mailgun by sinch

GUÍA

La guía de Mailgun sobre seguridad y el cumplimiento de la normativa en los emails

Protegiendo a nuestros clientes
en un entorno digital peligroso

Índice

Índice

INTRODUCCIÓN

Duras realidades sobre el email

Es hora de hacer frente a la realidad. Aunque a todos nos encanta usarlo, el email es un riesgo importante para la seguridad de tu empresa. Si estás leyendo esto, es probable que estés involucrado en proteger a aquellos que podrían verse afectados negativamente por una violación o por no cumplir con las normativas de privacidad.

No te engañes. Tanto evitar que los agentes malintencionados utilicen el correo electrónico para hacer el mal como seguir las mejores prácticas en materia de privacidad y seguridad son tareas difíciles. El equipo de Mailgun by Sinch es totalmente consciente de ello.

Sin embargo, **creemos que merece la pena proteger tu programa de email** y que educar a otros sobre cómo hacerlo promueve un mundo digital más seguro. En esta guía completa, descubrirás valiosas ideas y obtendrás consejos de expertos sobre cómo proporcionar esa protección.

Pero primero, enfrentémonos a los hechos. **Estas son cinco duras realidades sobre el email:**

1. El email es el mayor vector de amenazas

El email es una de las herramientas preferidas entre los ciberdelincuentes, y la bandeja de entrada uno de sus lugares favoritos.

Tanto si se trata de correo no deseado estándar, un ataque de phishing o un intento de lanzar ransomware y malware, la bandeja de entrada representa una oportunidad para que los agentes malintencionados hagan de las suyas... y sin ensuciarse las manos.

En 2022, la cadena hotelera Marriott informó de su tercera brecha de seguridad importante en cuatro años. Esta vez fue un ataque de ingeniería social que dio a un actor malintencionado acceso al ordenador de un empleado. Marriott ha gastado más de 16 millones de dólares este año para recuperarse de otra brecha que se produjo en 2018.

Los agentes malintencionados incluso están buscando formas de evitar la autenticación multifactor (MFA) con herramientas y técnicas de phishing por ataque de intermediario (AiTM). Microsoft dice que una artimaña reciente está poniendo en riesgo a miles de organizaciones.

El correo electrónico proporciona una vía que permite a los estafadores infiltrarse en las corporaciones. Se puede utilizar para llegar a un gran número de víctimas potenciales o para llegar a un público muy específico, como en el caso del "spear phishing" o "phishing dirigido". Dado que casi todo el mundo tiene una dirección de correo electrónico, los agentes malintencionados ni siquiera necesitan contar con un alto índice de éxito. Engañar a una sola persona es suficiente para trastornar a toda una organización.

Aun así, no podemos renunciar a utilizar el correo electrónico porque lo necesitamos.

2. El email va a seguir vigente

A pesar de los constantes cambios tecnológicos en la era digital, el correo electrónico sigue siendo una de las mejores formas de comunicarse con clientes y colegas, de llegar a una audiencia y de hacer negocios. Desde emails transaccionales que contienen información importante hasta emails de marketing que ayudan a impulsar el crecimiento de una empresa, sería difícil para una empresa funcionar sin enviar y recibir emails.

Cada vez que alguien configura un nuevo dispositivo móvil o abre una cuenta en línea, necesita una dirección de email. Es una información de identificación personal (PII) vital y que todos usamos para acceder a aplicaciones y servicios digitales. Por eso el robo de identidad es algo muy fácil cuando un delincuente obtiene acceso a una cuenta de email.

Se estima que se envían y reciben más de 333 000 millones de correos electrónicos en todo el mundo todos los días. **Para 2025, se espera que ese número supere los 376 000 millones**. Por supuesto, muchos de esos correos provienen de spammers y estafadores.

3. Las leyes y restricciones de privacidad son cada vez más estrictas

En un esfuerzo por hacer de la bandeja de entrada y de internet en general un lugar más seguro, los gobiernos están redactando leyes y las principales empresas tecnológicas están introduciendo nuevas funciones para proteger a las personas que utilizan sus servicios de email.

Por ejemplo, Apple sacudió el mundo del email cuando introdujo la Protección de la Privacidad de Mail en 2021. En 2017, Google dejó de leer los correos electrónicos de los usuarios de Gmail con fines publicitarios. Y los expertos en email de Mailgun dicen que los filtros de spam por IA de Gmail son los mejores del sector.

