

T5. Correo electrónico.

BOLETÍN DE EJERCICIOS

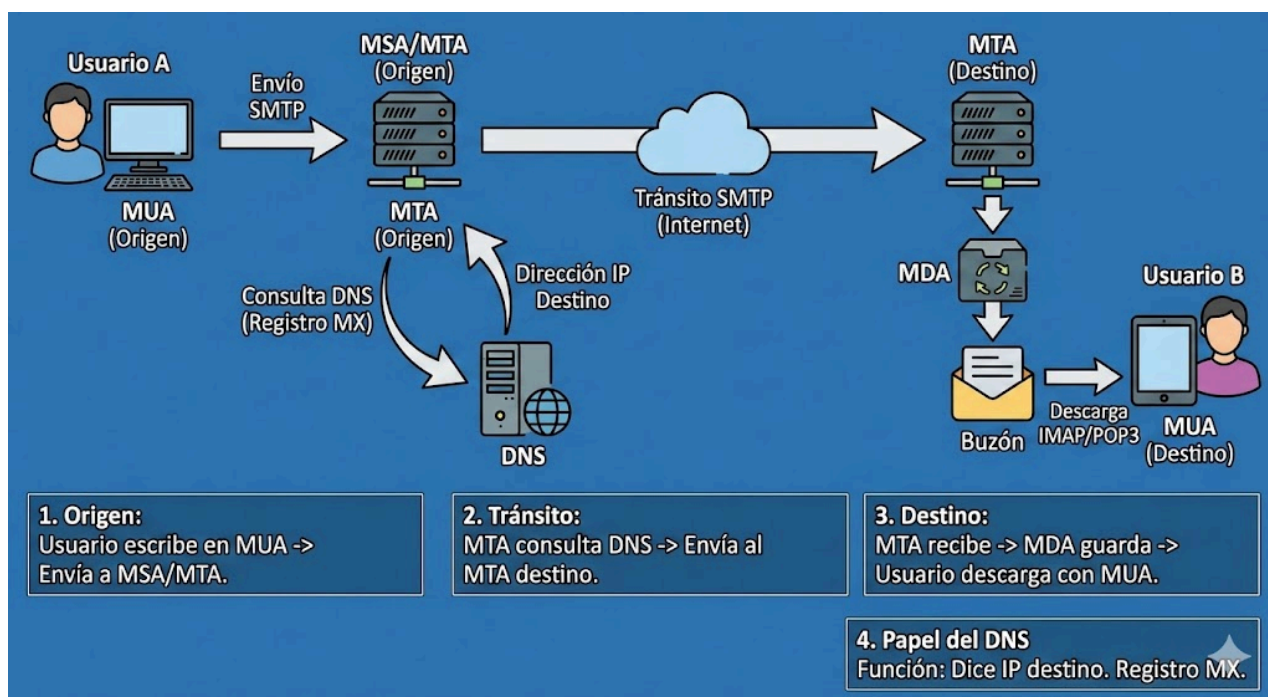
1. **Actividad Introductoria Correo.** Debes responder a las siguientes cuestiones que se te plantean, buscando la información correspondiente en la web / documentación del tema:

- a. ¿Qué **agentes** participan en el servicio de correo electrónico? Indica sus siglas en inglés y defínelos.
- MUA (Mail User Agent): Programa que usa el usuario (Outlook, Gmail).
 - MSA (Mail Submission Agent): Recibe el correo del usuario y lo valida.
 - MTA (Mail Transfer Agent): El "cartero". Transporta el correo entre servidores a través de Internet.
 - MDA (Mail Delivery Agent): Guarda el correo en el buzón final del usuario.
- b. ¿Es obligatorio introducir el encabezado **To** en un correo electrónico? ¿Qué diferencia existe entre utilizar el encabezado **Cc** y **Bcc**?

No. Se puede enviar sin destinatario visible (usando solo copia oculta).

- Cc: Los destinatarios reciben copia y todos ven las direcciones de los demás.
- Bcc: El destinatario recibe copia, pero nadie ve su dirección.

