**Apuntes Correo**

Contenido

[1. Actividad Introductoria Correo 4](#_Toc218787211)

[a. ¿Qué agentes participan en el servicio de correo electrónico? Indica sus siglas en inglés y defínelos. 4](#_Toc218787212)

[b. ¿Es obligatorio introducir el encabezado To en un correo electrónico? ¿Qué diferencia existe entre utilizar el encabezado Cc y Bcc? 4](#_Toc218787213)

[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. 5](#_Toc218787214)

[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. 6](#_Toc218787215)

[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? 6](#_Toc218787216)

[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. 6](#_Toc218787217)

[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. 7](#_Toc218787218)

[h. Resume los comandos y respuestas de una interacción exitosa del protocolo de recepción de correo. 7](#_Toc218787219)

[2. Clientes de correo electrónico (MUA). 8](#_Toc218787220)

[a. ¿Qué acciones/consejos puedes indicar para protegerte de correos maliciosos o de spam independientemente del cliente de correo que utilices? 8](#_Toc218787221)

[b. ¿Cuántos tipos de clientes de correo existen? ¿Cuáles son? ¿En qué se diferencian unos de otros? 8](#_Toc218787222)

[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. 9](#_Toc218787223)

[d. Busca en Internet el vídeo más ilustrativo y de mayor calidad relacionado con los servicios de correo electrónico a nivel de cliente. 10](#_Toc218787224)

[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. 11](#_Toc218787225)

[3. MUA II. Configuración del cliente de correo Mozilla Thunderbird. Para ello: 13](#_Toc218787226)

[a. 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. 13](#_Toc218787227)

[Gmail 14](#_Toc218787228)

[Outlook 19](#_Toc218787229)

[b. Envía un correo a tu cuenta de correo de Gmail usando Thunderbird. 21](#_Toc218787230)

[c. Consulta el correo de vía web. 21](#_Toc218787231)

[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. 21](#_Toc218787232)

[e. Busca en Youtube algún vídeo explicativo de la configuración de la cuenta de correo en Thunderbird que sea de calidad, actualizado y técnicamente interesante. 22](#_Toc218787233)

[4. (E) EMAIL Server. 23](#_Toc218787234)

[I. Configura la zona de tu dominio en el servidor DNS del aula: 24](#_Toc218787235)

[a. Conteniendo el registro MX apuntando hacia ***mail.tudominio.tld*** 24](#_Toc218787236)

[b. De manera que dicho nombre resuelva como la **ip tu servidor** de correo (será la misma del servidor Docker) y viceversa. 24](#_Toc218787237)

[II. Configuración de un servidor de correo SMTP usando **IRedMail**: 25](#_Toc218787238)

[a. Configura la **Ip estática** de tu servidor Docker y elige como DNS del profesor (10.255.0.75). 25](#_Toc218787239)

[b. Baja la imagen del servidor de correo iRedMail y siguiendo estas instrucciones ejecútalo para que: 26](#_Toc218787240)

[**Amavis** 29](#_Toc218787241)

[SpamAssasin 32](#_Toc218787242)

[***fail2ban*** 34](#_Toc218787243)

[SSL/**TLS** 37](#_Toc218787244)

[**Añadir cuentas de usuario.** 39](#_Toc218787245)

[iii. Realiza las siguientes pruebas de funcionamiento con el cliente webmail (roundcube) conectándote al propio servidor vía web. 41](#_Toc218787246)

[5. MUA + EMAIL Server. 50](#_Toc218787247)

[**PGP** 51](#_Toc218787248)

[**Exportar tu clave PGP.** 56](#_Toc218787249)

[**Importar PGP.** 57](#_Toc218787250)

[Configurar ThunderBird con SpamAssasin. 58](#_Toc218787251)

[6. **GPG** Instala el complemento ***mailvelope*** en Chrome y a continuación: 60](#_Toc218787252)

[Nombre de los Dominios de cada uno 65](#_Toc218787253)

[PONER EL PROMPT DE TU NOMBRE Y ETC 67](#_Toc218787254)

[Comandos para comprobar log de correos 68](#_Toc218787255)

1. Actividad Introductoria Correo.

Debes responder a las siguientes cuestiones que se te plantean, buscando la información correspondiente en la web / documentación del tema:

## ¿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.

## ¿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.

## 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.

Diagrama

El contenido generado por IA puede ser incorrecto.