Las leyes sobre la privacidad de los clientes, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Ley de Privacidad de los Consumidores de California (CCPA) en Estados Unidos, están diseñadas para dar más poder a las personas y, al mismo tiempo, evitar que se abuse de los datos sensibles.

El problema es que la mayoría de remitentes legítimos ya siguen todas las normas y las mejores prácticas. **Son los agentes malintencionados los que no las siguen**. Son delincuentes precisamente porque se niegan a seguir las leyes.

4. La ciberdelincuencia está en constante evolución

No importa lo que hagan los proveedores de correo y los ESP para evitar que los correos electrónicos maliciosos lleguen a la bandeja de entrada de la gente; los agentes malintencionados siempre parecen encontrar una forma de salirse con la suya. Sus tácticas siguen cambiando, volviéndose más complicadas, y sus estrategias siguen avanzando.

Nick Schafer lidera el equipo de Entregabilidad y cumplimiento de Mailgun. Nick y su equipo trabajan para mantener a los agentes malintencionados lejos de nuestra plataforma a través de, entre otras medidas, supervisar las actividades sospechosas y manteniéndose al día en cuanto a las tendencias de seguridad en el email. Nick lo describe como una batalla interminable:

"Odio tener que decir esto, pero la verdad es que pararlos por completo es imposible. Aunque se les puede batir. En cuanto descubrimos una forma de detener una estratagema de las suyas, ellos crean una nueva táctica. Pero eso no significa que nos debamos rendir. Si lo mejor que podemos hacer es frenarles, eso es lo que haremos".

Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

5. Los remitentes deben ir un paso por delante

Todo esto significa que los remitentes deben estar siempre al día en materias de seguridad para los emails y de protección de la privacidad. Tu organización tiene que hacer todo lo posible para evitar problemas, a la vez que se mantiene lista y preparada para mitigar la situación si pasase algo malo.

Para ir un paso por delante de los agentes malintencionados que quieren utilizar el email para estafar a sus suscriptores o engañar a las personas de su organización es necesario contar con lo siguiente:

- Una plantilla educada sobre el tema y consciente de los riesgos
- Protocolos sólidos de autenticación de emails
- Conocimiento de la normativa sobre privacidad y su relación con el email
- Socios que puedan ayudar a tu equipo a mantener la seguridad en cuanto al email

Nos centraremos en estas áreas a lo largo de esta guía. A lo largo de la guía, también escucharás de los expertos de Mailgun que trabajan estrechamente con los usuarios para proteger nuestra plataforma y los programas de correo electrónico de nuestros clientes.

Por qué merece la pena proteger el email

Aunque los spammers y los estafadores no cejan nunca en su empeño, centrarse en la seguridad del email y la protección de la privacidad es, sin duda, una tarea que merece la pena.

A continuación te indicamos a quién y qué estás protegiendo cuando priorizas la seguridad y el cumplimiento de las normativas:

1. El negocio

Según un estudio global de IBM, el coste promedio de una violación de datos fue de más de 4 millones de dólares en 2021, y **el impacto financiero promedio de un ataque de phishing fue de 4,65 millones de dólares**. Los ataques por correo electrónico empresarial (BEC), que son una forma de phishing dirigido, fueron los que más pérdidas generaron, con algo más de 5 millones de dólares por violación.

En el mismo estudio de IBM se descubrió que normalmente las empresas tardan más de 280 días en detener y resolver este tipo de ataques. Ahí se incluye el tiempo y los recursos que necesitan los equipos de TI y de ciberseguridad para identificar los puntos débiles y crear actualizaciones para corregir las vulnerabilidades.

2. Reputación de la marca

Las brechas de seguridad y las estafas relacionadas con tu organización provocan mala prensa y dañan la reputación de la marca, lo que se traduce en una pérdida de confianza. El estudio de IBM descubrió que las pérdidas en cuanto a ingresos **representaban el 38 % de los costes totales o casi 1,6 millones de dólares por brecha**.

Por supuesto, el impacto en la reputación de la marca puede ir más allá de lo que se mide en meros costes financieros. Las empresas que han sido víctima de ataques por suplantación de identidad de marca pueden encontrar que es menos probable que los contactos abran e interactúen con sus correos electrónicos, porque no están seguros de que los mensajes sean genuinos.