- c. Aporta un **diagrama** que clarifique el funcionamiento del correo con la presencia de todos los agentes del apartado **a)**. Apoyándote en el diagrama, explica los **pasos** que se producen desde el envío de correo por parte de un usuario hasta la recepción del mismo en otro cliente.



- d. ¿Qué papel desempeña el **DNS** en el funcionamiento del correo? Indica en qué pasos es necesario y qué registros/resoluciones se necesitan. Pon un ejemplo clarificador.

Función: Dice al servidor de origen a qué IP debe enviar el correo.

Registro necesario: Registro MX (Mail Exchanger).

Ejemplo: Si escribes a @gmail.com, el DNS busca el registro MX de Gmail para saber la dirección de sus servidores.

- e. ¿Qué **protocolos** de aplicación se usan? ¿En qué puertos y con qué protocolo de transporte? ¿en qué **pasos** del funcionamiento del correo? ¿entre qué agentes? ¿Qué protocolos son inseguros?

Protocolo	Función	Puertos (Inseguro / Seguro)	Agentes
SMTP	Enviar / Transferir	25, 587 / 465	MUA \rightarrow MTA y MTA \rightarrow MTA
POP3	Descargar (borra del server)	110 / 995	Servidor \rightarrow MUA
IMAP	Sincronizar (lee en server)	143 / 993	Servidor \leftrightarrow MUA

- f. Busca en Internet el vídeo más ilustrativo y de mayor calidad relacionado con el funcionamiento del servicio de correo electrónico. No importa si es en inglés.

 How Email Works

- g. Resume los comandos y respuestas de una interacción exitosa del protocolo de **envío** de correo. Mediante la utilidad de terminal remoto telnet prueba a interactuar con un servidor envío de correo y enviar un correo.

HELO: Saludo.

MAIL FROM: Tu correo.

RCPT TO: Destinatario.

DATA: Escribir mensaje (Asunto y cuerpo).

.: Punto final para enviar.

QUIT: Salir.

- h. Resume los comandos y respuestas de una interacción exitosa del protocolo de **recepción de correo**.

USER: Tu usuario.

PASS: Tu contraseña.

LIST: Ver lista de mensajes.

RETR 1: Leer mensaje 1.

DELE 1: Borrar mensaje 1.

QUIT: Salir.

2. Clientes de correo electrónico (MUA). Debes responder a las siguientes cuestiones que se te plantean, buscando la información correspondiente en la web:


a. ¿Qué acciones/consejos puedes indicar para protegerte de correos maliciosos o de spam independientemente del cliente de correo que utilices?

- Verifica el remitente: No mires solo el nombre, mira la dirección real (ejemplo@paypal-seguridad.com es falso; soporte@paypal.com es real).
- No descargues adjuntos inesperados: Especialmente .zip, .exe o documentos de Office con macros.
- Desactiva la carga automática de imágenes: Evita que los spammers sepan que has abierto el correo (pixel tracking).
- No hagas clic en "Darse de baja": Si el correo es claramente spam, hacer clic ahí solo confirma que tu cuenta existe. Márcalo como Spam.
- Usa 2FA: Activa la autenticación en dos pasos en tu cuenta.

b. ¿Cuántos tipos de clientes de correo existen? ¿Cuáles son? ¿En qué se diferencian unos de otros?

- Webmail (Correo Web):
 - Qué es: Se accede desde el navegador (Chrome, Edge). Todo está en la nube.
 - Ejemplo: Gmail, Outlook.com, Yahoo.
 - Ventaja: Accesible desde cualquier sitio sin instalar nada.
- Cliente de Escritorio (MUA Local):
 - Qué es: Programa instalado en el ordenador. Descarga y guarda los correos en tu disco duro.
 - Ejemplo: Thunderbird, Microsoft Outlook, Evolution.
 - Ventaja: Funciona sin internet (offline), gestiona varias cuentas mejor y es más rápido.

- c. ¿Qué clientes de correo vía web conoces? Enuméralos, escribe una breve reseña en la que des tu opinión sobre los que hayas utilizado y establece un sistema de puntuación para señalar los mejores.

