Guía del Profesor - Administración de Servicios de Correo Electrónico

Cómo Impartir la Sesión

Modelo de Aula Invertida (Flipped Classroom)

Este material está diseñado para aplicar la metodología de aula invertida siguiendo este esquema:

FASE 1: TRABAJO PREVIO EN CASA (2-3 días antes de la sesión)

Objetivo: El alumnado adquiere conocimientos teóricos de forma autónoma.

Actividades del alumnado:

1. **Revisar la documentación MkDocs** (60-90 minutos):
    - Leer los 6 módulos en orden: Conceptos Básicos → Arquitectura → Protocolos → DNS → Seguridad → Administración
    - Estudiar los diagramas Mermaid para comprender flujos y arquitecturas
    - Tomar notas sobre conceptos que no comprenden
2. **Completar el Kahoot** (20-35 minutos):
    - Realizar el cuestionario de 50 preguntas como autoevaluación
    - Identificar áreas que requieren refuerzo
    - Anotar dudas para resolver en clase

Actividades del docente:

- Enviar el enlace a la documentación MkDocs (se puede publicar con `mkdocs gh-deploy` o servir localmente con `mkdocs serve`)
- Programar el Kahoot y compartir el código de acceso
- Monitorear resultados del Kahoot para identificar conceptos problemáticos
- Preparar explicaciones reforzadas para los temas con menor tasa de acierto

Recursos necesarios:

- Acceso a la documentación MkDocs (online o archivo HTML estático)
- Kahoot configurado con las 50 preguntas
- Recurso audiovisual (videos de YouTube)

FASE 2: SESIÓN PRESENCIAL EN EL AULA (3-4 horas)

Objetivo: Aplicar conocimientos mediante prácticas, resolver dudas y profundizar conceptos complejos.

Estructura de la sesión:

1. Resolución de Dudas (20-30 minutos)

- Revisar resultados del Kahoot previo
- Identificar los 3-5 conceptos con mayor tasa de error
- Explicación reforzada usando la **Presentación PowerPoint**
- Turno de preguntas abierto

Conceptos que típicamente requieren refuerzo:

- Diferencia entre MTA, MDA y MUA
- Flujo completo de envío/recepción de correo
- Funcionamiento de SPF, DKIM y DMARC (conceptos más complejos)
- Interpretación de códigos SMTP (especialmente 4xx vs 5xx)

2. Demostración Práctica Guiada (30-40 minutos)

El docente realiza una demostración en vivo de:

1. **Análisis de cabeceras de correo real**:
    - Mostrar el path completo de un email
    - Identificar cada servidor MTA por el que pasó
    - Verificar registros SPF/DKIM/DMARC
2. **Consultas DNS**:
    - Consultar registros MX de dominios conocidos (gmail.com, outlook.com)
    - Mostrar registros SPF, DKIM y DMARC reales
    - Explicar cómo funcionan en conjunto

Herramientas recomendadas:

- `dig` / `nslookup` para consultas DNS
- MXToolbox (https://mxtoolbox.com) para validaciones
- Mail-Tester para analizar configuraciones
- Cliente de correo (Thunderbird) para ver cabeceras

3. Realización de Actividades Prácticas

Actividad Práctica 1 - Análisis de Infraestructura (45-60 minutos)

Entregable: Documento con tabla comparativa y conclusiones sobre las buenas prácticas encontradas.
Modalidad: Parejas
Evaluación: Formativa (10% de la nota)

Descanso (10-15 minutos)

Actividad Práctica 2 - Configuración de Servidor (60-90 minutos)

Entregable: Capturas de pantalla de:

1. Archivo `/etc/postfix/main.cf` configurado
2. Salida de `postqueue -p` mostrando cola vacía
3. Cliente de correo mostrando mensaje recibido
4. Fragmento de `/var/log/mail.log` con entrega exitosa

Tiempo: 60-90 minutos
Modalidad: Individual o parejas
Evaluación: Formativa (15% de la nota)

4. Cierre y Síntesis (10-15 minutos)

- Resumen de conceptos clave aprendidos
- Responder últimas dudas
- Explicar evaluación: examen test de 30 preguntas (próxima sesión)
- Recordar material de estudio disponible en MkDocs

FASE 3: EVALUACIÓN SUMATIVA (próxima sesión - 30-40 minutos)

Examen Test de 30 preguntas:

- Formato: Test tipo ASIR (similar a exámenes oficiales)
- Duración: 30 minutos
- Peso: 50-60% de la nota del tema
- Evalúa: Conocimientos teóricos y capacidad de análisis

Criterios de evaluación:

- Comprensión de arquitectura de correo electrónico
- Conocimiento de protocolos SMTP, POP3, IMAP
- Entendimiento de mecanismos de seguridad SPF/DKIM/DMARC
- Capacidad de interpretar logs y códigos SMTP
- Conocimientos de configuración básica Postfix/Dovecot