3. Reputación del remitente

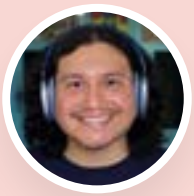
Además de la reputación de marca, los proveedores de correo como Gmail, Apple Mail y Yahoo Mail tienen formas de medir y puntuar la reputación de un remitente de correo electrónico. Si no se configuran correctamente los registros DNS para la autenticación del email, es más difícil que los proveedores de buzones confíen en que tus correos son legítimos.

Eso podría significar que los emails que envíes tengan más probabilidades de ser bloqueados o de caer en la carpeta de correo no deseado. Por lo tanto, si existe una ausencia de protocolos de autenticación o si los hay pero no funcionan bien, eso puede afectar negativamente a la reputación del remitente y a la entregabilidad de los emails.

4. Usuarios y clientes

Quizás la consideración más importante es cómo la seguridad y la autenticación de emails ayudan a proteger a tus clientes o a los usuarios de tus aplicaciones. La privacidad, las identidades y las finanzas de las personas a las que sirve tu organización están en riesgo si no das prioridad a la seguridad y el cumplimiento normativo.

Jonathan Torres dirige equipos de gestores de cuentas (TAM) para Mailgun y otros productos de Sinch. Jonathan nos recuerda que el email forma parte de un ecosistema digital interconectado.



"El cumplimiento, la seguridad y la entregabilidad del correo electrónico no son solo problemas para el remitente. Si solo piensas en el impacto que tiene todo eso en ti, estás viendo las cosas desde un prisma demasiado limitado. Los proveedores de buzones de email, los abonados, los clientes, los empleados, las marcas... Esos problemas afectan a todos estos ámbitos y más. Todo el mundo acaba implicado".

Jonathan Torres, mánager del equipo de TAM, Mailgun

PARTE 1

Estafas por email: ayer y hoy

Para entender por qué el correo electrónico es el mayor vector de amenazas en materia de ciberseguridad, y para comprender la gravedad de la situación, es útil mirar de dónde venimos y cómo hemos llegado hasta aquí.

Viajemos atrás en el tiempo hasta los días de juventud del email. Y acto seguido, echemos un vistazo a algunas estrategias comunes que utilizan los agentes malintencionados en los ataques por email modernos.

Los inicios del email

Al principio, el email era principalmente una forma de comunicación entre oficinas. El programador informático Ray Tomlinson introdujo lo que se cree que es una primera versión del correo electrónico en ARPANET en 1971. Varios años más tarde, un joven Shiva Ayyadurai creó un programa de software que llamó "EMAIL" para reemplazar bandejas de entrada físicas y notas en papel en una escuela de medicina de Nueva Jersey.

Pronto, el email se empezó a usar como medio para comunicarse entre diferentes organizaciones, lo que dio lugar a lo que muchos llaman el primer mensaje de correo electrónico no deseado. Gary Thuerk envió un mensaje no solicitado a cientos de empleados de ARPANET en 1978 promocionando un nuevo modelo de ordenador de la marca Digital Equipment Corporation. Thuerk afirma que el mensaje reportó unos ingresos netos de 13 millones de dólares a DEC.

Y así se abrió la caja de Pandora. El email era un canal ideal para convencer a la gente de que gastase dinero. Sin embargo, cuando el Wall Street Journal conmemoró el 30.º aniversario del correo no deseado en 2008, Thuerk explicó por qué él no se considera responsable del monstruo en que se ha acabado convirtiendo el correo electrónico no deseado.

"Si la aerolínea pierde tu equipaje, ¿la culpa es de los hermanos Wright?".

Gary Thuerk, "Padre del correo no deseado"

A medida que más consumidores adquirían ordenadores personales y acababan conectándose a internet, los agentes malintencionados vieron la oportunidad de explotar las bandejas de entrada para obtener más beneficios. Y era sencillo.

Cuando un correo electrónico era nuevo y emocionante, la gente lo abría, lo leía y respondía a casi cualquier mensaje recibido. El usuario promedio de internet también era bastante crédulo. Algunas de las artimañas en las que picaba la gente por aquel entonces son tan irrisorias que se han convertido en chistes hoy en día.

