Secuenza

Guía de entregabilidad: SPF, DKIM y DMARC

Que tus correos lleguen a la bandeja de entrada depende de dos cosas: que los proveedores puedan comprobar que eres tú y que tu buzón tenga buena fama. Esta guía explica los tres registros que lo demuestran, cómo se ponen en los proveedores más habituales y qué hábitos cuidan la reputación.

Por qué importa

Gmail, Yahoo y Outlook.com piden a quien envía con frecuencia que su dominio tenga **SPF, DKIM y DMARC**, que cada correo se pueda dar de baja con un clic y que casi nadie lo marque como spam. Sin esos registros, lo normal es que tus correos acaben en spam o ni siquiera lleguen.

Secuenza envía desde tu propio buzón, así que es tu proveedor de correo quien firma (o no) cada correo. Lo que tienes que hacer es publicar en el DNS de tu dominio los datos que lo confirman.

Antes de empezar: dónde está tu DNS

El DNS de tu dominio se gestiona donde lo compraste o donde lo apuntaste (el registrador, tu hosting, Cloudflare…), que no siempre es donde tienes el correo. Entra en ese panel y busca la zona DNS: ahí se añaden los registros de esta guía.

Un cambio de DNS tarda en verse de unos minutos a unas horas. Después, vuelve a **Comprobaciones** en Secuenza.

SPF: quién puede enviar por tu dominio

El SPF es un registro **TXT** en la raíz del dominio que empieza por `v=spf1`, dice qué servidores pueden enviar en su nombre y termina en `~all` (los demás, sospechosos) o `-all` (los demás, rechazados).

Proveedor	Lo que tiene que incluir tu SPF
Microsoft 365	`include:spf.protection.outlook.com`
Google Workspace	`include:_spf.google.com`
IONOS	`include:_spf-eu.ionos.com`
OVHcloud	`include:mx.ovh.com`
Hostinger	`include:_spf.mail.hostinger.com`
Aruba	`include:_spf.aruba.it`
Zoho Mail (UE)	`include:zoho.eu`

Por ejemplo, con Microsoft 365: `v=spf1 include:spf.protection.outlook.com ~all`.

Tres reglas que conviene saber:

- **Solo puede haber un SPF.** Si ya tienes uno (de tu web, de tu programa de facturas), no añadas otro: junta los `include` en el mismo registro. Con dos, los dos dejan de valer.
- **Como mucho, 10 consultas.** Cada `include` cuenta, y también los que tiene dentro. Si te pasas, los servidores lo dan por roto.
- **Nunca** `+all`: dejaría enviar a cualquiera en tu nombre.

Si tu buzón es una dirección de Gmail o de Outlook.com (no de tu dominio), no tienes que poner nada: el SPF y la firma son los del proveedor. Eso sí, esos buzones tienen cupos bajos y Secuenza los respeta.

DKIM: la firma de tus correos

Con DKIM, tu proveedor firma cada correo con una clave privada y tú publicas la clave pública en el DNS, en un nombre como `selector._domainkey.tudominio.es`. Así el que recibe sabe que el correo no se ha tocado por el camino y que sale de verdad de tu dominio.

- **Microsoft 365:** en el portal de Microsoft Defender, en la configuración de autenticación del correo (DKIM), elige tu dominio. Te da dos registros **CNAME** (`selector1` y `selector2`): ponlos en tu DNS y vuelve al portal para activar la firma.
- **Google Workspace:** en la consola de administración, en Gmail → Autenticar correo electrónico, genera un registro de **2048 bits**, ponlo como **TXT** en `google._domainkey` y pulsa «Iniciar autenticación».

- **IONOS, OVHcloud, Hostinger, Aruba, Zoho y la mayoría de hostings:** busca «DKIM» en el panel del correo. Muchos la activan solos si el DNS también está con ellos; si no, te dan el registro que hay que copiar.

Secuenza busca la firma con los nombres habituales de cada proveedor. Si la tienes con otro nombre, la **prueba real de envío** (del Pro) la encuentra. Usa claves de **2048 bits**: las de 1024 ya se consideran débiles.