Cliente Web	Reseña y Opinión	Puntuación
Roundcube	El más equilibrado. Tiene una interfaz moderna (AJAX), admite arrastrar y soltar correos, y es fácil de usar. Es el estándar actual en la mayoría de hostings porque se siente como una aplicación de escritorio.	 (5/5)
Horde	El más completo (Groupware). No solo es correo, incluye agenda, notas, tareas y herramientas colaborativas. Es muy potente, pero su interfaz suele ser más lenta y recargada ("estilo antiguo").	 (4/5)
RainLoop	El más moderno y ligero. Su diseño es minimalista y muy rápido. Lo mejor es que no guarda correos en su base de datos (accede directo al servidor), lo que lo hace muy seguro y fácil de mantener. <i>(Nota: Su sucesor actual es SnappyMail).</i>	 (4.5/5)
SquirrelMail	El clásico (Legacy). Interfaz de solo texto/HTML básico. Es feo y antiguo, pero extremadamente rápido y compatible con cualquier navegador, incluso de hace 20 años. Ya casi no se usa.	 (2/5)

- d. Busca en Internet el vídeo más ilustrativo y de mayor calidad relacionado con los servicios de correo electrónico a nivel de cliente.

 [What Is the Difference Between Email Clients and Webmail? - TheEmailToolbox.c...](#)

- e. Realiza una tabla comparativa, de clientes de correo para, según la plantilla siguiente indicando si poseen cada una de las características que se incluyen.

Características	Mailtrim	Thunderbird	Evolution
Generales			
Organizador (Calendario, agenda...)	x	x	x
Soporte para varias cuentas de correo	x	x	x
Integración con el escritorio	Media	Alta	Alta
Notificaciones sobre mensajes	x	x	x
Posibilidad de trabajar off-line	x	x	x
Libreta de direcciones	x	x	x
Importación de cuentas	Limitada	x	x
Protocolos de correo			
POP	x	x	x
IMAP	x	x	x
SMTP	x	x	x
Filtrado y seguridad			
Cifrado		x	x
Filtros correo no deseado	Básico	x	x
Filtros suplantación de identidad (phishing)		x	x
Firma digital		x	x
Copias de seguridad	Manual	Plugins	Plugins

3. MUA II. Configuración del cliente de correo **Mozilla Thunderbird**. Para ello:

- Configura el cliente de correo Mozilla Thunderbird para usar una cuenta de Gmail y otra Outlook bajo el sistema operativo Ubuntu Desktop. Realiza la configuración usando el protocolo IMAP.

Abre Thunderbird.

En la página de inicio (o menú ≡ Nuevo), elige "**Cuenta de correo existente**".



Configurar su dirección de correo electrónico existente.

Para utilizar su cuenta de correo electrónico actual, introduzca sus credenciales.
Thunderbird buscará automáticamente una configuración de servidor recomendada y que funcione.