## ¿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.

## ¿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 $\to$ MTA y MTA $\to$ MTA |
| **POP3** | Descargar (borra del server) | 110 / 995 | Servidor $\to$ MUA |
| **IMAP** | Sincronizar (lee en server) | 143 / 993 | Servidor $\leftrightarrow$ MUA |

## 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

Canal: PowerCert Animated Videos

<https://www.youtube.com/watch?v=ELioaGg4WOY>

## 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.

## 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.

1. Clientes de correo electrónico (MUA).

Debes responder a las siguientes cuestiones que se te plantean, buscando la información correspondiente en la web:

## ¿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.

## ¿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.

## ¿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. (*Nota: Su sucesor actual es* ***SnappyMail****)* | ⭐⭐⭐⭐  (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) |

## 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.com

Canal: The Email Toolbox

<https://www.youtube.com/watch?v=wsN01FKC54I>

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

Una captura de pantalla de un celular con letras

El contenido generado por IA puede ser incorrecto.Tabla

El contenido generado por IA puede ser incorrecto.

# 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**".

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

### Gmail

Escribe tus datos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

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

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Pulsa "**Hecho**".

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

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

### Outlook

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Pass: Usuario.12345

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Outlook tiene problemas al mandar, pero al final llegan:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

## 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.

## Consulta el correo de vía web.

## 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.

1. Si lees un correo en el móvil, en Thunderbird aparecerá como "leído".
2. Si envías un correo desde Thunderbird, aparecerá en "Enviados" en tu móvil.
3. No tienes que hacer nada extra; es la función nativa de IMAP.

## 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

Canal: TutorTube

<https://www.youtube.com/watch?v=AHzcPpacOpQ>

# (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:*

## Configura la zona de tu dominio en el servidor DNS del aula:

### Conteniendo el registro MX apuntando hacia ***mail.tudominio.tld***

### De manera que dicho nombre resuelva como la **ip tu servidor** de correo (será la misma del servidor Docker) y viceversa.

//Configuración de named.conf.local

// Archivo para busquedas directas

zone "initiald.com" {

type master;

file "db.initiald.com"; // Debe estar en /var/cache/bind/

allow-update { none; };

};

// Configuración de db.initiald.com

Bind data file

; PLANTILLA DE AYUDA PARA DNS

; GUARDAR COMO db.initiald.com

; BIND data file for initiald.com

;

$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.initiald.com.

; Directas

mail IN A 10.2.7.25

; Alias o sinonimo

mx IN CNAME mail

smtp IN CNAME mail

## Configuración de un servidor de correo SMTP usando **IRedMail**:

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

Texto

El contenido generado por IA puede ser incorrecto.

También en el archivo “**/etc/resolv.conf**”. ¿Esto se hace dentro del contenedor o en servidor Docker? Lo he puesto en ambos. **Creo que en realidad no hace falta**.

Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

### Baja la imagen del servidor de correo iRedMail y siguiendo estas [instrucciones](https://hub.docker.com/r/iredmail/mariadb) ejecútalo para que:

* + 1. Configura el **FQDN** (nombre completo ***mail.tudominio.tld***). [Ver ayuda en dockerhub](https://hub.docker.com/r/iredmail/mariadb).
    2. Define los dominios para los que se acepta correo entrante y reenvío. [Ver ayuda en DockerHub](https://hub.docker.com/r/iredmail/mariadb). Comprueba dentro del contenedor el valor de la variable [***mydestinations***](https://www.postfix.org/postconf.5.html#mydestination) de la configuración de postfix.

En la VM (o máquina real) donde vamos a tener los contenedores de docker:

* Instalamos Docker:

**apt update**

**apt install -y docker.io**

(Opcional) apt intall docker-compose (o docker-compose-v2)

* Creamos un directorio para iRedMail:

**mkdir /iredmail**

* Nos situamos en él. Creamos el archivo con los siguientes datos:

***echo HOSTNAME=mail.initiald.com >> iredmail-docker.conf***

***echo FIRST\_MAIL\_DOMAIN=initiald.com >> iredmail-docker.conf***

***echo FIRST\_MAIL\_DOMAIN\_ADMIN\_PASSWORD=12345 >> iredmail-docker.conf***

***echo MLMMJADMIN\_API\_TOKEN=$(openssl rand -base64 32) >> iredmail-docker.conf***

***echo ROUNDCUBE\_DES\_KEY=$(openssl rand -base64 24) >> iredmail-docker.conf***

* Creamos una serie de ficheros para el contenedor.

***mkdir -p data/{backup-mysql,clamav,custom,imapsieve\_copy,mailboxes,mlmmj,mlmmj-archive,mysql,sa\_rules,ssl,postfix\_queue}***

* Creamos un archivo .sh que usaremos para crear el contenedor.

**iredmail.sh**

***docker run \***

***--rm \***

***-d \***

***--name iredmail \***

***--env-file iredmail-docker.conf \***

***--hostname mail.initiald.com \***

***-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/imapsieve\_copy:/var/vmail/imapsieve\_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***

Ahora ejecutamos el archivo, pero debemos hacerlo como ROOT (no vale hacer un sudo).

**sh iredmail.sh**

Para entrar en el contenedor

**docker exec -ti iredmail /bin/bash**

Una vez dentro del contenedor, comprobamos el valor de “**mydestination**”.