DMARC: qué hacer con lo que no pasa

DMARC es un registro **TXT** en `_dmarc.tudominio.es` que dice a los proveedores qué hacer con un correo que dice ser de tu dominio pero no pasa SPF ni DKIM, y adónde mandarte los informes. Para que cuente, el dominio del remitente tiene que coincidir con el del SPF o el de la firma DKIM (la «alineación»).

Empieza observando:

```
v=DMARC1; p=none; rua=mailto:dmarc@tudominio.es
```

1. **Dos a cuatro semanas en `p=none`**: no cambia nada, pero recibes informes de quién envía por tu dominio. Revisa que todo lo legítimo sale firmado (tu buzón, tu web, tus facturas).
2. **Sube a `p=quarantine`**: lo que no pase irá a spam.
3. **Y después a `p=reject`**: lo que no pase se rechaza. Es lo que más protege tu dominio de quien quiera hacerse pasar por ti.

Los informes llegan en XML. Hay servicios gratuitos que los resumen; basta con mirarlos de vez en cuando.

Comprobarlo con Secuenza

En la ficha de cada buzón, **Comprobaciones** revisa SPF, DKIM y DMARC, y también la recepción de correo (MX), el nombre inverso del servidor, MTA-STS, BIMI y el cifrado. Cada comprobación sale en verde, ámbar o rojo, con lo que hay que poner y dónde. Si ya tienes un SPF, te propone el registro completo con lo que le falta.

Con el **Pro**, además:

- **Prueba real de envío:** Secuenza manda un correo de verdad desde tu buzón y te dice lo que ve el servidor que lo recibe: firma, SPF, alineación DMARC, cifrado y repaso antispam.
- **Listas negras:** comprueba si tu servidor o tu dominio aparecen en las listas que usan los filtros.

Y la sección **Seguridad** junta lo que ha parado el freno, tus cifras de 30 días frente a sus límites y el estado de cada buzón: lo explica Seguridad del envío.

La reputación: lo que miran los filtros

Con los registros bien puestos, lo que decide es cómo te comportas:

- **Empieza poco a poco.** Un buzón o un dominio nuevos que de repente envían cientos de correos parecen spam. El calentamiento de Secuenza sube el cupo día a día.
- **Respeta los cupos.** Secuenza usa para cada proveedor un cupo diario y por hora prudente, por debajo de su límite, y reparte los envíos por tu horario.
- **Que darse de baja sea fácil.** Cada correo lleva el enlace de baja y la cabecera para que Gmail y Outlook enseñen su botón de «Cancelar suscripción». Las bajas se aplican enseguida.
- **Listas limpias.** Nunca compres listas. Los correos devueltos y los inactivos se apartan, y el freno de seguridad para una campaña si hay demasiadas devoluciones o bajas, y el envío a un proveedor donde nadie abre tus correos.
- **Pocas quejas.** Si más de 2 o 3 de cada mil personas marcan tus correos como spam, los filtros te castigan. Escribe solo a quien espera tus correos.
- **Correos de persona.** Texto claro, pocos enlaces, nada de acortadores, imágenes con texto alrededor. Sube las imágenes desde el editor: las de Drive o Dropbox, o las pegadas dentro del correo, suelen acabar en spam. El repaso antispam te avisa de lo que suele pesar.
- **Que te respondan.** Una respuesta es la mejor señal de que tu correo es bienvenido. Escribe para que la gente conteste.

Si tus correos van a spam

1. Abre **Comprobaciones**: ¿están los tres registros en verde?
2. Con el Pro, haz la **prueba real de envío** y mira qué falla en el servidor que recibe.
3. Revisa el **repaso antispam** de los correos de la campaña.
4. Mira en **Seguridad** si el freno ha parado algún proveedor, y en **Resultados**, las bajas y las devoluciones: si suben, para y limpia la lista.
5. Baja el cupo unos días y vuelve a subirlo poco a poco.