Nombre completo
John Doe

Dirección de correo electrónico
john.doe@example.com

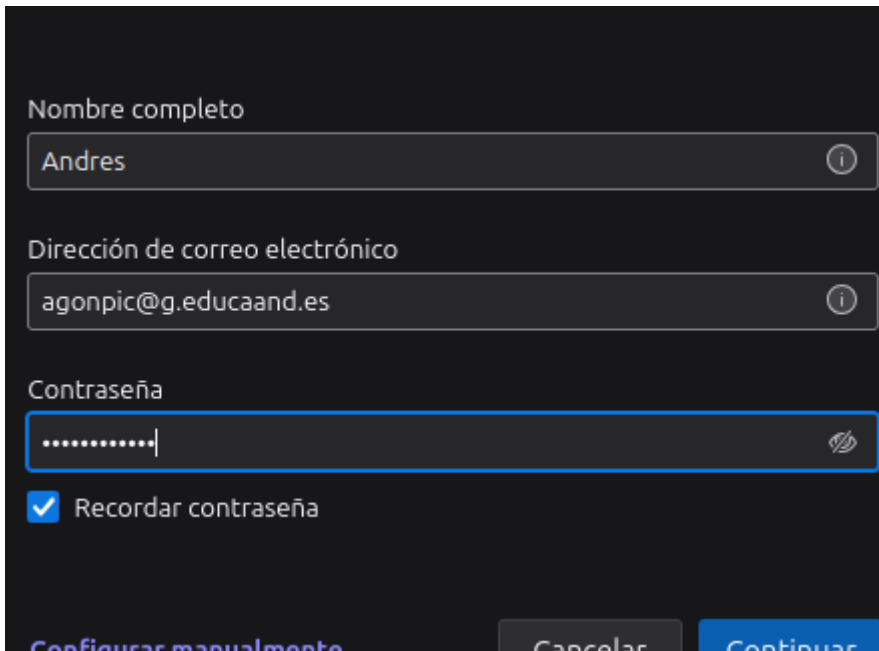
Contraseña

☒ Recordar contraseña

Cancelar Continuar



Escribe tu **Nombre**, **Dirección de correo** y **Contraseña**.



Nombre completo
Andres

Dirección de correo electrónico
agonpic@g.educaand.es

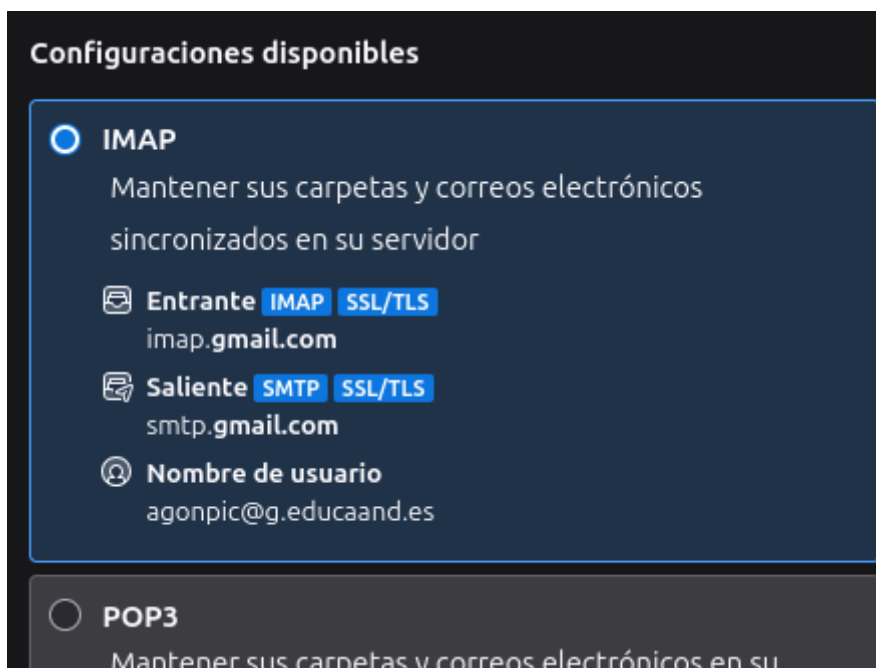
Contraseña
.....

☒ Recordar contraseña

Configurar manualmente Cancelar Continuar

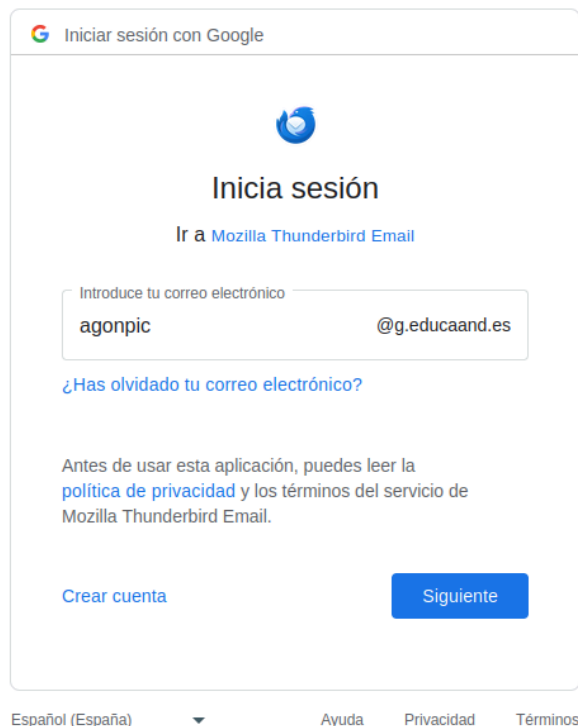
Pulsa **"Continuar"**.