**cat /etc/postfix/main.cf | grep mydestination**



**cat /etc/postfix/main.cf | grep hostname**

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

**ATENCIÓN**: **ClamAV** puede petarte el disco porque se pone a hacer actualizaciones, etc. Para evitarlo, no hay otra forma de pararlo que cambiarle el nombre.

Renombra el clam: **/usr/sbin/clamd**

Le pones cualquier NOMBRE Y YA ESTÁ. usa mv.

**mv /usr/sbin/clamd /usr/sbin/STOPclamd**

Versión ClamAV: **clamd -V**

* + 1. Usa el filtro [Amavis](https://docs.iredmail.org/manage.iredapd.html) para crear una lista negra de manera que no se acepte correo entrante del correo [spammer@](mailto:spammer@institutodh.net)l.io y desde otro dominio que tu elijas.

### **Amavis**

Listamos los plugins: ls -l /opt/iredapd/plugins/

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

Ahora debemos introducir en el listado de plugins activos el que vamos a crear más adelante, para ello modificamos el archivo de configuración:

**nano /opt/iredapd/settings.py**

Nos vamos a la sección “Enabled plugins” he introducimos: 'wblist\_admin'

Código QR

El contenido generado por IA puede ser incorrecto.

Ahora nos situamos en la carpeta de plugins: **/opt/iredapd/tools**

Para desactivar el **greylisting** y permitir que mande a todo el mundo de manera más rápida para el examen, usa[[1]](#footnote-1):

**python3 /opt/iredapd/tools/greylisting\_admin.py --disable --from '@.'**

**python3 /opt/iredapd/tools/greylisting\_admin.py --disable --from '@.'**

**python3 /opt/iredapd/tools/greylisting\_admin.py --disable --from '.'**



Comprobar estado de greylisting:

**“python3 /opt/iredapd/tools/greylisting\_admin.py --list"**

*“What this command does*

*--disable: Sets the greylisting status to disabled for the specified sender/recipient pair.*

*--from '@.': This is a wildcard in iRedAPD that represents any sender address.*

*Result: It inserts a record into the iredapd database (usually PostgreSQL or MariaDB) that tells the policy server to skip the "451" temporary rejection (greylisting) for all incoming mail.”*

Para añadir a la lista negra.

**python3 wblist\_admin.py --add --blacklist spammer@l.io**

CREO QUE ES MEJOR QUITAR EL ARROBA PUNTO, PORQUE BLOQUEA TU PROPIO DOMINIO.

Texto

El contenido generado por IA puede ser incorrecto.

Es probable que no tengamos Python en el contenedor.

**apt install python**

**pip install web.py**

**apt-get install python3-pip**

Ahora introducimos otro nombre en la lista negra.

**python3 wblist\_admin.py --add --blacklist neo@policia.es**

Texto

El contenido generado por IA puede ser incorrecto.

Si queremos quitar a alguien de la lista negra:

**python3 wblist\_admin.py --delete --blacklist @.**

Para ver a quien tenemos en la lista negra o blanca, usamos:

<https://docs.iredmail.org/amavisd.wblist.html>

**python3 wblist\_admin.py --list --whitelist**

Texto

El contenido generado por IA puede ser incorrecto.

**python3 wblist\_admin.py --list --blacklist**

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

**ATENCIÓN**: Es posible que también tengamos que establecer en la **white list** para poder enviar-recibir correos desde determinadas direcciones:

Ejemplo servidor de Andrés:

**python3 /opt/iredapd/tools/wblist\_admin.py --add --whitelist 10.2.3.25**

**ATENCIÓN:** Parece ser que cuando activamos las blacklist-whitelist, le da el siroco y te bloquea también tu propio servidor, por lo que no puedes mandar correos entre usuarios de tu dominio. Solución básica: pon el localhost en la whitelist.

**python3 /opt/iredapd/tools/wblist\_admin.py --add --whitelist 127.0.0.1**

* + 1. Configura [SpamAssasin](https://docs.google.com/presentation/d/1Z6cUcK0y9J0Kh_rnMUgXux_o6qA1BJz_VpozEGWiQag/edit#slide=id.g11363e58b8a_0_13) para que califique como spam los mensajes que tengan tus ***iniciales*** en el Asunto. Aporta pruebas en el siguiente ejercicio.

### [SpamAssasin](https://docs.google.com/presentation/d/1Z6cUcK0y9J0Kh_rnMUgXux_o6qA1BJz_VpozEGWiQag/edit#slide=id.g11363e58b8a_0_13)

**NO USAR. PROVOCA ERROR DE SMTP 451 SIN SOLUCIÓN.**

**Método 1:**

Fuera del contenedor, en el servidor, nos situamos en **/iredmail/data/sa\_rules/3.004004/updates\_spamassassin\_org**

Allí hay un archivo “local.cf” que usaremos como plantilla para nuestra tarea, lo copiamos.

