

Seguridad DNS: SPF, DKIM y DMARC paso a paso

Si has montado un servidor de correo y los mensajes acaban en spam, no es mala suerte: te faltan los tres registros de autenticación. SPF dice quién puede enviar por ti, DKIM firma cada mensaje y DMARC le cuenta al mundo qué hacer si algo falla.

PILA	TIEMPO	PASOS	PROBADO EN
SPF · DKIM · DMARC	~25 min	5	Ubuntu 24.04 LTS

SI PREFIERES QUE LO HAGA YO
50 €

Vas a necesitar acceso al panel DNS de tu dominio (IONOS, Cloudflare, OVH...) y, para DKIM, acceso al servidor de correo (Postfix con OpenDKIM).

Antes de copiar

En los comandos verás `tudominio.com`: sustitúyelo siempre por tu dominio real.

PASO 01 Registro SPF: quién puede enviar correo

Es un registro TXT en el dominio raíz que indica los servidores autorizados. `~all` = sospechoso pero se acepta; `-all` = rechazo.

spf.txt

```
@ IN TXT "v=spf1 mx a:mail.tudominio.com -all"
```



Un solo SPF

Solo puede existir un registro SPF por dominio. Si ya tienes uno (de Google Workspace, Mailchimp...), fusi6nalo en lugar de crear otro.

PASO 02 DKIM: firmar cada correo saliente

Instala OpenDKIM y genera el par de claves. La p6blica se publica como TXT bajo un selector (aquí `mail._domainkey`).

opendkim.sh

```
sudo apt install -y opendkim opendkim-tools
sudo mkdir -p /etc/opendkim/keys/tudominio.com
cd /etc/opendkim/keys/tudominio.com
sudo opendkim-genkey -s mail -d tudominio.com
sudo chown opendkim:opendkim mail.private
sudo cat mail.txt # este es el registro DNS que tienes que publicar
```

PASO 03 Registro DKIM en el DNS

Copia el contenido de `mail.txt` en el panel DNS como un TXT con nombre `mail._domainkey`.

dkim.txt

```
mail._domainkey IN TXT "v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA..."
```

PASO 04 DMARC: pol6tica e informes

Dice qu6 hacer cuando SPF o DKIM fallan, y te env6a informes. Empieza siempre con `p=none` para observar antes de bloquear.

dmARC.txt

```
_dmarc IN TXT "v=DMARC1; p=none; rua=mailto:dmARC@tudominio.com; adkim=s; aspf=s"
```

PASO 05 Validar con herramientas externas

Comprueba los tres registros con **dig** y haz una prueba real en mail-tester.com: el objetivo es 10/10.

```
comprobar.sh
```

```
dig +short TXT tudominio.com  
dig +short TXT mail._domainkey.tudominio.com  
dig +short TXT _dmarc.tudominio.com
```



Endurecer la política

Cuando lleves 2-4 semanas de informes DMARC sin sorpresas, pasa de **p=none** a **p=quarantine** y después a **p=reject**. Nunca saltes directamente a reject.

¿Prefieres que lo haga por ti?

Lo implemento por ti por **50 €**, con la configuración de seguridad inicial y esta guía aplicada a tu servidor.