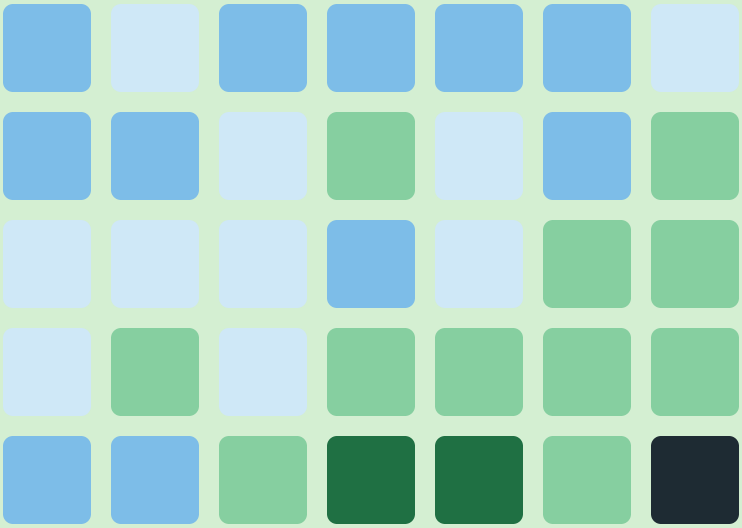
ATTESTA
CONSULTORA

GUÍA 03 · SEGURIDAD DE LA INFORMACIÓN

Correo que no se puede suplantar: SPF, DKIM y DMARC

Cómo impedir que terceros envíen correos a nombre de su dominio, con la configuración paso a paso en Microsoft 365 y en Google Workspace.



EN RESUMEN

- Sin autenticación, cualquiera puede enviar un correo que aparenta venir de su dominio. Es la base del fraude con facturas falsas y de la suplantación de ejecutivos.
- SPF, DKIM y DMARC son tres registros públicos en el DNS de su dominio. Juntos permiten al receptor verificar que un correo es legítimo y le indican qué hacer si no lo es.
- Desde 2024 y 2025, Google, Yahoo y Microsoft exigen estos registros a quienes envían grandes volúmenes. La meta para cualquier organización es llegar a una política DMARC de rechazo.

01

Cómo se suplanta un dominio

El protocolo de correo electrónico permite declarar cualquier remitente. Un tercero puede enviar un mensaje que muestre `finanzas@su-dominio.cl` en el campo De sin tener acceso a sus sistemas. Si su dominio no publica registros de autenticación, el servidor que recibe el mensaje no tiene cómo distinguirlo de uno legítimo.

Los casos más frecuentes son el cambio de cuenta bancaria en una factura, la instrucción urgente de pago atribuida a un ejecutivo y los enlaces de acceso falsos dirigidos a clientes o proveedores. En todos, el daño no recae solo en quien recibe el correo: también afecta la reputación del dominio suplantado.

02

Los tres registros

REGISTRO	QUÉ HACE	DÓNDE SE PUBLICA
SPF	Declara qué servidores están autorizados a enviar correo en nombre del dominio.	Registro TXT en la raíz del dominio. Debe existir uno solo y no superar 10 consultas DNS.
DKIM	Agrega a cada mensaje una firma criptográfica que el receptor verifica con una clave pública.	Registro TXT o CNAME bajo un selector, por ejemplo `selector1._domainkey`.
DMARC	Indica al receptor qué hacer si SPF y DKIM fallan o no coinciden con el remitente visible, y a dónde enviar informes.	Registro TXT en `_dmarc.su-dominio.cl`.

SPF y DKIM, por separado, no bastan: un atacante puede pasar SPF con su propio dominio y mostrar el suyo en el campo De. DMARC exige que al menos uno de los dos coincida con el dominio visible al destinatario, lo que se conoce como alineación.

03

Revise su dominio

Los registros son públicos. Desde una terminal de Windows, macOS o Linux puede consultarlos así:

```
nslookup -type=txt su-dominio.cl
nslookup -type=txt _dmarc.su-dominio.cl
```

También puede usar herramientas públicas de diagnóstico de correo, como MXToolbox. Revise tres cosas:

- Que exista **un solo** registro que comience con `v=spf1` y que incluya a todos los servicios que envían correo por su organización.
- Que exista un registro `v=DMARC1` y cuál es su política: `p=none` solo observa, `p=quarantine` envía a no deseados y `p=reject` rechaza.
- Que los correos que usted envía lleguen con `dkim=pass` en sus encabezados. En Outlook y Gmail se ve en la opción de mostrar el original del mensaje.

04

Configuración en Microsoft 365

1. **SPF.** Publique un registro TXT en la raíz del dominio. Si Microsoft 365 es su único emisor:

   ```
   v=spf1 include:spf.protection.outlook.com -all
   ```

   Agregue un `include` por cada servicio adicional que envíe a nombre del dominio.

2. **DKIM.** En el portal de Microsoft Defender, entre a Correo electrónico y colaboración, Directivas y reglas, Directivas de amenazas, Configuración de autenticación de correo electrónico, pestaña DKIM. Seleccione su dominio: el portal muestra los dos registros CNAME que debe publicar, `selector1._domainkey` y `selector2._domainkey`.

