



Verificación de Dominio Correo Electrónico en Salesforce

Luciano Straccia

CONSULTOR SALESFORCE SALES & SERVICES

straccialucianon@gmail.com

Tabla de contenido

Historial del documento	2
Introducción	3
Introducción.....	3
Motivación.....	3
Actores intervinientes	3
Configuración DKIM / CNAME	4
1. Introducción	4
2. Pasos.....	4
3. Identificar los dominios de envíos de emails individuales.....	4
4. Identificar los dominios de direcciones globales	5
5. Crear Clave DKIM en Salesforce	5
6. Buscar Clave DKIM en Salesforce	5
7. Buscar Clave DKIM en Salesforce	6
8. Verificar disponibilidad del dominio.....	6
Verificaciones de seguridad adicionales.....	7
1. Verificación de emails de la organización	7
2. Verificación de email de cada usuario	7
3. Verificación del dominio de la organización	7

Historial del documento

Versión	Fecha	Observaciones
1	07/05/2026	Versión inicial del documento

Introducción

Introducción

Salesforce ha ido incorporando requerimientos de seguridad para mejorar la seguridad en la plataforma en general y para el envío de correos electrónicos en particular.

A partir de ello se requiere asegurar la validez de dominios y cuentas de correos electrónicos.

Motivación

Motiva este documento la inclusión de nuevas normativas de seguridad por parte de Salesforce durante los primeros meses del año 2026.

Actores intervinientes

- Administrador de Salesforce
- Administrador de dominio web (o sea, el responsable del alojamiento donde está la web)
- Usuarios de correo electrónicos

Configuración DKIM / CNAME

1. Introducción

Para enviar correos electrónicos desde Salesforce a partir de abril de 2026 se debe poseer una clave DKIM y CNAME configurados.

¿Qué es DKIM?

Ver https://postmarkapp-com.translate.google/guides/dkim?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

¿Por qué es importante?

Por un tema de seguridad: busca que los mensajes no puedan ser alterados.

2. Pasos

- Identificar los dominios desde donde se realizan los envíos de emails individuales (ver punto 3)
- Identificar los dominios desde donde se realizan los envíos de emails con direcciones globales de la organización (ver punto 4)

Para cada uno de los dominios identificados en el punto anterior:

- Generar una clave DKIM en Salesforce (ver punto 5)
- Esperar unos minutos y buscar clave DKIM generada (ver punto 6)
- Pedir a quienes manejan el alojamiento web que publique los registros CNAME en el DNS del dominio.
- 48 horas después de la configuración del CNAME activar la clave DKIM en Salesforce (ver punto 7)
- Verificar disponibilidad del dominio (ver punto 8)

3. Identificar los dominios de envíos de emails individuales

- Ir a Configuración
- Buscar Usuarios → Usuarios
- Revisar todos los dominios de los usuarios activos (el dominio es lo que está después del arroba)

Para cada una de esos @ diferentes habrá que hacer las siguientes configuraciones.

4. Identificar los dominios de direcciones globales

- Ir a Configuración
- Buscar «Direcciones de toda la organización» (Organization-Wide Addresses)
- Buscar todas las direcciones que haya cargadas ahí (el dominio es lo que está después del arroba)

Para cada una de esos @ diferentes habrá que hacer las siguientes configuraciones.

5. Crear Clave DKIM en Salesforce

1. Ir a Configuración

2. Buscar "Clave DKIM"

3. Crear nueva Clave DKIM considerando:

- Tamaño de clave: 2048 bits (si cuando van a pegarlo al servidor de email en el paso 9b no les permite por cuestiones de tamaño, van a tener que generar otra clave pero de 1024 bits, pero ya actualmente se recomienda 2048 y es habitual que los servidores de email lo permitan)

- Selector: es un texto que aparecerá en el encabezado técnico cuando se envíe. sugiero uno que deje claro que es de la organización y que es desde salesforce, pero nunca debe tener información que no pueda hacerse pública (si nuestra OSC es Pepe y la generamos en Salesforce, entonces podría ser "pepesf")

- Selector alternativo: es otro selector. idem criterio con el anterior, que tenga alguna pequeña variante.

- Dominio: hay que poner el dominio de la organización (si los emails son @pepe.org entonces acá hay que escribir "pepe.org")

Patrón de coincidencia de dominio: son los dominios y subdominios desde donde se envía (recomiendo poner completo, o sea "pepe.org, *.pepe.org")

6. Buscar Clave DKIM en Salesforce

1. Ingresar a Configuración --> Clave DKIM

2. Acceder a la clave haciendo click en el nombre del selector (no en Modificar)

3. Van a encontrar dos nuevos textos largos que dicen:

- Registro CNAME
- Registro CNAME alternativo

Por el momento hasta acá llega la actividad del Administrador de Salesforce y debe pasar esos textos largos al administrador del alojamiento web para que realice la configuración.

7. Buscar Clave DKIM en Salesforce

1. Ingresar a Configuración --> Clave DKIM
2. Acceder a la clave haciendo click en el nombre del selector (no en Modificar)
3. Hacer click en el botón Activar. Si el botón Activar no está habilitado es porque el paso del alojamiento web no se completó correctamente.

8. Verificar disponibilidad del dominio

Una vez realizadas las acciones indicadas en los pasos anteriores realizar la verificación final.

Ver la sección siguiente "Verificaciones de seguridad adicionales", subsección "3. Verificación del dominio de la organización"

Verificaciones de seguridad adicionales

1. Verificación de emails de la organización

En esta verificación se busca que la organización tenga verificada la dirección de email general.

Resultado esperado: que todas las cuentas de email estén verificadas

Pasos:

- Ir a Configuración
- Buscar «Direcciones de toda la organización» (Organization-Wide Addresses)
- Verificar que todas las direcciones cargadas allí estén en estado Verificado

2. Verificación de email de cada usuario

En esta verificación se busca que todos los usuarios tengan verificado su correo electrónico.

Resultado esperado: que todos los usuarios tengan su email verificado

Pasos para verificación:

- Ir a Configuración
- Buscar Usuarios → Usuarios
- Revisar que todos los usuarios activos que puedan enviar email tengan verificado el correo electrónico. Para este paso, es conveniente agregar el campo «Correo electrónico verificado» a la lista de usuarios que se está observando. De esta forma queda el check de correo electrónico verificado junto al check de usuario activo. Todos los usuarios activos que podrán enviar emails deben tener el correo electrónico verificado.
- Verificar email de usuarios no verificados. Ingresar en cada usuario no verificado. Donde está el correo electrónico va a decir «Verificar». Allí se debe hacer click y el usuario recibirá un correo electrónico para aceptar la verificación del email.

3. Verificación del dominio de la organización

En esta verificación Salesforce revisa que se cumplan las condiciones mínimas de seguridad para operar con la plataforma y envíos de correos electrónicos desde el dominio. Busca evitar robo de identidad y uso de dominio sin permisos.

Resultado esperado: que la organización tenga verificado su dominio en Salesforce

Pasos para verificación:

- Ir a configuración
- Buscar “Disponibilidad” y cargar los dominios identificados
- Hacer click en “Check Verification”.
- Si el resultado es “Domain Verified” está todo configurado ok
- Si el resultado es “Domain Not Verified” es porque falló o falta alguna de todas las acciones indicadas en este documento