**cp local.cf csa.cf**

Introducimos:

***# --- Configuración para bloquear 'CSA' en el Asunto ---***

***# 1. Definición de la Regla (Pattern Match):***

***# Busca 'CSA' (insensible a mayúsculas/minúsculas) en el campo Subject.***

***header SUBJECT\_HAS\_MY\_INITIALS Subject =~ /CSA/i***

***# 2. Descripción:***

***describe SUBJECT\_HAS\_MY\_INITIALS Asunto contiene mis iniciales (CSA)***

***# 3. Puntuación (Score):***

***# Una puntuación de 10.0 es suficiente para marcar el correo como spam***

***score SUBJECT\_HAS\_MY\_INITIALS 10.0***

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Recargamos la configuración:

Tienes que reiniciar el contenedor:

**docker restart iredmail**

**Método Andrés:**

Desde dentro del contenedor:

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

**header REGLA\_INICIALES Subject =~ /CSA/i**

**describe REGLA\_INICIALES**

**score REGLA\_INICIALES 20.0**

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

**service amavis restart**

* + 1. Para evitar los intentos de adivinación de contraseñas, iRedMail usa [***fail2ban***](https://www.fail2ban.org/wiki/index.php/Postfix). 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)

### [***fail2ban***](https://www.fail2ban.org/wiki/index.php/Postfix)

**Método 1:**

<https://docs.iredmail.org/fail2ban.sql.html>

*“When some (bad) client triggers the ban, Fail2ban will perform actions defined in action = parameter in jail config file. For example, in jail dovecot (/etc/fail2ban/jail.d/dovecot.local):”*

**cat /etc/fail2ban/jail.d/dovecot.local**

Texto

El contenido generado por IA puede ser incorrecto.

Log:

cat /var/log/dovecot/dovecot.log



**Método Andrés:**

Desde dentro del contenedor:

**mkdir -p /opt/iredmail/custom/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]*

Texto

El contenido generado por IA puede ser incorrecto.

**Desglose de la configuración**

* **[dovecot-iredmail]**: Es el nombre de la sección o "jaula". Sirve para identificar estas reglas específicas dentro de Fail2ban.
* **enabled = true**: Indica que esta protección está **activa**. Si estuviera en false, Fail2ban ignoraría estas reglas.
* **filter = dovecot.iredmail**: Le dice a Fail2ban qué patrón de búsqueda debe usar. Buscará un archivo llamado dovecot.iredmail.conf en el directorio de filtros para saber exactamente qué errores de inicio de sesión se consideran "ataques".
* **logpath = /var/log/dovecot.log**: Es la ruta del archivo donde Dovecot anota todo lo que pasa. Fail2ban "lee" este archivo en tiempo real para buscar intrusos.
* **maxretry = 5**: Es el número de intentos permitidos. Si una IP falla **5 veces** al intentar entrar, será bloqueada.
* **bantime = 60m**: Es la duración del castigo. La IP atacante no podrá conectarse durante **60 minutos**.
* **findtime = 5m**: Es la ventana de tiempo. Los 5 fallos (maxretry) deben ocurrir dentro de un periodo de **5 minutos** para que se active el baneo.
* **action = iptables-multiport[...]**: Define **cómo** se bloquea al atacante:
  + Usa iptables para cerrar el paso.
  + Cierra los puertos específicos del correo: pop3, pop3s, imap, imaps y sieve.
  + Solo afecta al protocolo tcp.

**¿Cómo funciona en la práctica?**

1. Un bot intenta adivinar una contraseña de correo 5 veces en menos de 5 minutos.
2. Dovecot escribe esos fallos en /var/log/dovecot.log.
3. Fail2ban detecta esos fallos gracias al filtro dovecot.iredmail.
4. Fail2ban ejecuta una orden de iptables que prohíbe a esa IP acercarse a los puertos de correo durante una hora.
   1. 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?

### SSL/**TLS**

**Encontrar en etc, encontrar los archivos .key y .cert**

En el VM (fuera del docker o dentro) usar:

**sudo ss -tuln**

**Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.**

Los siguientes puertos indican que los servicios con soporte de cifrado (SSL/TLS) están escuchando correctamente:

* HTTPS (Web): Puerto 443 (vía Nginx/Apache).
* IMAPS (Correo): Puerto 993 (Dovecot).
* POP3S (Correo): Puerto 995 (Dovecot).
* SMTPS/Submission (Correo): Puertos 465 y 587 (Postfix).

Conclusión: Los servicios cifrados están activos porque aparecen en estado LISTEN.

Los certificados que se están usando están (dentro del contenedor Docker) en los directorios **/etc/ssl/certs/** y **/etc/ssl/private/**.

