciones en entornos de nube. • **RA3**: Monitorea el rendimiento de las redes para garantizar una gestión eficiente y un rendimiento óptimo, utilizando técnicas de monitoreo de rendimiento, disponibilidad y tráfico. • **RA4:** Implementa el balanceo de carga para distribuir eficientemente el tráfico de red y mejorar la disponibilidad y rendimiento de los servicios, empleando métodos de balanceo de carga y configurando balanceadores de carga de hardware y software. • **RA5:** Aplica medidas de seguridad para controlar y proteger el acceso a las redes, implementando principios de control de acceso, autenticación, autorización y auditoría (AAA), y gestionando identidades y políticas de acceso. • **RA6:** Previene ataques en la red para minimizar el impacto de incidentes de seguridad, configurando firewalls y sistemas de prevención de intrusos (IPS), utilizando sistemas de detección de intrusos (IDS) y herramientas de análisis de tráfico
Asignaturas correlativas previas
Para cursar debe tener aprobada: • Redes de Información
Asignaturas correlativas posteriores
Indicar las asignaturas correlativas posteriores: NO APLICA

Contenidos Mínimos

1 - Administración de Routers.

2- Configuración de Redes Virtuales.

3 - Monitoreo y Control.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL
MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

4– Balanceo de Carga

5- Seguridad para Acceso a Redes

6 - Detección y Respuesta frente a Ataques

Programa analítico, Unidades temáticas

UNIDAD TEMÁTICA Nº 1 Administración de Routers

Objetivo de la unidad: Capacitar a los estudiantes en la configuración y administración de routers, asegurando una correcta gestión y optimización del enrutamiento de datos en la red.

CONTENIDOS:

- **Introducción a los Routers:**
  - Funciones y tipos de routers.
  - Componentes y arquitectura de routers.
- **Protocolos de Enrutamiento:**
  - Enrutamiento estático vs. enrutamiento dinámico.
  - Protocolos de enrutamiento interior (RIP, OSPF, EIGRP).
  - Protocolos de enrutamiento exterior (BGP).
- **Configuración de Routers:**
  - Configuración básica (interfaces, rutas estáticas).
  - Configuración avanzada (ACLs, NAT, VPN).
- **Gestión y Monitoreo de Routers:**
  - Monitoreo del rendimiento del router.
  - Diagnóstico y solución de problemas.
- **Seguridad en Routers:**
  - Implementación de políticas de seguridad.
  - Actualización y mantenimiento de firmware.
- **Gestión con MikroTik:**
  - Winbox y WebFig: Utilización de herramientas de gestión.

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

- MikroTik Scripting: Creación y ejecución de scripts para automatizar tareas.

Resultados de aprendizaje intervinientes: RA1

TIEMPO ASIGNADO: 6,75 horas reloj

UNIDAD TEMÁTICA Nº 2 Configuración de Redes Virtuales

Objetivo de la unidad: Dotar a los estudiantes de conocimientos y habilidades para diseñar, implementar y gestionar redes virtuales, optimizando recursos y mejorando la flexibilidad de la infraestructura de red

CONTENIDOS:

- **Fundamentos de Redes Virtuales:**
  - Conceptos de virtualización de redes.
  - Beneficios y desafíos de las redes virtuales.
- **Tecnologías y Protocolos:**
  - VLAN (Virtual LAN).
  - VXLAN (Virtual Extensible LAN).
- **Herramientas y Soluciones:**
  - VMware NSX, Cisco ACI.
  - Open vSwitch.
- **Configuración y Administración:**
  - Creación y gestión de VLANs.
  - Configuración de redes virtuales en entornos de nube (AWS, Azure).
- **Seguridad en Redes Virtuales:**
  - Segmentación y aislamiento de redes.
  - Implementación de políticas de seguridad en entornos virtualizados.

Resultados de aprendizaje intervinientes: RA2

TIEMPO ASIGNADO: 6,75 horas reloj

DIRECCIÓN ACADÉMICA
COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

UNIDAD TEMÁTICA Nº 3 Monitoreo y Control

Objetivo de la unidad: Proporcionar a los estudiantes las habilidades y conocimientos necesarios para monitorear y controlar redes de manera efectiva, garantizando un rendimiento óptimo y una gestión eficiente.

CONTENIDOS:

Contenidos:

- **Introducción al Monitoreo de Redes:**
  - Importancia del monitoreo de redes.
  - Herramientas y técnicas de monitoreo (Nagios, Zabbix, SolarWinds).
- **Métodos de Monitoreo:**
  - Monitoreo de rendimiento (ancho de banda, latencia, jitter).
  - Monitoreo de disponibilidad y tiempo de actividad.
  - Monitoreo de tráfico y uso de recursos.
- **Protocolos y Tecnologías de Monitoreo:**
  - SNMP (Simple Network Management Protocol).
  - NetFlow y sFlow.
  - Syslog y su integración en sistemas de monitoreo.
- **Control de Redes:**
  - Técnicas de control de red.
  - Implementación de políticas de calidad de servicio (QoS).
  - Automatización del control de red..

