

DKIM y DMARC para c-tasc.org.pa

Oct 5, 2026 · @Justin

Qué se solicita

El dominio `c-tasc.org.pa` tiene SPF configurado, pero **no tiene DKIM ni DMARC**. Sin esos dos registros, un tercero puede enviar correos haciéndose pasar por el C-TASC AIP, y nuestros correos legítimos tienen más probabilidad de ser clasificados como spam.

Se solicitan tres cambios en el DNS:

1. **Agregar un registro TXT de DMARC** en `_dmarc` — el valor exacto está en la sección siguiente y se puede publicar de inmediato.
2. **Agregar dos registros CNAME de DKIM** — los valores exactos los genera el panel de Microsoft 365 y se detallan más abajo, porque no pueden redactarse a mano.
3. **Revisar el registro TXT comodín (`*`)** que existe hoy en la zona y que distorsiona cualquier diagnóstico de correo.

Ninguno de estos cambios interrumpe el correo actual. El registro DMARC que se propone arranca en modo observación (`p=none`), es decir, no bloquea nada: solo genera reportes.

Estado actual del DNS

Consultas hechas contra DNS público el 5 de octubre de 2026.

Elemento	Estado	Valor encontrado
MX	Correcto	<code>ctasc-org-pa0c.mail.protection.outlook.com</code> (Microsoft 365)
SPF	Correcto	<code>v=spf1 include:spf.protection.outlook.com -all</code>
DKIM	Ausente	<code>selector1._domainkey</code> y <code>selector2._domainkey</code> sin registro
DMARC	Ausente	No existe registro en <code>_dmarc</code>
TXT comodín <code>*</code>	Presente	Devuelve el SPF para cualquier subdominio inexistente

El dominio está alojado en un tenant de Microsoft 365 a nombre de *CENTRO DE TECNOLOGIA AVANZADA DE SEMICONDUCTORES-AIP*. Esto determina cómo se configura DKIM: en Microsoft 365 son registros CNAME, no TXT.

Sobre el comodín y el “falso DMARC”

Al consultar `_dmarc.c-tasc.org.pa` el DNS responde, pero lo que devuelve es el SPF, no un DMARC. La misma respuesta se obtiene al consultar cualquier nombre inventado dentro del dominio:

```
TXT _dmarc.c-tasc.org.pa          → v=spf1
include:spf.protection.outlook.com -all
TXT cualquiercosa-inexistente.c-tasc.org.pa → v=spf1
include:spf.protection.outlook.com -all
```

El segundo nombre no existe. Que ambos respondan lo mismo confirma que hay un registro TXT comodín (`*`) en la zona, y que **no hay un DMARC real**: un validador que busca `v=DMARC1` en `_dmarc` encuentra un SPF y concluye, correctamente, que el dominio no tiene política DMARC.

Registro 1: DMARC (publicar ahora)

Este registro es exacto y se puede agregar de inmediato.

Campo	Valor
Nombre / Host	<code>_dmarc</code>
Tipo	<code>TXT</code>
TTL	<code>3600</code>
Valor	<code>v=DMARC1; p=none; rua=mailto:dmarc@c-tasc.org.pa; fo=1; adkim=r; aspf=r; pct=100</code>

Si el panel de DNS pide el nombre completo en lugar del relativo, el host es `_dmarc.c-tasc.org.pa`.

Por qué `p=none` y no `p=reject`

`p=none` significa: *no bloques nada todavía, solo envía reportes*. Es la fase de observación, y es deliberada.

Una política `p=reject` publicada antes de tener el inventario completo de quién envía correo a nombre del dominio provoca que los correos legítimos empiecen a rechazarse sin aviso: no rebotan al remitente interno, simplemente no llegan al destinatario. El endurecimiento se hace después, por etapas, y está detallado más abajo.

Requisito previo del buón de reportes

La dirección `dmARC@c-tasc.org.pa` debe existir antes de publicar el registro, porque ahí llegan los reportes diarios de los proveedores de correo. Si no se desea crear un buzón nuevo, reemplazar esa dirección por `info@c-tasc.org.pa` en el valor del registro.

Registro 2: DKIM (se genera en Microsoft 365)

El valor de DKIM no puede redactarse a mano. DKIM es un par de claves criptográficas: la clave privada vive dentro de Microsoft 365 y firma cada correo saliente; la clave pública es la que se publica en el DNS. Un valor inventado no corresponde a ninguna clave privada, y el resultado es peor que no tener DKIM: todos los correos quedarían con una firma inválida, que es justamente la señal de un correo falsificado.

Por eso el primer paso lo hace el administrador de Microsoft 365, no el administrador del DNS. El panel genera las claves y muestra en pantalla los dos valores exactos que hay que publicar.

Paso 1 — Generar las claves (administrador de Microsoft 365)

1. Entrar a **security.microsoft.com**.
2. Ir a *Email & collaboration* → *Policies & rules* → *Threat policies* → *Email authentication settings*.
3. Abrir la pestaña **DKIM** y seleccionar el dominio `c-tasc.org.pa`.
4. Pulsar **Create DKIM keys**. El panel muestra dos valores CNAME: copiarlos completos.

Paso 2 — Publicar los dos CNAME (administrador del DNS)

Se agregan dos registros de tipo CNAME con los valores que entregó el panel. Tendrán esta forma:

Nombre / Host	Tipo	Apunta a
selector1._domainkey	CNAME	selector1-ctasc-org-pa0c._domainkey.<tenant>.onmicrosoft.com
selector2._domainkey	CNAME	selector2-ctasc-org-pa0c._domainkey.<tenant>.onmicrosoft.com

La porción `ctasc-org-pa0c` proviene del registro MX actual del dominio y ya está verificada. `<tenant>` es el dominio inicial de la organización en Microsoft (termina en `.onmicrosoft.com`) y aparece en el propio panel.