Para Nginx (Web): **grep -R "ssl\_certificate" /etc/nginx/**

Para Postfix (SMTP): **postconf -n | grep smtpd\_tls\_**

Para Dovecot (POP3/IMAP): **grep -r "ssl\_cert" /etc/dovecot/**

d. Añade algunas cuentas de usuario mediante el panel de administración de iRedMail (usuario postmaster@tudominio, web: <https://ip/iredadmin>)

### **Añadir cuentas de usuario.**

Entramos en <https://10.2.7.25/iredadmin> con la cuenta del postmaster.

Vamos a:

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Contraseñas deben ser 8 caracteres mínimo, mayúscula y carácter especial.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

## 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.*

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

**cat /var/log/mail.log | grep Takumi**

Dec 8 11:19:08 mail amavis[754]: (00754-11) Passed UNCHECKED {RelayedTaggedInternal}, ORIGINATING/MYNETS LOCAL [127.0.0.1]:57158 ESMTP/ESMTP <itsuki@initiald.com> -> <takumi@initiald.com>, (), Queue-ID: 4dPzyD6svnz4wCr, Message-ID: <4433b8b71d7ac1a31ae8e9ca2b2d7f87@initiald.com>, mail\_id: BmaPn\_gP0iuE, b: dIqQKJ3AU, Hits: -, size: 539, queued\_as: 4dPzyN25bwz4wCx, Subject: "Probando", From: <itsuki@initiald.com>, User-Agent: Roundcube\_Webmail, helo=localhost, 7278 ms

Dec 8 11:19:08 mail amavis[754]: (00754-11) Passed UNCHECKED, <itsuki@initiald.com> -> <takumi@initiald.com>, Hits: -, tag=2, tag2=6.2, kill=6.9, queued\_as: 4dPzyN25bwz4wCx, L/Y/Y/Y

Dec 8 11:19:08 mail postfix/amavis/smtp[2740]: 4dPzyD6svnz4wCr: to=<takumi@initiald.com>, relay=127.0.0.1[127.0.0.1]:10026, delay=7.4, delays=0.12/0.02/0.01/7.3, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4dPzyN25bwz4wCx)

Dec 8 11:19:08 mail postfix/pipe[2767]: 4dPzyN25bwz4wCx: to=<takumi@initiald.com>, relay=dovecot, delay=0.13, delays=0.02/0.02/0/0.08, dsn=2.0.0, status=sent (delivered via dovecot service)

**Este comando y su resultado muestran el rastro completo de un correo electrónico enviado dentro de tu servidor. El comando cat /var/log/mail.log | grep Takumi básicamente lee el historial de correos y filtra solo las líneas donde aparece el destinatario "Takumi".**

**Aquí tienes la explicación de lo que sucedió en esos milisegundos del 8 de diciembre:**

**Resumen del flujo**

**El usuario Itsuki envió un correo a Takumi usando el webmail (Roundcube). El servidor lo recibió, lo escaneó en busca de virus/spam (Amavis) y finalmente lo entregó en la bandeja de entrada (Dovecot).**

**Análisis paso a paso**

**1. El escaneo de seguridad (Amavis)**

amavis[754]: ... Passed UNCHECKED ... <itsuki@initiald.com> -> <takumi@initiald.com>

* **¿Qué pasó?**: El sistema de seguridad **Amavis** recibió el correo.
* **Estado**: Dice UNCHECKED porque probablemente el correo es interno (desde el mismo servidor) y el sistema confía en él sin pasarle el antivirus completo.
* **Detalles**: El correo pesa 539 bytes y el asunto es "Probando". Se envió usando **Roundcube Webmail**.

***2. La puntuación de Spam***

*amavis[754]: ... tag=2, tag2=6.2, kill=6.9 ...*

* ***¿Qué pasó?****: Amavis le asignó etiquetas de control.*
* ***Significado****: Indica que si el correo llegara a* ***6.2*** *puntos de sospecha, se marcaría como SPAM, y si llegara a* ***6.9*** *(kill), el servidor lo borraría directamente. En este caso, el correo pasó sin problemas.*

***3. El paso por Postfix (MTA)***

*postfix/amavis/smtp[2740]: 4dPzyD6svnz4wCr: to=<takumi@initiald.com>, relay=127.0.0.1... status=sent*

* ***¿Qué pasó?****: Postfix (el cartero del servidor) terminó de hablar con Amavis.*
* ***Resultado****: El mensaje se reenvía internamente de la cola de escaneo a la cola de entrega final. El estado status=sent aquí significa que Amavis lo devolvió con éxito a Postfix.*

***4. Entrega final a la bandeja de entrada***

*postfix/pipe[2767]: 4dPzyN25bwz4wCx: to=<takumi@initiald.com>, relay=dovecot... status=sent (delivered via dovecot service)*

* ***¿Qué pasó?****: Esta es la línea más importante. Postfix le entregó el correo a* ***Dovecot****.*
* ***Resultado****: El correo ha sido guardado físicamente en la carpeta del usuario Takumi. El proceso terminó correctamente (delivered).*