Resultados de aprendizaje intervinientes: RA3

TIEMPO ASIGNADO: 4,5 horas reloj

UNIDAD TEMÁTICA Nº 4 Balanceo de Carga

Objetivo de la unidad: Enseñar a los estudiantes las técnicas y tecnologías para distribuir eficientemente el tráfico de red y mejorar la disponibilidad y rendimiento de los servicios.

CONTENIDOS:

- **Conceptos Básicos de Balanceo de Carga:**
  - Definición y beneficios del balanceo de carga.
  - Escenarios y casos de uso.
- **Métodos de Balanceo de Carga:**
  - Round Robin.
  - Least Connections.
  - IP Hashing.
- **Tecnologías de Balanceo de Carga:**
  - Balanceadores de carga de hardware y software.
  - Herramientas y soluciones (HAProxy, NGINX, F5).
- **Implementación y Configuración:**
  - Configuración básica y avanzada de balanceadores de carga.
  - Monitorización y ajuste del balanceo de carga.
- **Alta Disponibilidad y Redundancia:**
  - Configuración de clusters de balanceadores de carga.
  - Técnicas de failover y recuperación.

Resultados de aprendizaje intervinientes: RA4

TIEMPO ASIGNADO: 6,75 horas reloj

UNIDAD TEMÁTICA Nº 5 Seguridad para Acceso a Redes

Objetivo de la unidad: Asegurar que los estudiantes comprendan y puedan implementar medidas de seguridad robustas para controlar y proteger el acceso a las redes.

CONTENIDOS:

- **Conceptos Básicos de Seguridad de Acceso:**
  - Principios de control de acceso.
  - Autenticación, autorización y auditoría (AAA).
- **Métodos de Control de Acceso:**

DIRECCIÓN ACADÉMICA
COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

- Listas de Control de Acceso (ACLs).
- Políticas de seguridad basadas en roles (RBAC).

- **Autenticación y Autorización:**
  - Protocolo RADIUS.
  - Protocolo TACACS+.
  - Autenticación multifactor (MFA).
- **Tecnologías y Herramientas:**
  - Implementación de 802.1X.
  - Soluciones NAC (Network Access Control).
- **Herramientas de Práctica:**
  - **Active Directory (AD) de Microsoft:**
    - Configuración y gestión de usuarios y grupos.
    - Políticas de grupo (GPO) y su implementación.
    - Prácticas de autenticación y autorización en un entorno AD.
  - **FreeIPA:**
    - Instalación y configuración básica.
    - Gestión de identidades y políticas de acceso.
    - Integración con otros servicios de red.
- **Buenas Prácticas y Políticas:**
  - Desarrollo e implementación de políticas de acceso.
  - Auditorías y cumplimiento de políticas de seguridad.

Resultados de aprendizaje intervinientes: RA5

TIEMPO ASIGNADO: 6,75 horas reloj

UNIDAD TEMÁTICA Nº 6 Prevención, Detección y Respuesta frente a Ataques

Objetivo de la unidad: Equipar a los estudiantes con las habilidades necesarias para prevenir, detectar y responder a ataques en la red, minimizando el impacto de incidentes de seguridad.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

CONTENIDOS:

- **Prevención de Ataques:**
  - Políticas y prácticas de prevención.
  - Configuración de firewalls y sistemas de prevención de intrusos (IPS).
- **Detección de Ataques:**
  - Sistemas de detección de intrusos (IDS).
  - Análisis de tráfico y comportamiento anómalo.
- **Herramientas de Detección:**
  - Snort, Suricata.
  - SIEM (Security Information and Event Management).
- **Respuesta a Incidentes:**
  - Planificación y preparación de respuesta a incidentes.
  - Procedimientos de contención y mitigación.
- **Recuperación y Reporte:**
  - Estrategias de recuperación post-incidente.
  - Documentación y reporte de incidentes.

Resultados de aprendizaje intervinientes: RA6

TIEMPO ASIGNADO: 13.5 horas reloj

Formación práctica de laboratorio: 22,5 hs. reloj (total de horas para la materia)

Metodología de enseñanza
Dictado de clases y realización de prácticas en aula tradicional, presentación de proyectos y simulaciones en software. La modalidad utilizada se desarrolla en el método de aprendizaje mediante resolución de problemas, análisis experimental y desarrollo de trabajos prácticos en forma grupal.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

Se realizan clases orientativas en los conceptos teóricos necesarios para el desarrollo de las actividades, complementándose con la lectura por los alumnos de esos temas en la bibliografía adoptada.

Se presentan ejercicios tipo a resolver en el aula como modelo para la resolución por parte de los alumnos en forma grupal e individual.

Por último, cerrando los conocimientos de cada módulo de estudio (ver contenidos del programa analítico) se proponen realización de prácticas en gabinete sobre equipos PC con conectividad a servidores Windows/Linux y equipamiento de red.

MODALIDAD DE LA ENSEÑANZA

En esta asignatura se utilizan como estrategias de enseñanza la clase expositiva, con el enriquecimiento de debates en clases sobre casos reales.

