SPF, DKIM y DMARC para tu dominio en DirectAdmin

Esta guía explica cómo dejar bien configurada la autenticación del correo de un dominio desde tu panel de DirectAdmin: **SPF**, **DKIM** y **DMARC**. Son tres registros DNS que permiten a los servidores de destino (Gmail, Outlook, IONOS…) comprobar que el correo que envías con tu dominio sale realmente de ti. Sin ellos, tus correos tienen muchas más papeletas para acabar en la carpeta de spam o ser rechazados.

Hazlo cada vez que añadas un dominio nuevo a tu cuenta. Son cinco minutos.

Antes de empezar: ¿dónde está el DNS de tu dominio?

Todo lo que sigue se hace en el panel **solo si el DNS del dominio está en nuestros servidores** . Compruébalo con cualquier herramienta de consulta DNS (por ejemplo `dig NS ejemplo.es` o una web como https://mxtoolbox.com/DNSLookup.aspx):

- **Si los servidores de nombres son los nuestros** (los que te indicamos al dar de alta el hosting): sigue esta guía tal cual.
- **Si el DNS está en otro sitio** (Cloudflare, el panel de tu registrador…): los registros hay que crearlos allí, copiando los valores que te da el panel. Lee el aviso del paso 1 antes de activar DKIM.

> **Dominios con eñe o tildes:** el panel los muestra en su forma técnica, que empieza por `xn--`. Por ejemplo, `carpintería-ejemplo.es` aparece como `xn--carpintera-ejemplo-pyb.es`. Es el mismo dominio; selecciónalo así en el panel.

Paso 1 — Activar DKIM

DKIM añade una firma digital a cada correo que envías. En nuestros servidores no se activa sola: la activas tú por dominio.

1. En el panel, entra en **Cuentas de Correo Electrónico**.
2. Arriba, en el selector de dominio, elige el dominio.
3. Pulsa el botón **Activar DKIM**, en la parte superior de la página.

El panel genera la clave y publica automáticamente su registro DNS (un registro `TXT` con nombre `x._domainkey`). Puedes comprobarlo en **Administración DNS**.

> **Aviso si el DNS está fuera:** desde el momento en que pulsas **Activar DKIM**, tus correos salen firmados. Si el registro `x._domainkey` no está publicado en el DNS real del dominio, los destinatarios ven una firma que no pueden comprobar, y eso es **peor que no tener DKIM**. Con DNS externo, copia primero el registro `x._domainkey` (desde **Administración DNS** del panel) a tu proveedor de DNS y activa DKIM después, o hazlo todo seguido y comprueba la publicación en el momento.

Paso 2 — Crear el buzón que recibirá los informes DMARC

DMARC hace que los grandes proveedores te envíen informes periódicos con el resultado de los correos que ven salir con tu dominio. Necesitas un buzón que exista para recibirlos; si no existe, esos informes rebotan.

1. En **Cuentas de Correo Electrónico**, pulsa **Crear cuenta**.
2. Crea `dmarc@tudominio` (o usa un buzón que ya revises, por ejemplo `postmaster@tudominio`).

Los informes llegan como ficheros adjuntos comprimidos (XML). No hace falta leerlos a diario; son útiles para comprobar, antes de endurecer la política, que todo tu correo legítimo pasa las comprobaciones.

Paso 3 — Crear el registro DMARC

1. Entra en **Administración DNS** y elige el dominio.
2. Pulsa **Añadir Registro**.
3. En **Tipo de registro** elige `TXT`.
4. En **Nombre** escribe `_dmarc` (solo eso; el panel completa el resto del nombre).

5. En el selector del tipo de valor (**Sencillo / DMARC / SPF**) elige **DMARC**. El panel muestra un pequeño formulario:
   - **Tipo de política de dominio:** `Ninguno` para empezar.
   - **Tipo de política de subdominio:** `El mismo que el dominio`.
   - **Correo electrónico agregado (RUA):** el buzón del paso 2, por ejemplo `dmarc@tudominio`.
   - El resto de campos, con su valor por defecto.
6. Pulsa **Guardar**.

El registro resultante debe quedar así:

```
_dmarc   TXT   "v=DMARC1; p=none; rua=mailto:dmarc@tudominio"
```

Si prefieres no usar el formulario, elige **Sencillo** y pega ese valor tal cual, cambiando `tudominio` por el tuyo.

¿Por qué empezar con la política `none`?

La política dice a los receptores qué hacer con un correo que falla la comprobación:

Política	Qué hace el receptor	Cuándo usarla
`none`	Nada: entrega el correo y te envía el informe	Al empezar, siempre
`quarantine`	Lo manda a la carpeta de spam	Cuando los informes muestran que todo tu correo legítimo pasa
`reject`	Lo rechaza	Solo cuando estás seguro de que no hay remitentes legítimos sin autenticar

Empezar directamente con `quarantine` o `reject` es la forma más habitual de que desaparezca correo legítimo: por ejemplo, el que envía en tu nombre una herramienta de newsletters, una tienda online o un programa de facturación que no está incluido en tu SPF. Deja `none` al menos dos o cuatro semanas, revisa los informes y endurece solo cuando todo salga en verde.

Paso 4 — Comprobar el SPF

El panel crea un registro SPF al dar de alta el dominio. Compruébalo en **Administración DNS**: debe existir un registro `TXT` en el propio dominio que empiece por `v=spf1`, por ejemplo:

```
v=spf1 a mx ip4:203.0.113.10 ~all
```

Solo debe haber **un** registro SPF por dominio. Si envías correo con tu dominio desde algún servicio externo (Brevo, Mailchimp, Google Workspace, Microsoft 365, un programa de facturación…), ese servicio te indicará qué añadir a ese mismo registro, normalmente un `include:`. No crees un segundo registro `v=spf1`: dos registros SPF invalidan ambos.

Paso 5 — Verificar

Los cambios en nuestros servidores DNS se aplican en pocos minutos. Para comprobar que todo está publicado:

- **DMARC:** https://mxtoolbox.com/dmarc.aspx con tu dominio.
- **DKIM:** https://mxtoolbox.com/dkim.aspx con tu dominio y el selector `x`.
- **SPF:** https://mxtoolbox.com/spf.aspx con tu dominio.

La prueba definitiva es enviar un correo a una cuenta de Gmail, abrirlo, ir a **Mostrar original** y comprobar que **SPF**, **DKIM** y **DMARC** aparecen como `PASS`.

Resumen rápido para cada dominio nuevo

- **SPF:** existe un único registro `v=spf1` e incluye todos los servicios que envían correo con tu dominio.
- **DKIM:** activado desde **Cuentas de Correo Electrónico** → **Activar DKIM**, y publicado en el DNS real del dominio.
- **Buzón de informes:** existe `dmarc@tudominio` (o el que hayas elegido).
- **DMARC:** registro `_dmarc` con `p=none` al principio; se endurece más adelante con los informes delante.

Si tu dominio pertenece a un revendedor que gestiona tu cuenta, o no ves la opción **Administración DNS** en tu panel, pídele a tu proveedor que te active el control DNS o que haga estos pasos por ti.

Revision #1
Created 2026-10-07 07:35:44 UTC by Abkrim
Updated 2026-10-07 07:35:44 UTC by Abkrim