*b. Correo desde un usuario local a un usuario de otro servidor de clase. Aporta los logs del envío.*

**cat /var/log/mail.log | grep** [**neo@policia.es**](mailto:neo@policia.es)

Dec 8 11:12:59 mail amavis[754]: (00754-09) Passed UNCHECKED {RelayedTaggedInternal}, ORIGINATING/MYNETS LOCAL [127.0.0.1]:57518 ESMTP/ESMTP <itsuki@initiald.com> -> <neo@policia.es>, (), Queue-ID: 4dPzq75ht6z4wCL, Message-ID: <4a113654809908c70965a3bdb7cd8c0a@initiald.com>, mail\_id: ccaZOxDC8ymN, b: Jz8Y-NPCl, Hits: -, size: 536, queued\_as: 4dPzqH1MTyz4wCr, Subject: "Saludos", From: <itsuki@initiald.com>, User-Agent: Roundcube\_Webmail, helo=localhost, 7328 ms

Dec 8 11:12:59 mail amavis[754]: (00754-09) Passed UNCHECKED, <itsuki@initiald.com> -> <neo@policia.es>, Hits: -, tag=2, tag2=6.2, kill=6.9, queued\_as: 4dPzqH1MTyz4wCr, L/Y/Y/Y

Dec 8 11:12:59 mail postfix/amavis/smtp[2601]: 4dPzq75ht6z4wCL: to=<neo@policia.es>, relay=127.0.0.1[127.0.0.1]:10026, delay=7.5, delays=0.15/0.03/0.01/7.3, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4dPzqH1MTyz4wCr)

Dec 8 11:13:05 mail postfix/smtp[2621]: 4dPzqH1MTyz4wCr: to=<neo@policia.es>, relay=mail.policia.es[10.2.3.25]:25, delay=6.6, delays=0.03/0.04/6.4/0.19, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 4dPzqP5QYrz3wsl)

*Aquí la situación es distinta a la anterior. Mientras que el correo para "Takumi" era* ***interno*** *(se quedaba en tu propio servidor), este correo para neo@policia.es es un* ***envío externo****.*

*La gran diferencia está en la última línea: el servidor ha logrado sacar el correo hacia internet.*

***Análisis del envío***

* ***El Emisor****: itsuki@initiald.com (desde tu webmail Roundcube).*
* ***El Destinatario****: neo@policia.es (un dominio externo).*
* ***El Asunto****: "Saludos".*

***Lo que nos dicen las líneas clave***

***1. El procesamiento interno (Amavis)***

*Al igual que en el caso anterior, el correo pasa por el filtro de seguridad local (Passed UNCHECKED). Tu servidor verifica que el correo de Itsuki no sea malicioso antes de intentar enviarlo fuera. Tardó unos* ***7.3 segundos*** *en procesarlo.*

***2. La salida al mundo exterior (Postfix SMTP)***

*postfix/smtp[2621]: ... relay=mail.policia.es[10.2.3.25]:25 ... status=sent*

*Aquí es donde ocurre la magia del envío:*

* ***relay=mail.policia.es****: Tu servidor contactó con el servidor de correo de la policía.*
* ***[10.2.3.25]:25****: Se conectó a esa dirección IP a través del puerto 25 (el puerto estándar para transferencia de correo entre servidores).*
* ***status=sent****: ¡Éxito! El servidor remoto* ***aceptó*** *el correo.*
* ***(250 2.0.0 Ok: queued as ...)****: Esta es la respuesta del servidor de la policía. Te están confirmando: "Recibido, lo hemos puesto en nuestra cola para entregárselo a Neo".*

*c. Correo desde un usuario local a un destinatario exterior. Aporta los logs del envío.*

Para mandar a usuarios del exterior, usa como destinatario un correo temporal (Gmail te dará problemas). <https://temp-mail.org/es/>

Interfaz de usuario gráfica, Sitio web

El contenido generado por IA puede ser incorrecto.

**root@mail:/opt/iredapd/tools# cat /var/log/mail.log | grep jogef59813@crsay.com**

Dec 11 13:39:15 mail amavis[749]: (00749-17) Passed UNCHECKED {RelayedInternal}, ORIGINATING/MYNETS LOCAL [127.0.0.1]:36818 ESMTP/ESMTP <postmaster@initiald.com> -> <jogef59813@crsay.com>, (), Queue-ID: 4dRtwW5XX3z4wG6, Message-ID: <9a58368ba9ebe151f280d484157bce75@initiald.com>, mail\_id: 3lqAP6rKPiL7, b: IhrNgwPtx, Hits: 0.1, size: 566, queued\_as: 4dRtwg1Gvdz4wG7, Subject: "probando de nuevo", From: <postmaster@initiald.com>, User-Agent: Roundcube\_Webmail, helo=localhost, Tests: [ALL\_TRUSTED=0.1], autolearn=ham autolearn\_force=no, autolearnscore=0, dkim\_new=dkim:initiald.com, 7345 ms

