redcricket

Quién puede escribir a nombre de tu empresa

SPF, DKIM y DMARC explicados sin jerga, con el orden correcto para activarlos y los errores que se cometen siempre.

Sirve con cualquier proveedor de correo. No requiere cuenta ni registro.

Los tres registros, en una página

Son tres entradas de texto en el DNS de tu dominio. Juntas le dicen al resto del mundo quién tiene permiso de enviar correo con tu nombre y qué hacer cuando alguien no lo tiene.

SPF La **lista de quién puede enviar** en tu nombre: tu proveedor de correo, tu herramienta de facturación, la de marketing. Vive en un registro TXT del dominio raíz.

DKIM La **firma** que prueba que el mensaje salió de ahí y que nadie lo alteró en el camino. La llave pública vive en selector._domainkey.tudominio.

DMARC La **regla**: qué debe hacer quien recibe cuando un correo no pasa SPF ni DKIM —nada, cuarentena o rechazo— y **a dónde mandarte el reporte**. Vive en _dmarc.tudominio.

Cómo se ven

SPF

```
v=spf1 include:_spf.tuproveedor.com include:otroservicio.com ~all
```

DMARC

```
v=DMARC1; p=none; rua=mailto:reportes@tudominio.com; pct=100
```

> **Lo único que hay que entender del SPF:** ~all significa «lo demás es sospechoso», -all significa «lo demás recházalo». Empezar por ~all evita tirar correo legítimo mientras terminas de inventariar quién envía por ti.

El orden correcto para activarlos

Casi todos los problemas vienen de hacer esto al revés: publicar DMARC en rechazo antes de saber quién envía en tu nombre. El orden importa más que la velocidad.

01 **Inventaría quién envía por ti.** Correo del equipo, facturación, el sistema de tickets, la herramienta de marketing, el ERP. Es el paso que nadie hace y el que causa los problemas de los otros cuatro.

02 **Publica SPF con ~all**, incluyendo a todos los del paso 1. **Un solo registro SPF por dominio** — dos registros es un error de configuración, no una suma.

03 **Activa DKIM en cada servicio** que envíe por ti. Cada uno publica su propio selector; no compiten entre sí.

04 **Publica DMARC en p=none con rua.** No bloquea nada todavía: solo te manda reportes. Es el paso que convierte esto en información en vez de suposición.

05 **Lee los reportes unas semanas** y corrige lo que aparezca enviando por ti sin estar en la lista.

06 **Sube a p=quarantine y después a p=reject**, cuando los reportes estén limpios. Aquí es donde el dominio queda realmente protegido — y solo aquí es seguro llegar.

> **El paso 4 es el que casi siempre se salta**, y es el único que da visibilidad. Un DMARC sin rua es una regla sin nadie que la lea.

Cinco errores que se cometen siempre

- **Dos registros SPF en el mismo dominio.** No se suman: la validación falla. Si hay que agregar un servicio, se agrega un include: al registro que ya existe.
- **Pasarse del límite de diez consultas DNS del SPF.** Cada include: cuenta, y algunos incluyen otros por dentro. Al pasarse, el SPF deja de evaluarse — sin aviso.
- **Publicar p=reject el primer día.** Es la forma más rápida de que dejen de llegar tus propias facturas.
- **Olvidar a los que envían por ti.** La herramienta de marketing, el sistema de tickets y el ERP mandan correo con tu dominio. Si no están en SPF y sin DKIM, DMARC los rechaza.
- **Usar +all.** Significa «cualquiera puede enviar en mi nombre». Anula el propósito del registro.

Y uno que no es error, pero cuesta caro

Los tres registros se configuran una vez —casi siempre al migrar el correo— y **nadie los vuelve a mirar**. Un cambio de proveedor, un DNS que alguien tocó o una herramienta nueva debilitan la configuración sin que nadie se entere. **Esto no es un proyecto: es un estado que se vigila.**

Hoja de registro por dominio

Una fila por cada dominio desde el que sale correo — incluidos los que ya no se usan pero siguen existiendo, que son los que suelen estar abiertos.

Dominio	SPF	DKIM	DMARC	Responsable	Próxima revisión

En la columna de DMARC anota la política (none, quarantine o reject), no un sí o un no. La diferencia entre none y reject es la diferencia entre saber y estar protegido.

Dónde encaja Red Cricket

Los seis pasos se pueden hacer a mano, y esta guía alcanza para hacerlos. Lo que no se sostiene a mano es el **estado**: nadie vuelve a mirar tres registros de DNS hasta que algo deja de funcionar.

Autenticación de Correo es uno de los ocho módulos de Red Cricket Cloud. Vigila los tres registros de forma continua, avisa cuando un cambio debilita la configuración, y deja DMARC configurado con una guía paso a paso.

Se prueba treinta días, sin tarjeta: cloud.redcricket.net/es/register

Esta guía es material de referencia y no constituye asesoría técnica ni una evaluación de tu configuración. Verifica cada cambio de DNS antes de aplicarlo en producción.