La estafa por email del "príncipe nigeriano" es un ejemplo perfecto. Había muchos sistemas similares de fraude electrónico que decían a los destinatarios que había ganado la lotería o que habían recibido una herencia inesperada de un pariente olvidado. Sorprendentemente, muchas de estas antiguas y aparentemente desfasadas tácticas aún se utilizan a día de hoy.

En los años 90, el email era un poco como el salvaje oeste americano, con spammers causando estragos como los forajidos de antaño. Pero un nuevo sheriff estaba a punto de llegar a la ciudad, o a la bandeja de entrada para ser más precisos.

Medidas contra el correo no deseado

Avancemos ahora hasta principios de los años 2000. Era un periodo en el que el acceso telefónico a internet, los pantalones vaqueros desgastados y los CD de los años 90 ya estaban en declive. También era un periodo en el que el correo no deseado por email se disparó y, en respuesta, los legisladores estadounidenses aprobaron la Ley CAN-SPAM en 2003.

Hacia esa misma época, Kate Nowrouzi empezó a trabajar en America Online (AOL). En la actualidad, Kate es la vicepresidenta de Entregabilidad y desarrollo de productos de Mailgun. En aquel entonces, ella formaba parte del equipo antispam de AOL.

En 2003, AOL seguía siendo uno de los mayores proveedores de servicios de email del mundo, junto con Hotmail y Yahoo Mail. En su apogeo, AOL llegó a contar con más de 35 millones de usuarios. Era el proveedor más usado para email y conectividad a internet. AOL también estaba en la cresta de la ola en la lucha contra el correo no deseado.

Kate y el equipo antispam de AOL empezaron a darse cuenta de lo difícil que era determinar si un mensaje era correo no deseado o un correo electrónico legítimo que un abonado deseaba recibir. El tipo de contenido o la industria involucrada no eran una indicación idónea. Incluso las empresas que se dedican a contenidos para adultos o que venden Viagra tienen motivos reales para enviar correos electrónicos a los suscriptores.

"Teníamos algoritmos integrados en los filtros para detectar patrones de correo no deseado, y solíamos realizar análisis manuales sobre el tráfico entrante que era sospechoso. Pero la definición de "correo no deseado" puede ser muy diferente según a quién preguntes. Así que decidimos dar poder a los miembros de AOL. Les permitimos decidir si deseaban o no recibir ciertos correos".

Kate Nowrouzi, vicepresidenta de Entregabilidad y desarrollo de producto, Mailgun

Esto resultó en la primera **función "marcar como spam"**, lo que convirtió a AOL en el primer proveedor de servicios de email en incluir un **intercambio de información** con sus usuarios como principales beneficiados. A continuación, el equipo antispam de AOL comenzó a desarrollar reglas para evaluar cuántas quejas de correo no deseado (según un porcentaje del volumen) podría recibir un remitente antes de que AOL bloqueara sus correos electrónicos. Esto finalmente condujo a la métrica de emails conocida como el **índice de quejas**, que es un factor que los proveedores de servicios de email utilizan para juzgar la reputación del remitente.

Y claro, aunque todo esto ayudó a *controlar el correo no deseado*, no lo detuvo por completo. Los agentes malintencionados empezaron a desarrollar nuevas tácticas.

Crece la sofisticación

Kate señala que no todo el correo electrónico no deseado es igual. Hay spammers tradicionales que simplemente no tienen permiso para enviarte correos electrónicos y solo quieren hacer algo de dinero contigo. Sin embargo, son los remitentes con ideas potencialmente dañinas en mente los que representan la mayor amenaza. Y esos estafadores cada vez se vuelven más astutos.

"Las cosas han cambiado mucho. El correo no deseado está en constante evolución. Es un ciclo interminable. En Mailgun mejoramos nuestra plataforma como proveedor de servicios de correo electrónico, y los ISP hacen lo mismo por su parte. Así que todos estamos trabajando arduamente para proteger a nuestros usuarios de actividades maliciosas. Pero a veces los spammers pueden ser muy convincentes, especialmente si utilizan la ingeniería social".

Kate Nowrouzi, vicepresidenta de Entregabilidad y desarrollo de producto, Mailgun

Los agresores son capaces de llevar a cabo estos ataques de ingeniería social en la bandeja de entrada porque hoy en día hay mucha información sobre las personas y las empresas disponible en línea. Pueden descubrir muchas cosas simplemente examinando la presencia pública de una persona o empresa objetivo en las redes sociales.