Duración Estimada

Distribución de Tiempo

Fase	Actividad	Duración
PRE-CLASE	Lectura documentación MkDocs	60-90 min
	Kahoot autoevaluación	15-20 min
	Total trabajo en casa	**75-110 min**
CLASE	Resolución de dudas + PowerPoint	20-30 min
	Demostración guiada	30-40 min
	Actividad Práctica 1 (DNS)	45-60 min

Fase	Actividad	Duración
	Descanso	10-15 min
	Actividad Práctica 2 (Configuración)	60-90 min
	Kahoot en vivo	10-15 min
	Cierre y síntesis	10-15 min
	Total sesión presencial	**185-265 min (3-4.5 h)**
POST-CLASE	Examen test	30-40 min

Recomendaciones de Planificación

Opción A - Sesiones de 3 horas:

- Acortar la Actividad Práctica 2 a versión simplificada (solo instalación y envío local)
- Combinar resolución de dudas con demostración

Opción B - Sesiones de 4 horas:

- Tiempo completo para ambas actividades prácticas
- Permite atender dudas individuales durante las prácticas

Opción C - Dos sesiones de 2 horas:

- Sesión 1: Dudas + Demo + Actividad 1
- Sesión 2: Actividad 2 + Kahoot + Cierre

Conceptos Clave

Los conceptos que el alumnado **DEBE** dominar al final del tema:

1. Arquitectura del Sistema de Correo

Conceptos esenciales:

- **MUA (Mail User Agent)**: Cliente de correo del usuario
- **MTA (Mail Transfer Agent)**: Servidor que transfiere correo entre sistemas (ej: Postfix)
- **MDA (Mail Delivery Agent)**: Software que almacena correo en buzón (ej: Dovecot LDA)
- **Flujo completo**: MUA origen → MTA origen → MTA destino → MDA destino → MUA destino

Importancia: Base para entender todo el sistema.

---

2. Protocolos de Comunicación

SMTP (Simple Mail Transfer Protocol):

- Puerto 25 (relay entre servidores), 587 (submission con autenticación)
- Funcionamiento basado en comandos: `HELO`, `MAIL FROM`, `RCPT TO`, `DATA`

- **Códigos de respuesta**:
  - 2xx: Éxito
  - 4xx: Error temporal (reintentar)
  - 5xx: Error permanente (bounce)

POP3 vs IMAP:

- POP3: Descarga y elimina del servidor (puerto 110/995)
- IMAP: Sincronización bidireccional (puerto 143/993)
- **Recomendación**: Usar IMAP en entornos modernos

Importancia: Necesario para troubleshooting y configuración.

---

3. DNS y Correo Electrónico

Registros críticos:

- **MX**: Define servidores de correo y prioridades
- **A/AAAA**: Resolución de nombres de servidores MX
- **PTR**: Reverse DNS (requerido para evitar spam)
- **TXT**: Contiene SPF, DKIM, DMARC

Importancia: Sin DNS correcto, el correo no funciona.

---

4. Seguridad y Autenticación

TLS/SSL:

- STARTTLS vs TLS implícito
- Puertos seguros: 465 (SMTPS), 587 (SMTP+STARTTLS), 993 (IMAPS), 995 (POP3S)

SPF (Sender Policy Framework):

- Valida que la IP de origen está autorizada por el dominio
- Formato: `v=spf1 ip4:x.x.x.x include:dominio.com -all`

DKIM (DomainKeys Identified Mail):

- Firma digital del mensaje usando criptografía
- Clave privada en servidor, clave pública en DNS

DMARC (Domain-based Message Authentication):

- Política unificada SPF+DKIM
- Políticas: `none` (monitor), `quarantine` (spam), `reject` (rechazar)

Importancia: Imprescindible para evitar spam y suplantación.

---

5. Administración de Postfix y Dovecot

Postfix (main.cf):

- Parámetros críticos: `myhostname`, `mynetworks`, `mydestination`
- **Open Relay**: Configuración insegura que permite spam
- Comandos: `postfix check`, `postfix reload`, `postqueue -p`

Dovecot:

- Configuración modular en `/etc/dovecot/conf.d/`
- `mail_location = maildir:~/Maildir`
- Autenticación y protocolos IMAP/POP3

Logs:

- Ubicación: `/var/log/mail.log` (Debian/Ubuntu)
- Lectura de códigos SMTP en logs
- Identificar: entrega exitosa, bounce, deferido

Importancia: Habilidad práctica para el puesto de trabajo.