Importante: la tabla anterior sirve para reconocer el formato, no para copiarla. Deben publicarse los valores exactos que muestre el panel de Microsoft.

Paso 3 — Activar la firma (administrador de Microsoft 365)

Una vez publicados los CNAME, volver a la misma pantalla de DKIM y poner el interruptor del dominio en **Enabled**. Si Microsoft responde que no encuentra los registros, esperar a que el DNS propague (hasta el TTL configurado) y reintentar.

Registro 3: revisar el TXT comodín

La zona tiene un registro TXT comodín (`*`) que devuelve el SPF del dominio para cualquier nombre que no exista. Lo más probable es que se haya originado al cargar el SPF con `*` o con el campo de host vacío, en lugar de `@`.

No impide que los registros nuevos funcionen: cuando existe un registro real en un nombre exacto — `_dmarc`, `selector1._domainkey` — ese registro tiene prioridad sobre el comodín. Pero conviene corregirlo por dos razones:

- **Distorsiona los diagnósticos.** Cualquier herramienta que pregunte “¿existe DMARC?” recibe una respuesta afirmativa con contenido equivocado, lo que dificulta verificar si un cambio quedó bien aplicado.
- **Publica un SPF para servidores que no existen**, lo cual no aporta protección y sí genera confusión en auditorías posteriores.

Recomendación: verificar en el panel de DNS si el registro SPF quedó cargado con host `*` y, de ser así, dejarlo únicamente en `@` (el dominio raíz). Este punto es independiente de DKIM y DMARC y puede atenderse después, sin bloquear los otros dos.

Orden de aplicación

El orden importa: endurecer DMARC antes de tener DKIM activo y el inventario de remitentes completo provoca la pérdida de correo legítimo.

Fase	Cuándo	Acción	Valor de DMARC
1	Ahora	Publicar DMARC en observación y activar DKIM	<code>v=DMARC1; p=none; rua=mailto:dmarc@c-tasc.org.pa; fo=1; adkim=r; aspf=r; pct=100</code>
2	2 a 4 semanas después	Revisar reportes e inventariar remitentes	sin cambios
3	Reportes sin remitentes legítimos fallando	Cuarentena parcial	<code>v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@c-tasc.org.pa</code>
4	1 a 2 semanas después, sin incidentes	Cuarentena total	<code>v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@c-tasc.org.pa</code>
5	1 a 2 semanas después, sin incidentes	Rechazo	<code>v=DMARC1; p=reject; rua=mailto:dmarc@c-tasc.org.pa</code>

Cada fase consiste en reemplazar el valor del mismo registro TXT en `_dmarc`. No se agregan registros nuevos.

La fase 2 es la que no conviene saltarse: los reportes DMARC indican qué servidores están enviando correo a nombre del dominio. Es habitual descubrir ahí sistemas legítimos que nadie tenía presentes — facturación, formularios web, boletines, plataformas de terceros — que deben autorizarse en SPF o DKIM antes de pasar a `p=reject`.

Pendiente fuera del DNS: el correo que envía el sitio web

El sitio `c-tasc.org.pa` envía correos por su cuenta: el formulario de contacto y el de presentación de propuestas de licitaciones. Esos envíos no salen de un buzón de Microsoft 365, sino del servidor de correo configurado en Odoo.

El SPF actual termina en `-all`, que significa *rechazar todo lo que no provenga de Microsoft 365*. Si Odoo envía con remitente `@c-tasc.org.pa` a través de otro servidor, esos correos **ya hoy están fallando la verificación SPF**, y al llegar a la fase 5 (`p=reject`) pasarían a rechazarse de forma definitiva.

Verificación, en el backend de Odoo: **Ajustes → Técnico → Correo → Servidores de correo saliente**.

- Si el servidor saliente es el SMTP de Microsoft 365 autenticado con un buzón real del dominio, no hay nada que corregir.
- Si Odoo envía por un servidor propio o de terceros, hay dos caminos: configurarlo para que relaye autenticado por Microsoft 365 (recomendado), o autorizar expresamente ese servidor en el registro SPF.

Este punto corresponde al área web, no al administrador del DNS, pero debe resolverse antes de llegar a la fase 5.

Verificación posterior

Después de publicar los registros y esperar la propagación (hasta el TTL, normalmente menos de una hora):

- ☐ `_dmarc.c-tasc.org.pa` devuelve un valor que empieza con `v=DMARC1` — si devuelve `v=spf1`, el registro no quedó creado y se está viendo el comodín
- ☐ `selector1._domainkey.c-tasc.org.pa` y `selector2._domainkey.c-tasc.org.pa` resuelven hacia `*.onmicrosoft.com`
- ☐ En el panel de Microsoft, el dominio figura con DKIM en estado **Enabled**
- ☐ Un correo de prueba enviado a una cuenta externa (Gmail, por ejemplo) muestra `dkim=pass`, `spf=pass` y `dmarc=pass` al abrir el original del mensaje
- ☐ A los pocos días empiezan a llegar los reportes DMARC al buzón configurado en `rua`

Para consultar los registros desde cualquier equipo, sin herramientas adicionales:

```
nslookup -type=TXT _dmarc.c-tasc.org.pa
nslookup -type=CNAME selector1._domainkey.c-tasc.org.pa
```

La última verificación — la del correo de prueba — es la que realmente confirma el resultado: comprueba la cadena completa, desde la firma que aplica Microsoft hasta la validación que hace el servidor que recibe.