Hoy en día, en lugar de estafas por correo electrónico que proceden de un falso príncipe nigeriano, **estas estafas pueden parecer mensajes procedentes de tu banco, tu mejor amigo o tu jefe**.

No hace mucho tiempo, Kate hizo una donación en un evento de recaudación de fondos público en Facebook. Luego recibió lo que *creía* que era un email del anfitrión de esa recaudación de fondos, un conocido fundador en Silicon Valley. En el email se le daba las gracias por donar y se le pedía más apoyo en forma de tarjetas de regalo de Amazon.

En un principio Kate no se percató de uno de los signos reveladores de que el email era falso: un guion bajo en la dirección de correo electrónico entre el nombre y el apellido del remitente, algo que difería de la dirección de email real. Pero a medida que continuaban las comunicaciones con el estafador, vio signos más evidentes, como una ortografía y gramática deficiente y un uso extraño de los emojis. Una serie de cosas que no eran típicas del individuo que los estafadores estaban suplantando.

> *"Si yo que he estado en esta industria durante 20 años piqué con esta artimaña, no me quiero imaginar qué pasaría con alguien como mi madre".*
>
> Kate Nowrouzi, vicepresidenta de Entregabilidad y desarrollo de producto, Mailgun

Adentrándonos en la mente de un estafador moderno

Aunque hay muchos tipos diferentes de estafas por email y muchas formas de eliminarlas, uno de los ataques más frecuentes en los últimos años es una forma de phishing conocida como "**suplantación de identidad de marca**". Este ataque consiste en que los agentes malintencionados encuentran formas de suplantar a una empresa a través de correos electrónicos y sitios web falsos con el fin de engañar a la gente para que les den las credenciales de su cuenta u otra información confidencial. La autenticación de email con DMARC es la mejor manera de protegerse contra estas amenazas.

Sin embargo, si un agente malintencionado obtiene las credenciales SMTP o las claves API, puede literalmente enviar mensajes como si fuesen de tu marca, lo que podría causar graves estragos.

Jonathan Torres se puso en la piel de un estafador y explicó el proceso básico. Así es como suele ocurrir, en tan solo cinco sencillos pasos.

Cómo funciona la suplantación de marcas por email

Paso 1

Encontrar una marca reconocible que sea vulnerable a la suplantación de identidad.

Las empresas relacionadas con el mundo de las finanzas, el comercio electrónico y la tecnología se encuentran entre las que tienen más probabilidades de ser suplantadas.

Paso 2

Buscar claves API desprotegidas o "craquear" las contraseñas SMTP.

Esto permite a los agentes malintencionados enviar como si fuesen la propia marca, engañando a los proveedores de correo y a los abonados.

Paso 3

Diseñar una página de destino falsa o una página de inicio de sesión falsa.

Con unas cuantas herramientas básicas y el logotipo correcto, es fácil imitar el aspecto del sitio web de una marca.

Paso 4

Redactar un email falso pero convincente.

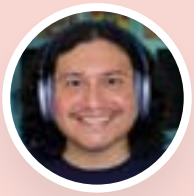
Los estafadores suelen apelar a las urgencias para inducir a las víctimas a actuar sin pensar.

Paso 5

Recopilar las credenciales de la víctima.

El email dirige a los destinatarios a la página de destino falsa. Allí, la persona intenta iniciar sesión en su cuenta, pero en realidad lo que está haciendo es desvelar información confidencial a un estafador.

Como puedes ver, no es necesario ser un superhacker para urdir un ataque por suplantación de marca. Cualquiera que tenga algunas herramientas como Photoshop, un creador de sitios web gratuito y una lista de direcciones de email puede intentarlo. Imitar a una marca reconocible es pan comido.



"Si puedes enviar un email que parezca provenir de una empresa conocida, puedes enviar a la gente a páginas de destino falsas. Y cuando un estafador tiene acceso a tus correos reales, son fáciles de replicar".

Jonathan Torres, mánager del equipo de TAM, Mailgun

Así pues, ¿qué pueden hacer los equipos técnicos para evitar la suplantación de marcas? **La mejor defensa contra la suplantación es implementar protocolos de autenticación de correo electrónico**, algo de lo que hablaremos en la Parte 5. Pero si no quieres parecer un spammer a ojos de los proveedores de email y los destinatarios, también tendrás que conocer y atenerte a ciertas normas y reglamentos importantes.

