

ALTA DE DOMINIO DE EMPRESA

Registros DNS para enviar con SendyPOP

Qué registros hay que publicar en el DNS de tu dominio para que SendyPOP envíe en nombre de tu empresa, cómo hacerlo sin afectar a otro proveedor de email que ya uses y cómo comprobar que quedó bien.

PARA QUIÉN	QUÉ SE TOCA	TIEMPO
El área de sistemas o quien administre el DNS del dominio.	Se agregan 2 registros nuevos, se edita 1 y se revisa 1. No se borra nada.	15 minutos de trabajo; la propagación suele tardar de minutos a unas horas.

1 Resumen de registros

En los ejemplos, `tuempresa.com` representa tu dominio. Los valores exactos para tu dominio aparecen en SendyPOP, en **Dominios**, al agregar el dominio. Copialos desde ahí, en especial la clave DKIM.

FUNCIÓN	TIPO	HOST / NOMBRE	VALOR	SI YA EXISTE
SPF (obligatorio)	TXT	@	v=spf1 include:_spf.sendypop. com ~all	Editar: sumar include:_spf.sendypop. com al SPF actual
DKIM (obligatorio)	TXT	spop202606. _domainkey	v=DKIM1; k=rsa; p=... (clave completa del panel)	Agregar: no choca con otros DKIM
DMARC (obligatorio)	TXT	_dmarc	v=DMARC1; p=none; rua=mailto:dmarc@tuemp resa.com	Conservar el DMARC existente
Tracking (obligatorio)	CNAME	track	sendypop.com	Agregar: host exclusivo

2 Antes de empezar

1. **Avisá a tu proveedor de SendyPOP qué dominio vas a usar.** Tené en cuenta que la antigüedad del dominio influye en los resultados de tus campañas: cuanto más tiempo tiene un dominio, más confiable es para los sistemas de email.

2. **Tu proveedor da de alta el dominio en SendyPOP y genera la clave DKIM propia de ese dominio.** Te envía los valores exactos a publicar (SPF, DKIM, DMARC y tracking), que también vas a ver en **Dominios**. No uses claves de ejemplo ni de otro dominio.
3. Guardá una copia de la zona DNS actual (captura o exportación). Sirve para volver atrás si hiciera falta.
4. Anotá qué otros servicios envían correo con tu dominio: Google Workspace, Microsoft 365, otra plataforma de email marketing, el sistema de facturación, etc. Ninguno se da de baja.

3 Detalle de cada registro

TXT SPF: autoriza los servidores de SendyPOP

CAMPO	VALOR
Host	@ (el dominio raíz, <code>tuempresa.com</code>)
Valor si no tenés SPF	<code>v=spf1 include:_spf.sendypop.com ~all</code>
TTL	3600, o el valor por defecto del panel

SI YA USÁS OTRO PROVEEDOR

Un dominio puede tener **un solo** registro SPF. No crees un segundo TXT que empiece con `v=spf1` : con dos registros, SPF falla para todos los proveedores. Editá el existente y agregá `include:_spf.sendypop.com` antes del final (`~all` o `-all`), sin quitar nada y sin cambiar ese final.

Antes

```
v=spf1 include:_spf.google.com include:_spf.embluemail.com -all
```

Después

```
v=spf1 include:_spf.google.com include:_spf.embluemail.com include:_spf.sendypop.com -all
```

SPF admite como máximo **10 consultas DNS** en total (cada `include` cuenta, junto con lo que incluye por dentro). `_spf.sendypop.com` suma exactamente una, porque lista directamente las IPs. Si tu SPF ya está cerca del límite, avisanos antes de publicar. En SendyPOP, la tarjeta del SPF muestra el valor publicado y, si falta SendyPOP, te propone el registro combinado listo para copiar.

TXT DKIM: firma de los mensajes

CAMPO	VALOR
Host	<code>spop202606._domainkey</code>
Nombre completo	<code>spop202606._domainkey.tuempresa.com</code>
Valor	<code>v=DKIM1; k=rsa; p=MIIBIjANBgkq...IDAQAB</code> Copiá la clave completa desde SentryPOP. No la tipees a mano.

La clave la genera SentryPOP para tu dominio al darlo de alta. Si no la recibiste, pedila a tu proveedor de SentryPOP o copiala desde **Dominios**.

SI YA USÁS OTRO PROVEEDOR

Cada proveedor usa su propio selector (la parte antes de `._domainkey`), así que el de SentryPOP convive con los demás. No modifiques ni borres otros registros `...._domainkey` (por ejemplo `google._domainkey`, `selector1._domainkey` de Microsoft 365 u otros de tu plataforma actual).

La clave es larga. Algunos paneles la dividen en fragmentos de 255 caracteres entre comillas: es normal y no afecta la validación. Lo que no debe pasar es que se agreguen espacios dentro de la clave o que se corte.

TXT DMARC: política del dominio

CAMPO	VALOR
Host	<code>_dmarc</code>
Valor si no tenés DMARC	<code>v=DMARC1; p=none; rua=mailto:dmarc@tuempresa.com</code>

SI YA TENÉS DMARC

No lo reemplaces. SentryPOP sólo necesita que exista un DMARC válido y funciona con cualquier política (`none` , `quarantine` o `reject`), incluso en modo estricto (`adkim=s` ; `aspf=s`). SentryPOP firma con tu propio dominio y usa un remitente de ese mismo dominio, así que queda alineado.

Gmail, Yahoo y Microsoft exigen DMARC a quienes envían volumen. Si no tenés, empezá con `p=none` y una casilla real en `rua` para recibir los reportes; más adelante podés endurecer la política.