IMPORTANTE: Thunderbird detectará la configuración. Asegúrate de que marca la opción **IMAP (Carpetas remotas)** y no POP3.



Pulsa **"Hecho"**.

Autenticación moderna (OAuth2): Se abrirá una ventana emergente del navegador (Google o Microsoft). Inicia sesión ahí y da permiso a Thunderbird.



- b. Envía un correo a tu cuenta de correo de Gmail usando Thunderbird.
 - 1. En Thunderbird, pulsa el botón "Redactar".
 - 2. En el campo "Desde:", selecciona tu cuenta de Outlook.
 - 3. En "Para:", escribe tu dirección de Gmail.
 - 4. Asunto: "Prueba Thunderbird Ubuntu".
 - 5. Enviar.
 - 6. Abre tu navegador (Firefox/Chrome), entra en gmail.com e inicia sesión. Verás el correo en la Bandeja de entrada. Esto confirma que el envío (SMTP) y la recepción funcionan.
- c. Consulta el correo de vía web.
- d. Configura la cuenta de correo en algún dispositivo móvil de que dispongas. Debes sincronizar la configuración para que todos los dispositivos tengan el correo actualizado.

Para tener el correo actualizado en todos lados (PC y Móvil), la clave es usar **siempre el protocolo IMAP**.


Instrucciones:

- 1. En tu móvil (Android/iOS), ve a Ajustes > Cuentas o abre la app de Gmail/Outlook.
- 2. Añade la cuenta.
- 3. El móvil elegirá **IMAP** automáticamente por defecto.

¿Por qué se sincroniza?

Al usar IMAP en el PC (Thunderbird) y en el Móvil, ambos dispositivos miran al servidor.

- e. Si lees un correo en el móvil, en Thunderbird aparecerá como "leído".
 - f. Si envías un correo desde Thunderbird, aparecerá en "Enviados" en tu móvil.
 - g. No tienes que hacer nada extra; es la función nativa de IMAP.
-
- h. Busca en Youtube algún vídeo explicativo de la configuración de la cuenta de correo en Thunderbird que sea de calidad, actualizado y técnicamente interesante.

 [Thunderbird - Lesson 1 - Setting Up Thunderbird](#)

4. **(E) EMAIL Server.** Objetivo: crear un servidor de envío de correo electrónico funcional. Para ello, debes configurar un servidor de correo personalizando una imagen docker de IRedMail en tu Servidor Docker, bajo el nombre de dominio **que elijas**, teniendo en cuenta los apartados que se detallan a continuación:

- i. Configura la zona de tu dominio en el servidor DNS del aula:
 - a. Conteniendo el registro MX apuntando hacia **mail.tudominio.tld**
 - b. De manera que dicho nombre resuelva como la **ip tu servidor** de correo (será la misma del servidor Docker) y viceversa.

```
$TTL      1D

@ IN SOA dnsdjfr.institutodh.net. root.institutodh.net. (
                        2025112701 ; Serial Basado en el dia e
incrementando
                        604800 ; Refresh
                        86400 ; Retry
                        2419200 ; Expire
                        604800 ) ; Default TTL

; Servidores DNS del dominio
                IN      NS                dnsdjfr.institutodh.net.

; Correo
                IN      MX 10      mail.policia.es.

; Directas
mail IN A 10.2.3.25

; Alias o sinonimo
mx IN CNAME mail
smtp IN CNAME mail
```

ii. Configuración de un servidor de correo SMTP usando **IRedMail**:

- a. Configura la **Ip estática** de tu servidor Docker y elige como DNS del profesor (10.255.0.75).

```
network:
  version: 2
  ethernets:
    ens18:
      addresses:
        - "10.2.3.25/24"
      nameservers:
        addresses:
          - 10.255.0.75
          - 1.1.1.1
        search: []
      routes:
        - to: "default"
          via: "10.2.3.1"
```

- b. Bajala imagen del servidor de correo iRedMail y siguiendo estas [instrucciones](#) ejecútalo para que:

- i. Configura el **FQDN** (nombre completo **mail.tudominio.tld**). [Ver ayuda en dockerhub](#).

```
docker run --rm --name iredmail --env-file iredmail-docker.conf
--hostname mail.policia.es -p 80:80 -p 443:443 -p 110:110 -p
995:995 -p 143:143 -p 993:993 -p 25:25 -p 465:465 -p
587:587 -v /iredmail/data/backup-mysql:/var/vmail/backup/mysql -v
/iredmail/data/mailboxes:/var/vmail/vmail1 -v
/iredmail/data/mlmmj:/var/vmail/mlmmj -v
/iredmail/data/mlmmj-archive:/var/vmail/mlmmj-archive -v
/iredmail/data/imap sieve_copy:/var/vmail/imap sieve_copy -v
/iredmail/data/custom:/opt/iredmail/custom -v
/iredmail/data/ssl:/opt/iredmail/ssl -v /iredmail/data/mysql:/var/lib/mysql
-v /iredmail/data/clamav:/var/lib/clamav -v
/iredmail/data/sa_rules:/var/lib/spamassassin -v
/iredmail/data/postfix_queue:/var/spool/postfix iredmail/mariadb:stable
```

- ii. Define los dominios para los que se acepta correo entrante y reenvío. [Ver ayuda en DockerHub](#). Comprueba dentro del contenedor el valor de la variable [mydestinations](#) de la configuración de postfix.

HOSTNAME=mail.policia.es

FIRST_MAIL_DOMAIN=policia.es

FIRST_MAIL_DOMAIN_ADMIN_PASSWORD=Naruto@1234

MLMMJADMIN_API_TOKEN=lkwmMLkVnafNBx2vXNGMu1HdQUM/b+G
TsVKqpEOqqgY=

ROUNDcube_DES_KEY=ozcUAZ7n1ErA/L+/FIb0kB34GLeNUJFN

- iii. Usa el filtro [Amavis](#) para crear una lista negra de manera que no se acepte correo entrante del correo [spammer@l.io](#) y desde otro dominio que tu elijas.

listar plugins

```
root@mail:/# nano /opt/iredapd/plugins/
__init__.py          reject_null_sender.py      sql_ml_access_policy.py
__pycache__          reject_sender_login_mismatch.py  throttle.py
amavisd_wblist.py    reject_to_hostname.py      wblast_rdns.py
greylisting.py       senderscore.py             whitelist_outbound_recipient.py
ldap_force_change_password.py  sql_alias_access_policy.py
ldap_maillist_access_policy.py  sql_force_change_password.py
root@mail:/# nano /opt/iredapd/plugins/
```

Añadir a la config

```
# Enabled plugins.
plugins = ['reject_null_sender', 'reject_sender_login_mismatch', 'greylisting', 'throttle', 'amavisd_wblist', 's
# SRS (Sender Rewriting Scheme)
```

cd /opt/iredapd/tools/

python3 wblast_admin.py --add --blacklist spammer@l.io @.

```
root@mail:/# cd /opt/iredapd/tools/
root@mail:/opt/iredapd/tools# python3 wblast_admin.py --add --blacklist spammer@l.io @.
* Establishing SQL connection.
* Add inbound blacklist for account: @.
* Add senders: spammer@l.io, @.
root@mail:/opt/iredapd/tools# |
```

python3 wblast_admin.py --add --blacklist takumi@initiald.com @.

```
root@mail:/opt/iredapd/tools# python3 wblast_admin.py --add --blacklist takumi@initiald.com @.
* Establishing SQL connection.
* Add inbound blacklist for account: @.
* Add senders: takumi@initiald.com, @.
root@mail:/opt/iredapd/tools# |
```