Errores Típicos del Alumnado

1. Confusión entre Componentes (MUA/MTA/MDA)

Error común:

"Thunderbird es un MTA porque envía correos"

Corrección:

- Thunderbird es MUA (cliente del usuario)
- El MTA es el servidor (Postfix, Exim, etc.)
- El MDA es quien guarda en el buzón (Dovecot LDA, Postfix local, etc.)

Cómo prevenirlo:

- Usar el diagrama de flujo de la documentación MkDocs
- Hacer ejercicios de identificación con casos reales
- Dibujar en la pizarra el flujo completo paso a paso

---

2. No Diferenciar POP3 de IMAP

Error común:

Usar "POP3" e "IMAP" como sinónimos o no saber cuándo usar cada uno.

Corrección:

- POP3: Descarga local, ideal para un solo dispositivo
- IMAP: Sincronización, ideal para múltiples dispositivos
- IMAP es el estándar actual

Cómo prevenirlo:

- Demostrar en vivo con Thunderbird la diferencia
- Preguntar: "¿Qué pasa si leo un correo en el móvil con POP3? ¿Y con IMAP?"

---

3. Confundir Códigos SMTP 4xx y 5xx

Error común:

"Código 450 significa que el usuario no existe"

Corrección:

- 4xx = Error TEMPORAL → el servidor reintenta automáticamente
- 5xx = Error PERMANENTE → bounce al remitente
- 450 es "mailbox busy" (temporal), 550 es "user unknown" (permanente)

Cómo prevenirlo:

- Regla nemotécnica: "**4** tiene la palabra cuat**RO**, R de **Reintentar**"
- Analizar logs reales en la Actividad Práctica 2

---

4. No Comprender SPF/DKIM/DMARC

Error común:

Memorizar los nombres sin entender qué hace cada uno.

Corrección:

- SPF valida **IP de origen**
- DKIM valida **integridad del mensaje** (no alterado)
- DMARC es la **política** que dice qué hacer si fallan SPF/DKIM

Analogía útil:

- SPF = "¿Esta carta viene del cartero autorizado?"
- DKIM = "¿El sello de lacre está intacto?"
- DMARC = "Si el cartero no está autorizado o el sello está roto, ¿qué hago? ¿La acepto, la rechazo o la marco como sospechosa?"

Cómo prevenirlo:

- Usar el diagrama de flujo de validación de seguridad.md
- Hacer que consulten registros reales de dominios conocidos
- Usar la Actividad Práctica 1 para visualizar estos registros

---

5. Open Relay: No Entender el Riesgo

Error común:

Configurar `mynetworks = 0.0.0.0/0` sin entender las consecuencias.

Corrección:

- Open Relay = servidor que acepta correo de CUALQUIERA para CUALQUIER destino
- Consecuencia: Spammers lo usan, IP entra en blacklists, servidor bloqueado
- Configuración correcta: `mynetworks = 127.0.0.0/8 [::1]/128 192.168.x.0/24`

Cómo prevenirlo:

- ADVERTENCIA ENFÁTICA en la clase presencial
- Mostrar ejemplo de dominio en blacklist (MXToolbox Blacklist Check)
- Incluir pregunta específica en el examen test

---

6. No Saber Interpretar Logs

Error común:

Ver un log y no identificar si el correo se entregó o no.

Corrección:

Enseñar a buscar:

- `status=sent (250 ...)` → Entregado exitosamente
- `status=bounced (550 ...)` → Rechazado permanentemente
- `status=deferred (4xx ...)` → Error temporal, se reintentará

Cómo prevenirlo:

- Analizar logs reales durante la demostración
- En la Actividad Práctica 2, pedir que capturen fragmentos de log
- Incluir preguntas de interpretación de logs en el examen

---

7. Confundir Puertos

Error común:

"SMTP usa el puerto 25 siempre"

Corrección:

- **25**: Relay entre servidores MTA (no debe usarse para clientes)
- **587**: Submission con autenticación (clientes → servidor)
- **465**: SMTPS (TLS implícito, también para clientes)
- **143**: IMAP sin cifrar
- **993**: IMAPS (IMAP sobre TLS)
- **110**: POP3 sin cifrar

- **995**: POP3S (POP3 sobre TLS)

Cómo prevenirlo:

- Tabla de referencia en la pizarra durante toda la sesión
- Preguntar constantemente: "¿Qué puerto usamos aquí y por qué?"

---

8. No Verificar DNS Antes de Configurar

Error común:

Intentar configurar un servidor de correo sin tener registros MX correctos.

Corrección:

- **PRIMERO** configurar DNS (MX, A, PTR)
- **DESPUÉS** configurar el servidor
- Validar con `dig` antes de empezar la configuración

Cómo prevenirlo:

- Actividad Práctica 1 (DNS) ANTES de Actividad Práctica 2 (Configuración)
- Checklist de prerequisitos al inicio de la práctica 2