

PROTOCOLO TÉCNICO OFICIAL · ESTÁNDARES 2026

Manual de Entregabilidad

Blindaje Anti-Spam: SPF, DKIM & DMARC

Protocolo de blindaje para Systeme.io, Cloudflare y pasarelas de email.

AUTOR & CERTIFICACIÓN

Antonio Salguero

Economista & Desarrollador Web

www.embudostech.com

1. Los 3 Requisitos Críticos de Google y Yahoo (2026)

- **Tasa de Quejas de Spam Inferior al 0.10 %:** Si tu ratio supera el **0.30 %**, tus correos se bloquean de raíz a nivel de servidor receptor.
- **Alineación Obligatoria de Dominio Propio:** Prohibido enviar correos comerciales usando cuentas gratuitas (@gmail.com, @yahoo.es). Es indispensable un dominio corporativo (@tunegocio.com) autenticado.
- **Baja Inmediata en 1 Clic (List-Unsubscribe):** Cabecera técnica obligatoria en todo envío comercial masivo.

2. Autenticación DNS: SPF y DKIM

Introduce estos registros en tu panel de DNS (*Cloudflare, Namecheap, Hostinger, GoDaddy o Dinahosting*):

2.1 1. Firma SPF (Sender Policy Framework)

Autoriza a los servidores de Systeme.io a emitir correo con tu dominio. Solo debe existir **un único registro SPF** en tu dominio raíz.

Registro SPF (Tipo TXT en Dominio Raíz)

Tipo: TXT | **Host:** @ (o tu dominio raíz) | **TTL:** Automático / 3600

Valor Exacto: v=spf1 include:_spf.systeme.io ~all

Si usas Google Workspace o Microsoft 365, combínalo en una sola línea:

v=spf1 include:_spf.google.com include:_spf.systeme.io ~all

2.2 2. Firmas Criptográficas DKIM

Garantiza que el email no ha sido alterado ni falsificado. En Systeme.io (*Configuración → Correos → Dominios*), se generan automáticamente **3 registros CNAME**:

Registros DKIM (3x Tipo CNAME generados por Systeme.io)

Registro	Nombre / Host	Valor / Destino Canónico
CNAME 1:	systemeio1._domainkey	systemeio1._domainkey.systeme.io
CNAME 2:	systemeio2._domainkey	systemeio2._domainkey.systeme.io
CNAME 3:	systemeio3._domainkey	systemeio3._domainkey.systeme.io

⚠ ¡El Fallo Crítico en Cloudflare (Error Común #1)!

Si usas Cloudflare, los 3 registros CNAME de DKIM deben tener la nube en modo «**Solo DNS**» (**Nube Gris**). Si dejas la **Nube Naranja (Proxy)**, Cloudflare ocultará las claves públicas, provocando un fallo permanente de autenticación en Systeme.io que impedirá el envío de campañas.

3. Política de Seguridad DMARC

Indica a los servidores de destino (Gmail, Outlook, Yahoo) qué hacer si un correo entrante no supera las comprobaciones de SPF o DKIM:

Registro DMARC Recomendado para Nuevos Dominios (Tipo TXT)

Tipo: TXT | **Host:** _dmarc | **TTL:** Automático

Valor / Contenido:

```
v=DMARC1; p=none; rua=mailto:dmarc@tudominio.com; pct=100; adkim=r; aspf=r
```

- **p=none : Modo de auditoría inicial.** Monitoriza el tráfico legítimo sin bloquear entregas mientras se estabilizan los registros.
- **rua=mailto:... :** Buzón donde recibirás reportes automáticos de intentos de suplantación.
- **Evolución Segura (Tras 30 días):** Cambiar gradualmente a **p=quarantine** (desviar correos sospechosos a spam) y posteriormente a **p=reject** (máximo blindaje mundial).

4. Cómo Vencer al Algoritmo y Evitar la Pestaña Promociones

Gmail examina el contenido y el comportamiento del usuario para clasificar el correo entre la pestaña *Principal* y la de *Promociones*:

Factor	Causa de Caída en Promociones	Estrategia para Bandeja Principal
Ratio Texto/Imagen	Correos tipo catálogo con banners enormes y escaso texto.	Regla 60/40: Prioridad al texto redactado en párrafos breves. Máximo 1 imagen ligera.
Enlaces	Enlaces a través de acortadores externos (<i>bit.ly</i> , <i>tinyurl</i>).	Enlaces directos a tu propio dominio verificado o anclas de texto descriptivas.
Palabras Filtro	Mayúsculas repetitivas, signos (\$!;) y términos como "URGENTE" o "GRATIS".	Redacción conversacional natural, como si escribieras a un colega de trabajo.
Interacción	Envíos unidireccionales que no invitan a la respuesta del lector.	Fomentar respuestas: Pedir que el lector responda en el primer correo.

El «Truco de Oro» de la Interacción Temprana

En el primer correo que reciban tus nuevos suscriptores, incluye esta posdata final:

«P.D.: Respóndeme a este correo con un .ºK"para saber que te ha llegado bien el material».

Cuando el usuario te responde, Gmail añade automáticamente tu dirección a su libreta de contactos seguros y todos tus correos futuros entrarán directamente en la **Bandeja Principal**.

5. 5º Protocolo de Calentamiento de Dominio (Warm-Up)

Si tu dominio es reciente o llevas meses sin enviar, nunca envíes a toda tu lista de golpe. Sigue este escalado progresivo de 4 semanas:

Semana	Límite Diario	Segmento de Audiencia Prioritario
Semana 1	50 emails / día	Suscriptores dados de alta en los últimos 7 días.
Semana 2	150 emails / día	Usuarios que hayan abierto algún correo en los últimos 30 días.
Semana 3	500 emails / día	Base general de contactos, excluyendo bajas y rebotes.
Semana 4+	Volumen regular	Envíos masivos con supervisión de reputación en Postmaster Tools.

6. Checklist de Auditoría Pre-Vuelo

Verifica cada punto en tu cuenta antes de activar automatizaciones o campañas masivas:

- ☐ **Firma SPF Única:** Registro SPF validado sin superar el límite estricto de 10 consultas DNS (*DNS lookups limit*).
- ☐ **Firmas DKIM Validadas:** Los 3 registros CNAME de DKIM activos con estado verde dentro del panel de Systeme.io.
- ☐ **Cloudflare en Modo Solo DNS:** Nube Gris verificada para todas las firmas de correo (evita la Nube Naranja de proxy).
- ☐ **Política DMARC Operativa:** Registro TXT creado en el host `_dmarc` con política de monitorización `p=none`.
- ☐ **Calificación Mail-Tester:** Puntuación superior a **9.5 sobre 10** en test de mensaje enviado desde la plataforma.
- ☐ **Enlace de Baja Operativo:** Enlace de cancelación (*Unsubscribe*) visible, legible y en 1 clic al pie de cada correo.
- ☐ **Google Postmaster Tools:** Dominio verificado para monitorizar en tiempo real la tasa de quejas y la reputación de IP.

7. Herramientas Gratuitas de Diagnóstico Recomendadas

Herramienta	Acceso	Objetivo Técnico
Mail-Tester	<code>mail-tester.com</code>	Analiza la puntuación antispam del email y listas negras.
MXToolbox	<code>mxtoolbox.com</code>	Verifica la propagación y sintaxis de SPF, DKIM y DMARC.
Google Postmaster	<code>postmaster.google.com</code>	Monitoriza la reputación de tu dominio y el porcentaje de quejas.