Dec 11 13:39:15 mail amavis[749]: (00749-17) Passed UNCHECKED, <postmaster@initiald.com> -> <jogef59813@crsay.com>, Hits: 0.1, tag=2, tag2=6.2, kill=6.9, queued\_as: 4dRtwg1Gvdz4wG7, L/0/0/0

Dec 11 13:39:15 mail postfix/amavis/smtp[29578]: 4dRtwW5XX3z4wG6: to=<jogef59813@crsay.com>, relay=127.0.0.1[127.0.0.1]:10026, delay=7.6, delays=0.23/0.02/0/7.4, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4dRtwg1Gvdz4wG7)

Dec 11 13:39:15 mail postfix/smtp[29619]: 4dRtwg1Gvdz4wG7: to=<jogef59813@crsay.com>, relay=mail.crsay.com[157.230.201.21]:25, delay=0.82, delays=0.02/0.03/0.48/0.3, dsn=2.0.0, status=sent (250 Message Queued (42949412-ADDD-45D5-BD5D-D38251F768B5.1))

*Este es otro caso de un* ***envío externo exitoso****, muy similar al de la policía, pero con un detalle técnico importante: aquí se ha aplicado* ***DKIM*** *(una firma digital de seguridad).*

*Aquí tienes el análisis de lo que sucedió el* ***11 de diciembre****:*

***Resumen del Envío***

* ***Emisor:*** *postmaster@initiald.com (Cuenta de administrador).*
* ***Destinatario:*** *jogef59813@crsay.com (Un dominio externo).*
* ***Asunto:*** *"probando de nuevo".*
* ***Resultado:*** *Entregado correctamente al servidor de destino.*

***Detalles técnicos destacados***

***1. Firma DKIM (dkim\_new=dkim:initiald.com)***

*A diferencia de los logs anteriores, aquí vemos que Amavis aplicó una firma* ***DKIM****.*

* ***¿Para qué sirve?*** *Es un sello digital que le dice al servidor de destino (crsay.com) que el correo realmente viene de tu servidor y no ha sido alterado. Esto ayuda mucho a que tus correos* ***no lleguen a la carpeta de Spam****.*

***2. Calificación de Spam (Hits: 0.1)***

*El sistema analizó el correo y le dio una puntuación de* ***0.1****. Es una puntuación bajísima (muy buena), lo que indica que es un correo limpio. El test ALL\_TRUSTED indica que, como viene de tu propia red local, el sistema confía plenamente en él.*

***3. Conexión y Entrega rápida***

*relay=mail.crsay.com[157.230.201.21]:25 status=sent (250 Message Queued (...))*

* *Tu servidor encontró al servidor de crsay.com en la IP 157.230.201.21.*
* *La conexión fue muy rápida: la parte de red (0.48/0.3) sumó menos de un segundo.*
* *El servidor de destino aceptó el correo y le asignó su propio código de seguimiento: 42949412-ADDD....*

*d. Aporta la prueba de recepción de correo de otro compañero de clase.*

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

*e. Envía los correos necesarios para las pruebas del apartado anterior.*

*- Aporta los logs que muestran el envío y la entrega del correo:*

Eso se comprueba en **/var/log/mail.log**. Creo que en ambos equipos (remitente y destinatario).

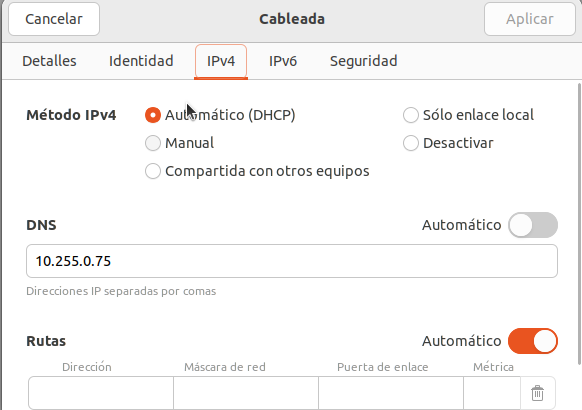
El resto son pantallazos.

Ten cuidado, los logs se borran con cada reinicio del servidor iredmail.

# MUA + EMAIL Server.

Configura el cliente de correo **Thunderbird** para usar una cuenta de correo en tu servidor iRedMail de manera cifrada y:

Para que el Thunderbird pueda ver el servidor de correo “smtp.initiald.com”, debes poner en la configuración gráfica de Ubuntu el DNS “**10.255.0.75**”.



a. Envía un correo desde la cuenta de un usuario de tu dominio a una cuenta de correo externa.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

* 1. [Crea un par de claves PGP](https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq#w_i-have-never-used-openpgp-with-thunderbird-before-how-do-i-setup-openpgp) 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.