Por cada unidad temática se desarrollan actividades prácticas a través de problemas a resolver en forma escrita, simulaciones en ambientes de hardware y software y experiencias sobre equipamiento real.

Recomendaciones para el estudio

En virtud de la experiencia desarrollada a lo largo de varios años de dictado de la materia, se recomienda a los alumnos el estudio continuo de la misma tratando de no dejar contenidos sin repasar. Así mismo se recomienda la asistencia a clases a efectos de aprovechar las explicaciones y discusiones reflexivas brindadas por los docentes, ya que muchos conceptos se brindan y/o analizan en clase y son difíciles de obtenerlos de la bibliografía.

Se recomienda la interacción con los docentes ya sea en forma presencial en el aula o a través de los medios asincrónicos ofrecidos, grupo de difusión, campus virtual y e-mail.

Metodología de evaluación

La cátedra establece su régimen de evaluación y cursada en función de las Ordenanzas 1549/16 y 991/19.

Para la evaluación se establece un examen parcial teórico-práctico con dos (2) instancias de recuperación y un trabajo práctico integrador como instancias de evaluación.

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

APROBACIÓN DIRECTA

Para promocionar, el alumno deberá obtener en cada instancia de evaluación (parcial y trabajo integrador) una nota igual o superior a 6 (seis) puntos, debiendo cumplir al menos con el 75% de asistencia, sin posibilidades de reincorporación. Los alumnos que no cumplan con alguna de estas condiciones podrán optar por la aprobación no directa, siempre y cuando cumplan con las condiciones establecidas para la misma.

La calificación final surgirá del promedio de las instancias evaluativas, siendo la misma un número entero entre seis (6) y diez (10).

El parcial tendrá dos instancias de recuperación.

APROBACIÓN NO DIRECTA – EXAMEN FINAL

Las condiciones para la Aprobación no Directa — Examen Final estarán basadas en instancias evaluativas que aseguren un nivel mínimo y básico de aprendizaje según los objetivos planteados por la Cátedra.

En el caso de que la nota final de al menos una instancia evaluativa sea 4 (cuatro) o 5 (cinco), independientemente de las notas obtenidas en las restantes instancias evaluativas aprobadas, el estudiante obtendrá la Aprobación No Directa — Examen Final.

Si el estudiante decidiera recuperar alguna de las instancias evaluativas aprobadas con nota 4(cuatro) o 5 (cinco), prevalecerá la calificación más alta.

El examen final consiste en un coloquio en donde se evaluarán conceptos teóricos y prácticos de los contenidos curriculares de la materia. La nota final quedará determinada en función del conocimiento de lo demostrado por el alumno.

Recursos necesarios

Espacio físico: aula para dictado clases teórico-prácticas, laboratorio para prácticas presenciales.

Recursos tecnológicos de apoyo: proyector multimedia, softwares de simulación, computadoras de laboratorios, accesos a equipos de red para realizar prácticas, del laboratorio de uso de cátedras.

Referencias bibliográficas

Cloud Native Data Center Networking - Dinesh G. Dutt - Segunda Edición - O'Reilly - ISBN 9781492045601

Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud - William Stallings - Segunda Edición - Addison-Wesley Professional - ISBN 0134175395

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Alberto
Director de Departamento
DISI - UTN - FRLP

BGP Design and Implementation - Randy Zhang, Micah Bartell - Primera Edición - CiscoPress - ISBN 0133433552
MPLS and VPN Architectures - Ivan Pepelnjak, Jim Guichard - Primera Edición - Cisco Press - ISBN 1587050811
Modsecurity Handbook - Ivan Ristic - Segunda edición - Feisty Duck - ISBN 1907117024
Web Application Security, A Beginner's Guide - Bryan Sullivan,Vincent Liu - Segunda edición - McGraw Hill - ISBN 9780071776127
HACKING EXPOSED WEB APPLICATIONS - Joel Scambray, Vincent Liu, Caleb Sima - Tercera Edición - McGraw Hill - ISBN 978-0071740647
Aplicaciones seguras - Xavier Perramon - Primera Edición - FUOC - ISBN P06/M2107/01772
Bibliografía Complementaria
Understanding IPv6 - Joseph Davies - Segunda Edición - Microsoft Press - ISBN 0735624461
Guide to Computer Network Security - Joseph Migga Kizza - Quinta Edición - Springer - ISBN 3030381404
End-to-End Network Security Defense-in-Depth - Omar Santos - Primera Edición - Cisco Systems - ISBN 1587053322
Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications - Ivan Ristic - Tercera Edición - Lightning Source Inc - ISBN 1907117040
Hacking Exposed Wireless: Wireless Security Secrets & Solutions - Johnny Cache, Joshua Wright and Vincent Liu - Tercera Edición - Mc Graw Hill - ISBN 0071666613

DIRECCIÓN ACADÉMICA
ES COPIA FIEL DEL ORIGINAL

MARIA EUGENIA LAVORATTO
DIRECTORA
DIRECCIÓN ACADÉMICA
U.T.N. F.R.L.P.

Ing. Guerrieri Ruben Albert
Director de Departamento
DISI - UTN - FRLP