3. **Copie los valores exactos del portal.** Desde mayo de 2025, Microsoft usa un formato nuevo de destino para los dominios que configuran DKIM por primera vez. No copie valores de ejemplos ni de otros dominios.

4. **Active la firma.** Cuando el portal detecte los registros, active la opción de firmar los mensajes con DKIM. El estado debe indicar que el dominio está firmando.

05

Configuración en Google Workspace

1. **SPF.** Publique un registro TXT en la raíz del dominio. Si Google Workspace es su único emisor:

   ```
   v=spf1 include:_spf.google.com ~all
   ```

   Agregue un `include` por cada servicio adicional.

2. **DKIM.** En la Consola del administrador, entre a Aplicaciones, Google Workspace, Gmail, Autenticar correo electrónico. Genere una clave de 2048 bits si su proveedor de DNS lo permite.

3. **Publique la clave.** Cree un registro TXT con el nombre que indica la consola, normalmente `google._domainkey`, y el valor que comienza con `v=DKIM1`.

4. **Inicie la autenticación.** Vuelva a la consola, presione Iniciar autenticación y envíe un correo de prueba para confirmar `dkim=pass` en los encabezados.

> **ANTES DE ENDURECER LA POLÍTICA**
>
> Facturación electrónica, sistemas de cobranza, plataformas de marketing, CRM y formularios del sitio web suelen enviar correo a nombre del dominio. Si no los incluye en SPF o no configura DKIM en ellos, sus correos empezarán a rechazarse cuando DMARC pase a `p=reject`.

06

El camino hasta el rechazo

1. **Observar.** Publique DMARC en modo de observación y pida los informes agregados a un buzón dedicado:

   ```
   v=DMARC1; p=none; rua=mailto:dmarc@su-dominio.cl
   ```

2. **Analizar.** Durante algunas semanas, revise los informes para identificar todos los servicios que envían a nombre del dominio y corrija los que fallan.

3. **Cuarentena.** Cuando el correo legítimo pase de forma consistente, cambie a `p=quarantine`. Puede aplicarlo de forma gradual con el parámetro `pct`.

4. **Rechazo.** Con la cuarentena estable, pase a `p=reject`. Desde ese momento, los receptores que aplican DMARC rechazan los correos que suplantan su dominio.

Cambie también el SPF a `-all` cuando tenga identificados todos los emisores, y mantenga la revisión de los informes: cada servicio nuevo que envíe correo debe pasar por esta lista.

07

Lo que ya exigen los grandes proveedores

Desde febrero de 2024, Google y Yahoo exigen SPF, DKIM y DMARC (como mínimo con `p=none`) a los remitentes que envían más de 5.000 mensajes diarios a sus usuarios. Microsoft anunció requisitos equivalentes para Outlook.com en 2025. Aunque su organización no alcance ese volumen, los mismos registros mejoran la entrega de sus correos y protegen su dominio.

08

Errores frecuentes

- **Dos registros SPF.** El estándar admite uno solo; con dos, la verificación falla.
- **Más de 10 consultas DNS en SPF.** Cada `include` suma consultas; al superar el límite, SPF falla para todos los correos.
- **Publicar DKIM y no activar la firma.** En Microsoft 365 y Google Workspace, publicar el registro no basta: hay que activar la firma en la consola.
- **Quedarse en `p=none`.** La observación es una etapa, no un destino: con `p=none` los correos que suplantan su dominio se siguen entregando.
- **No revisar los informes.** Sin revisar los informes DMARC no se sabe qué servicios fallan antes de endurecer la política.

SIGUIENTE PASO

¿Su dominio se puede suplantar hoy?

La evaluación de correo corporativo revisa SPF, DKIM y DMARC, la protección contra suplantación, los reenvíos y las reglas de sus buzones, en Microsoft 365 o en Google Workspace, y entrega las correcciones priorizadas. Solicite una reunión de diagnóstico de 30 minutos.

attesta.cl/contacto



SOBRE ATTESTA

Attesta es una consultora de gestión y protección de datos y de seguridad de la información. Nuestro equipo evalúa la configuración de seguridad de Microsoft 365 y de Google Workspace, y acompaña a las organizaciones hasta su sistema de gestión ISO/IEC 27001.

attesta.cl · contacto@attesta.cl · Av. Manquehue Sur 520, Of. 205, Las Condes

Aviso. Esta guía es informativa. Las rutas de menú de Microsoft 365 y Google Workspace corresponden a octubre de 2026 y pueden cambiar; ante cualquier diferencia, siga la documentación oficial de cada fabricante.

FUENTES

- Microsoft Learn. Configurar DKIM para firmar correo de su dominio de Microsoft 365. learn.microsoft.com.
- Google Workspace. Configurar DKIM. knowledge.workspace.google.com.
- RFC 7208 (SPF), RFC 6376 (DKIM) y RFC 7489 (DMARC).
- Requisitos para remitentes masivos de Google, Yahoo y Microsoft: síntesis de PowerDMARC, 2026.