CNAME Tracking: enlaces y aperturas con tu dominio

CAMPO	VALOR
Host	<code>track</code> (nombre completo <code>track.tuempresa.com</code>)
Destino	<code>sendypop.com</code> (algunos paneles lo piden con punto final: <code>sendypop.com.</code>)

Los enlaces de tus campañas se miden a través de `https://track.tuempresa.com` en lugar de un dominio ajeno, lo que mejora la confianza de los filtros. SendyPOP emite el certificado HTTPS de este host de forma automática.

IMPORTANTE

El host `track` debe tener **sólo** el CNAME: sin registros A, AAAA ni TXT en ese mismo nombre.

En **Cloudflare**, dejá el registro en **Solo DNS** (nube gris), no en modo proxy.

Si tu proveedor agrega el dominio al final y queda `sendypop.com.tuempresa.com`, cargá el destino con punto final: `sendypop.com`.

Si `track` ya lo usa otro servicio, no lo pises: escribinos y lo resolvemos antes de publicar.

4 Convivencia con otro proveedor de email

Podés usar SendyPOP en paralelo con tu plataforma actual, sin darla de baja. Cada servicio firma con su propio selector DKIM y usa sus propios hosts, y todos comparten un único SPF. Ejemplo real de una zona que usa Google Workspace para el correo diario, eMBlue para campañas y suma SendyPOP:

REGISTRO	TIPO	PERTENECE A	ACCIÓN
<code>tuempresa.com (SPF)</code>	TXT	Todos	Editar: se suma <code>include:_spf.sendypop.com</code>
<code>tuempresa.com</code>	MX	Google Workspace	No tocar
<code>epexo._domainkey</code>	TXT	eMBlue	No tocar
<code>google._domainkey</code>	TXT	Google Workspace	No tocar
<code>bounce</code>	CNAME	eMBlue (rebotes)	No tocar
<code>_dmarc</code>	TXT	Dominio	No tocar
<code>spop202606._domainkey</code>	TXT	SendyPOP	Agregar
<code>track</code>	CNAME	SendyPOP	Agregar
Verificaciones de Google, Facebook, etc.	TXT	Otros servicios	No tocar

SendyPOP **no necesita cambiar los MX** ni ningún registro de recepción de correo: tu casilla sigue funcionando igual. Tampoco requiere un host propio de rebotes, así que no hace falta tocar los de tu otro proveedor.

5 Verificación

1. Esperá la propagación. Depende del TTL de tu zona: normalmente minutos, a veces unas horas. SentryPOP consulta directamente los servidores DNS de tu dominio, así que ve los cambios apenas se publican.
2. En SentryPOP, abrí el dominio y tocá **Verificar dominio**. El panel muestra cada registro como verificado, pendiente o con un valor distinto del esperado, y qué encontró publicado.
3. Abrió `https://track.tuempresa.com/api/health` en el navegador: debe responder sin error de certificado.
4. Creá o validá un remitente con tu dominio (por ejemplo `novedades@tuempresa.com`) y mandá una prueba a casillas propias de Gmail y Outlook. En "Mostrar original" deben figurar **SPF: PASS, DKIM: PASS y DMARC: PASS**.
5. Confirmá que tu otro proveedor sigue autenticando bien con un envío de prueba desde esa plataforma.

Para consultar los registros desde una computadora:

Windows (PowerShell)

```
Resolve-DnsName tuempresa.com -Type TXT
Resolve-DnsName spop202606._domainkey.tuempresa.com -Type TXT
Resolve-DnsName _dmarc.tuempresa.com -Type TXT
Resolve-DnsName track.tuempresa.com -Type CNAME
```

macOS / Linux

```
dig +short TXT tuempresa.com
dig +short TXT spop202606._domainkey.tuempresa.com
dig +short TXT _dmarc.tuempresa.com
dig +short CNAME track.tuempresa.com
```

NO ENVÍES CAMPAÑAS TODAVÍA SI...

SPF, DKIM, DMARC o el tracking figuran como pendientes. Hasta que el dominio esté verificado, SentryPOP no habilita envíos desde él. Si tu dominio tiene DMARC en `quarantine` o `reject`, un mensaje sin autenticar va directo a spam o se rechaza.

6 Errores frecuentes

SÍNTOMA	CAUSA HABITUAL	SOLUCIÓN
SPF falla para todos los proveedores	Se creó un segundo TXT <code>v=spf1</code>	Unificar todo en un solo registro
SPF con "permerror"	Más de 10 consultas DNS en el SPF	Quitar servicios que ya no se usan, o consultarnos
El panel no encuentra el DKIM	El host quedó como <code>spop202606._domainkey.tuempresa.com.tuempresa.com</code>	Cargar sólo <code>spop202606._domainkey</code> : el panel completa el dominio
DKIM con valor distinto	Clave cortada o con espacios agregados	Volver a copiarla completa desde SentryPOP
Tracking pendiente	El destino quedó como <code>sendypop.com.tuempresa.com</code>	Cargar el destino con punto final: <code>sendypop.com.</code>
Tracking sin certificado	Proxy de Cloudflare activo, o A/AAAA en <code>track</code>	Pasar a Solo DNS y dejar únicamente el CNAME
Dejó de funcionar el otro proveedor	Se reemplazó el SPF o el DMARC en vez de editarlo	Restaurar el valor anterior y sumar sólo el <code>include</code>

7 Cómo volver atrás

Si decidís dejar de usar SentryPOP, revertir no afecta a tus otros servicios:

- Quitá `include:_spf.sendypop.com` del SPF, dejando el resto igual.
- Borrá sólo `spop202606._domainkey` y el CNAME `track`.
- No modifiques MX, DMARC ni los registros de otros proveedores.