PARTE 2

Cumplimiento y panorama normativo

Antes de centrarnos en cómo evitar que los agentes malintencionados utilicen el correo electrónico para hacer el mal, vamos a asegurarnos de que tú mismo sigas todas las reglas correctas como remitente legítimo y de confianza.

En primer lugar, aquí tenemos un resumen rápido sobre las partes involucradas en los emails y la privacidad de los datos:

1. Sujetos de datos:

Este término hace referencia al consumidor o destinatario de las comunicaciones por email. Los sujetos de datos son personas cuyos datos personales son recopilados, almacenados y utilizados por otros. Las normas de privacidad tienen como objetivo proteger sus derechos.

2. Responsables del tratamiento:

Los responsables del tratamiento son los que recopilan, almacenan y distribuyen la información personal de los sujetos de datos. Son responsables de proteger esa información de identificación personal sin importar adónde vaya esta o quién la manipule.

3. Encargados del tratamiento:

Los encargados del tratamiento son entidades que procesan datos personales en nombre de los responsables del tratamiento. Por lo general, se trata de proveedores externos de soluciones que necesitan acceso a información de identificación personal para brindar un servicio. Debe haber un contrato vigente entre los encargados y los responsables del tratamiento que defina ciertas cosas, como el uso de los datos, el almacenamiento seguro y lo que ocurre con los datos personales cuando la relación comercial termina.

Como remitente de emails, lo más probable es que tu empresa entre en la categoría de "Responsable del tratamiento", mientras que Mailgun sería un "Encargado del tratamiento". Darine Fayed, Delegada de Protección de Datos (DPO) de Mailgun, dice que, aunque nuestra empresa va más allá en lo que respecta al cumplimiento normativo, en última instancia, esta responsabilidad cae sobre los remitentes.

"Cualquiera que utilice datos personales, debe protegerlos. Pero los responsables del tratamiento deben especificar cómo deben almacenarse, tratarse y transferirse los datos personales a terceros. Todo eso se debe hacer de una manera estrictamente conforme con las normativas".

Darine Fayed, Delegada de Protección de Datos y Directora Jurídica, Mailgun

Resumen de las leyes más importantes sobre privacidad de los clientes

Echemos un vistazo a algunos estándares y normativas clave relacionadas con la privacidad del consumidor y la relación de estos con el email.

Hay mucho por tratar, así que aquí abordaremos los conceptos básicos y te indicaremos otros recursos donde podrás obtener más información sobre normativas específicas y cómo pueden estas afectarte como remitente.

RGPD

Esta es la más importante. Promulgada en 2018, el Reglamento General de Protección de Datos (RGPD) de la UE ha hecho mucho para impulsar la privacidad de los consumidores en la dirección correcta.

Aunque los profesionales del marketing estaban muy preocupados por el impacto que el RGPD podría tener en sus actividades, resultó ser algo bueno para todos. Muchos de los requisitos del RGPD ya se consideraban buenas prácticas para los remitentes de correo electrónico, y el reglamento ha llevado a otros a reforzar la protección de la privacidad para ajustarse a la ley.

Algunas de las directrices más importantes del RGPD para los remitentes de email son:

- Obtener consentimiento para enviar emails a alguien
  - Obtener consentimiento explícito para los mensajes comerciales
  - Consentimiento implícito para la mayoría de correos electrónicos transaccionales
- Incluir la posibilidad de cancelar la suscripción a comunicaciones por email (enlace para cancelar la suscripción)
- Garantizar un almacenamiento seguro de los datos utilizados para la personalización de emails

- La capacidad de proporcionar o eliminar toda la información de identificación personal relacionada con un sujeto si este presenta una solicitud de acceso a sus datos de sujeto (DSAR)
- Enlaces a la política de privacidad de la empresa siempre que se recojan datos de identificación personal, como direcciones de email

Darine afirma que las políticas de privacidad de las empresas deben estar redactadas de forma clara y directa, y reducir al mínimo la jerga legal.