### **PGP**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Envío desde el remitente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Desde el destinatario.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

### **Exportar tu clave PGP.**

“Administrador de claves OpenPGP”.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Selecciona la clave y dale a exportar en archivo.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Generará un archivo en formato “.asc”

¿Recuerdas que no puedes mandar correo a Gmail porque no lo acepta? Puedes enviárselo por correo a un correo temporal o puedes abrir el archivo con un editor de texto y pasar el contenido a otro archivo en tu PC.

### **Importar PGP.**

**ATENCIÓN**: para poder mandar correo cifrado a otros usuarios, debemos tener su certificado PGP público.

En nuestro caso, para el examen, debemos de habernos descargado el archivo desde aquí: <https://drive.google.com/drive/folders/1uXTGrYxv9o0BHUBrNWsJGgEgL46TqOBl>

Luego se la mandamos con el correo (podemos mandárnosla a nosotros mismos) y luego:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

* 1. Configura tu cliente de correo para tener en cuenta los correos marcados como SPAM por SpamAssasin y que se muevan a la carpeta de Correo No Deseado.

### Configurar ThunderBird con SpamAssasin.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.



Método 2:

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

* 1. Envía los correos necesarios para las pruebas del ejercicio anterior.

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

Instalamos Chrome en la VM cliente donde hemos configurado antes ThunderBird. Seguimos estos pasos:

<https://www.manusoft.es/linux/instalar-google-chrome-en-ubuntu-desde-terminal/>

* Primero descargamos el paquete con el Google Chrome más reciente:

**wget -c** [**https://dl.google.com/linux/direct/google-chrome-stable\_current\_amd64.deb**](https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb)

* Cuando el proceso termine, actualizamos con el comando:

**sudo apt-get update**

* Y una vez termine de actualizar instalamos la librería de indicadores de sistema para poder ver el icono de Google Chrome en nuestro lanzador (y algunos más):

**sudo apt-get install libappindicator1**

* Y para terminar, instalamos Google Chrome:

**sudo dpkg -i google-chrome-stable\_current\_amd64.deb**

Ahora instalamos el complemento ***mailvelope.***

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Diagrama

El contenido generado por IA puede ser incorrecto.

* 1. Crea la clave privada y pública PGP.

Le damos a “Generar llave”.

Interfaz de usuario gráfica, Texto, Aplicación, Teams

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Está marcada la casilla de subir la clave al servidor de Claves de Mailvelope.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

El contenido generado por IA puede ser incorrecto.

Creamos una copia de seguridad.

Se guarda automáticamente en Descargas. Podemos gestionarlas desde aquí.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

* 1. Publica tu clave en el servidor de claves de mailvelope.

Si no hemos sincronizado con el servidor de claves de mailvelope. Solo tenemos que seleccionar la cuenta y nos vamos a:

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.



* 1. Envía un mensaje a UN COMPAÑERO indicando ejercicio realizado, cifrándolo y firmándolo.
  2. Desencripta la respuesta del COMPAÑERO, comprobando que es legítima.

# Nombre de los Dominios de cada uno

ANEXO DOMINIOS

[ELIGE TU DOMINIO AQUÍ](https://docs.google.com/spreadsheets/d/1kdV4H3iiVlbsCmT9_E5xgodgn_ZEZ19w9DNv9V0VQ_A/edit?gid=0#gid=0)

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | **Nº** | **Alumno/a** | **DOMINIO** |
|  | 1 | Cepeda Ramírez  José Javier | [***powerking.com***](http://powerking.com/) |
|  | 2 | Espina García  Pablo | [***spear.com***](http://spear.com/) |
|  | 3 | González Pichardo  Andrés | [***policia.es***](http://policia.es/) |
|  | 4 | Luque Espinosa  Armando | [***roller.com***](http://roller.com) |
|  | 5 | Reig Camacho  Mario | [***cabramocha.com***](http://cabramocha.com/) |
|  | 6 | Rubio Vigueras  Gonzalo | [***vengance.com***](http://vengance.com/) |
|  | 7 | Suárez Abad  Cristóbal | [***initiald.com***](http://asir.com/) |
|  | 8 | Villegas Basilio  Sergio | [***svb.io***](http://svb.io/) |

Rango IPs estáticas para los servidores de correo:

10.2.X.25; X = NumeroDeLista

/24 = 255.255.255.0

# PONER EL PROMPT DE TU NOMBRE Y ETC

export PS1="\e[01,31m Cristobal \e[01;35m \D{%A %e %B %G %R} \e[00;31m \n\[\033[01;32m\][\u@\h\[\033[01;37m\] \W\[\033[01;32m\]]\$\[\033[00m\]"

# Comandos para comprobar log de correos

**grep "yokahe" /var/log/mail.log | sed 's/, /\n /g'**

**cat /var/log/mail.log | sed 's/, /\n /g'**

1. <https://docs.iredmail.org/manage.iredapd.html> [↑](#footnote-ref-1)