

SPF, DKIM y DMARC en los dominios de tus clientes (revendedores)

Esta guía es para **revendedores** de DirectAdmin: cómo dejar bien configurada la autenticación del correo (**SPF**, **DKIM** y **DMARC**) de los dominios de tus clientes, y qué tienes que revisar cada vez que das de alta uno nuevo.

Los pasos técnicos de cada registro están en la guía de usuario, que es la que puedes pasar a tus clientes: [SPF, DKIM y DMARC para tu dominio en DirectAdmin](#). Aquí está lo que cambia por ser revendedor.

Antes de nada: ¿quién gestiona el DNS del dominio?

Es la pregunta que decide todo lo demás, y conviene hacerla al dar de alta el dominio, no cuando el cliente se queja de que sus correos van a spam:

- **DNS en nuestros servidores** (los servidores de nombres que te indicamos al contratar): todo se hace desde el panel y se publica solo.
- **DNS externo** (Cloudflare, el registrador del cliente, otro proveedor): el panel genera los valores, pero los registros hay que crearlos en ese proveedor. Compruébalo con `dig NS dominio.es` o con <https://mxtoolbox.com/DNSLookup.aspx>.

1 — Que tus clientes puedan gestionar su DNS: «Control DNS»

Para que un usuario vea **Administración DNS** en su panel, su cuenta tiene que tener activado **Control DNS**. Se define en el paquete que asignas (**Administrar Paquetes de Usuario**) o al modificar el usuario.

- **Con Control DNS activo:** el cliente puede seguir la guía de usuario por su cuenta.

- **Sin Control DNS:** el cliente no ve la opción, pero tú sí puedes editar su zona. El propio panel lo avisa: «*El control de DNS está desactivado para este usuario. Puede editar la zona porque su cuenta principal tiene Control DNS activado.*»

Decide qué modelo quieres para cada cliente. Si tus clientes no son técnicos, lo habitual es dejar el control DNS desactivado y hacer tú estos pasos.

2 — Actuar sobre la cuenta de un cliente

1. En tu panel de revendedor, entra en **Listado de Usuarios** y abre el usuario.
2. En las acciones del usuario, pulsa **Impersonate** (el panel en español muestra esta opción sin traducir). Entrás en su panel con su nivel de usuario, sin necesitar su contraseña.
3. Desde ahí, sigue la guía de usuario: **Activar DKIM** en **Cuentas de Correo Electrónico**, crear el buzón de informes y añadir el registro `_dmarc` en **Administración DNS**.
4. Para volver a tu cuenta, pulsa **Cambiar a tu-usuario** en la barra superior.

Tus propios dominios (los de tu cuenta de revendedor) se configuran igual, desde tu nivel de usuario.

3 — DKIM: no se activa solo

En nuestros servidores DKIM **no se genera automáticamente** al crear un dominio: hay que pulsar **Activar DKIM** por cada dominio. Es intencionado: así no se firma correo con una clave que todavía no está publicada.

Con **DNS externo**, el orden importa. En cuanto se activa DKIM, el correo sale firmado; si el registro `x._domainkey` no está publicado en el DNS real, los receptores ven una firma imposible de comprobar, y eso es **peor que no tener DKIM**. Copia primero el registro desde **Administración DNS** al proveedor externo, comprueba que se publica y deja DKIM activado solo cuando lo esté.

4 — DMARC: una política por cliente, y siempre empezando por `none`

Para cada dominio:

```
_dmarc    TXT    "v=DMARC1; p=none; rua=mailto:dmarc@dominio-del-cliente"
```

- El buzón de `rua` **tiene que existir**: créalo en la cuenta del cliente o apunta a uno que ya se revise. Si no existe, los informes rebotan contra tu propio servidor.
- Empieza siempre con `p=none`. Pasar a `quarantine` o `reject` sin haber revisado los informes es la causa más frecuente de correo legítimo perdido: casi todos los clientes tienen algún remitente que no conocen de antemano (la herramienta de newsletters, la tienda online, el programa de facturación).
- Si gestionas muchos clientes, centralizar los informes en un único buzón tuyo es cómodo, pero ten en cuenta que un buzón de **otro dominio** necesita que ese dominio publique la autorización correspondiente (un registro `TXT` en `dominio-del-cliente._report._dmarc.tu-dominio`). Lo más sencillo es un buzón por dominio.

5 — SPF: uno solo por dominio

El panel crea el SPF del dominio al darlo de alta. Revisa que haya **un único** registro `v=spf1` y que incluya los servicios externos que use el cliente para enviar correo (`include:` del proveedor correspondiente). Dos registros SPF en el mismo dominio invalidan ambos.

Lista de comprobación al dar de alta un dominio de cliente

- **DNS**: sabes dónde está (nuestro o externo).
- **Control DNS**: decidido para ese usuario (lo gestiona él o lo gestionas tú).
- **SPF**: un único `v=spf1`, con los servicios externos del cliente incluidos.
- **DKIM**: activado, y su registro `x._domainkey` publicado en el DNS real **antes** de que el cliente empiece a enviar.
- **Buzón de informes**: existe.
- **DMARC**: `_dmarc` con `p=none`; revisión de informes programada antes de endurecer.
- **Verificación**: correo de prueba a Gmail → **Mostrar original** → SPF, DKIM y DMARC en `PASS`.

Revision #1

Created 2026-10-07 09:35:44 UTC by Abkrim

Updated 2026-10-07 09:35:44 UTC by Abkrim