> *"Cualquier política de privacidad debe ser clara, comprensible y transparente. Eso significa que tiene que informar a sus abonados y clientes de los datos que se recopilan, para qué fines se piensan utilizar, durante cuánto tiempo se van a almacenar y si se van a transferir a alguna parte. Tu abuela debería poder comprar algo en línea y entender la política de privacidad implicada".*
>
> Darine Fayed, Delegada de Protección de Datos y Directora Jurídica, Mailgun

El RGPD llevó a muchos otros países a examinar con más detalle sus leyes de privacidad de datos. La siguiente lista es una buena muestra de ello. ¡Prepárate para zambullirte en una sopa de letras!

- India implementó la Ley de Protección de Datos Personales (PDPB)
- China cuenta con la Ley de Protección de Datos Personales (PIPL)
- Japón utiliza su Ley de Privacidad de la Información Personal (PIPA)
- Australia ha actualizado su Ley de Privacidad para abordar las cuestiones digitales
- Gran Bretaña promulgó el RGPD del Reino Unido después del Brexit
- Brasil tiene una Ley General de Protección de Datos Personales (LGPD)
- Canadá se atiene a su Ley de Protección de la Información Personal y Documentos Electrónicos (PIPEDA)

Es importante recordar que si tu organización hace negocios con personas en un país específico, debe cumplir con las leyes de privacidad de datos de esa nación. Afortunadamente, si ya estás siguiendo las directrices del RGPD, estarás cubierto en la mayoría de las áreas.

Obtén información sobre el enfoque de Mailgun con respecto al cumplimiento del RGPD.

Obtén detalles importantes sobre nuestro enfoque respecto al RGPD, incluidos el almacenamiento, la seguridad, el procesamiento y la forma en que brindamos soporte a nuestros clientes en lo tocante a los derechos de los sujetos de datos.

CCPA

En Estados Unidos, la normativa sobre privacidad de datos más completa es el California Consumer Privacy Act (CCPA), que se convirtió en ley no mucho después del RGPD. De nuevo, hay muchas similitudes entre las dos normativas, y el CCPA refleja las mejores prácticas comunes para los remitentes de email.

Aunque el CCPA sólo cubre a los residentes del estado de California, muchas empresas estadounidenses e internacionales tienen contactos que residen ahí. Eso significa que deben cumplir con el CCPA.

Aunque hay otros estados con sus propias leyes de privacidad de datos, y otras propuestas están pasando por el proceso legislativo, Darine Fayed dice que una ley federal en los Estados Unidos podría estar en camino en los próximos años.

PCI DSS

La norma de seguridad de datos de la industria de las tarjetas de pago (PCI DSS) tiene por objeto proteger la información de los titulares de tarjetas de crédito. Es una norma mundial que se aplica a cualquier organización que acepte pagos en línea.

El cumplimiento de PCI incluye requisitos para proteger datos como los números de tarjeta de crédito conforme se transmiten a través de redes abiertas, incluidos los emails. En la mayoría de los casos, enviar los datos del titular de la tarjeta por correo electrónico no es una buena idea. Si por algún motivo tienes que transmitir los datos del titular de la tarjeta por correo, asegúrate de que estén siempre cifrados.

Por supuesto, eso es difícil de hacer, especialmente si los números terminan en la bandeja de entrada de alguien o en la carpeta de correos enviados, donde un hacker podría encontrarlos. Es por eso que el requisito 4.2 de la PCI DSS establece que los datos de las tarjetas de crédito no pueden capturarse, transmitirse ni almacenarse a través de tecnologías de mensajería de usuario final, como el email.

La mayoría de las empresas utilizan terceros para el procesamiento de las tarjetas de crédito, y esa empresa se encarga del cumplimiento de PCI. Por ejemplo, Mailgun utiliza el procesador de pagos Stripe. Sin embargo, aun trabajando con un tercero, si tienes datos de titulares de tarjetas almacenados en tus propios servidores o sistemas, debes cumplir con las normas PCI.

HIPAA

La Ley de Portabilidad y Responsabilidad del Seguro Médico de EE. UU. (HIPAA) es una ley estadounidense que se aplica principalmente a las empresas de atención médica. Incluye requisitos que describen cómo evitar que los datos personales sanitarios (PHI, por sus siglas en inglés) de un paciente se revelen incorrectamente.