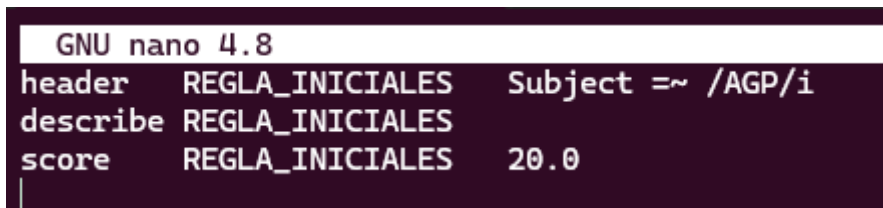
- iv. Configura [SpamAssassin](#) para que califique como spam los mensajes que tengan tus **iniciales** en el Asunto. Aporta pruebas en el siguiente ejercicio.

```
nano /opt/iredmail/custom/spamassassin/custom.cf
```

```
header REGLA_INICIALES Subject =~ /AGP/i
```

```
describe REGLA_INICIALES
```

```
score REGLA_INICIALES 20.0
```



```
GNU nano 4.8
header REGLA_INICIALES Subject =~ /AGP/i
describe REGLA_INICIALES
score REGLA_INICIALES 20.0
|
```

```
service amavis restart
```

- v. Para evitar los intentos de adivinación de contraseñas, iRedMail usa [fail2ban](#). Muestra las líneas de configuración que provocan el baneo de los atacantes. ~~Muestra los logs de un baneo por múltiples fallos de autenticación.~~ (Ayuda: mira /etc/fail2ban)

```
nano /opt/iredmail/custom/fail2ban/jail.local
```

```
[dovecot-iredmail]
```

```
enabled = true
```

```
filter = dovecot.iredmail
```

```
logpath = /var/log/dovecot.log
```





```
maxretry = 5
```

```
bantime = 60m
```

```
findtime = 5m
```

```
action = iptables-multiport[name=dovecot,
port="pop3,pop3s,imap,imaps,sieve", protocol=tcp]
```

- c. Configura el servidor para que utilice cifrado (SSL/TLS). Simplemente comprueba que los puertos de los servicios cifrados están activos y averigua dónde se encuentran los certificados que está usando (ficheros .key, .crt) ¿cómo podrías configurar un certificado válido?
- d. Añade algunas cuentas de usuario mediante el panel de administración de iRedMail (usuario *postmaster@tudominio*, web: <https://ip/iredadmin>)

<input type="checkbox"/> Display Name	Mail Address	User/Employee ID	Quota
<input type="checkbox"/> Andres	 andres@policia.es		18 KB / Unlimited
<input type="checkbox"/> neo	 neo@policia.es		326 Bytes / Unlimited
<input type="checkbox"/> postmaster	  postmaster@policia.es		86 KB / Unlimited

Choose Action ▼ Apply

- iii. Realiza las siguientes pruebas de funcionamiento con el cliente **webmail (roundcube)** conectándote al propio servidor vía web.
 - a. Correo entre usuarios locales del servidor. Crea los que sean necesarios, relacionados con tu nombre de dominio. Aporta los logs que muestran el envío y la entrega del correo. Aporta los envíos, la comprobación de correo, y las respuestas.
 - b. Correo desde un usuario local a un usuario de otro servidor de clase. Aporta los logs del envío.
 - c. Correo desde un usuario local a un destinatario exterior. Aporta los logs del envío.
 - d. Aporta la prueba de recepción de correo de otro compañero de clase.
 - e. Envía los correos necesarios para las pruebas del apartado anterior.

5. **MUA + EMAIL Server.** Configura el cliente de correo **Thunderbird** para usar una cuenta de correo en tu servidor iRedMail de manera cifrada y:

- a. Envía un correo desde la cuenta de un usuario de tu dominio a una cuenta de correo externa.
- b. [Crea un par de claves PGP](#) para tu cuenta de correo y envía un correo cifrado y firmado desde la cuenta de un usuario de tu dominio a otro usuario del aula. Dicho usuario debe responderte.
- c. Configura tu cliente de correo para tener en cuenta los correos marcados como SPAM por SpamAssassin y que se muevan a la carpeta de Correo No Deseado.
- d. Envía los correos necesarios para las pruebas del ejercicio anterior.

6. **GPG** Instala el complemento mailvelope en Chrome y a continuación:

- a. Crea la clave privada y pública PGP.
- b. Publica tu clave en el servidor de claves de mailvelope.
- c. Envía un mensaje a UN COMPAÑERO indicando ejercicio realizado, cifrándolo y firmándolo.
- d. Descripta la respuesta del COMPAÑERO, comprobando que es legítima.