La cuestión más importante relevante a HIPAA para los remitentes es que cualquier email que contenga PHI **debe cifrarse en tránsito**. Más allá de eso, las empresas de atención médica también deben obtener el consentimiento para enviar correos electrónicos a los pacientes, especificar cómo se utilizará la PHI en una política de privacidad y tener una manera de almacenar de forma segura las comunicaciones por email que contengan esa información.

Obtén consejos más detallados de Mailgun sobre el cumplimiento normativo de la HIPAA y en los emails.

Por tanto, un factor a tener en cuenta es el software y los servicios que utilices para enviar y recibir emails. Para averiguar cómo un proveedor de servicios de correo electrónico (ESP) aborda la privacidad en la atención médica, solicita consultar el Acuerdo de Socio Comercial de HIPAA (BAA). El BAA define las responsabilidades del remitente y del encargado en cuanto al cumplimiento de la HIPAA.

Consulta el BAA de HIPAA de Mailgun.

Revisa el documento legal que explica cómo enfocamos la división de derechos y responsabilidades cuando se trata de proteger los datos personales sanitarios.

Por qué es importante el cumplimiento en materias de email

Aunque sin duda es cierto que el incumplimiento puede desembocar en elevadas multas, Darine Fayed dice que no debería ser la única motivación para adherirse a las normativas de privacidad.

> *"No es cuestión de respetar la privacidad de datos porque tengas miedo de las multas por incumplimiento del RGPD o cualquier otra autoridad que vaya a sancionarte. Eso no es lo importante. Es una decisión de la empresa. Si tratas a las personas con respeto en cuanto a su privacidad, volverán. Las personas son ahora mucho más conscientes de los riesgos en cuanto a privacidad, y de sus derechos. Quieren confiar en las marcas, pero también esperan que estas traten sus datos personales con el debido cuidado".*
>
> Darine Fayed, Delegada de Protección de Datos y Directora Jurídica, Mailgun

Según la encuesta de Cisco sobre la privacidad de los consumidores, **el 89 % de las personas dicen preocuparse por la privacidad de los datos y quieren tener un mayor control**. Sin embargo, menos de un tercio ha emprendido acciones siguiendo esas preocupaciones sobre la privacidad. Lo cierto es que la mayoría de las personas esperan que las tecnologías que utilizan les proporcionen la protección de la privacidad que necesitan. Cumplir con las normativas te ayuda a satisfacer esas expectativas.

PARTE 3

El panorama de las amenazas por email

Para ayudar a tu equipo a comprender las cambiantes amenazas a la seguridad en materia de email a las que se enfrenta tu organización, repasemos algunas conclusiones clave extraídas en investigaciones recientes de líderes en el sector de la ciberseguridad.

Aunque estas estadísticas fluctúan de un año a otro, e incluso de un trimestre a otro, ayudan a hacernos una idea de los desafíos a los que se enfrentan los equipos técnicos mientras trabajan para proteger los emails y todo lo que está conectado al canal.

Phishing: el mayor problema en materia de ciberseguridad

Según Deloitte y muchas otras fuentes, **el 91 % de los ciberataques comienzan con un email de phishing**. La bandeja de entrada es el punto de partida y, a partir de ahí, los estafadores pueden robar credenciales, entregar malware, como el troyano Emotet, o pedir un rescate por los archivos y datos digitales de una empresa.

Según un informe de 2021 de Cisco, **el 50 % de las organizaciones encuestadas experimentaron actividad de ransomware en el año anterior**. Estas brechas de seguridad se pueden pagar muy caras. Una investigación de Palo Alto Networks sacó a la luz **que el pago promedio por ransomware en 2022 se acerca al millón de dólares**, lo que supone un aumento del 71 % con respecto al año anterior.

Por qué el email es una grave amenaza

91 %

Ataques que comienzan con phishing vía email

50 %

Organizaciones que experimentan actividad de ransomware

96 %

Organizaciones atacadas por phishing vía email

El informe de Mimecast, State of Email Security 2022, revela que tres de cada cuatro empresas encuestadas experimentaron un aumento en las amenazas vía email, mientras que el **96 % afirma haber sido objetivo del phishing vía email**.

Nick Schafer, de Mailgun, está de acuerdo en que el ransomware puede reportar a los agentes malintencionados un gran beneficio. Sin embargo, afirma que el gran número de ataques de phishing por email debería convertirlo en una prioridad de seguridad para todas las organizaciones

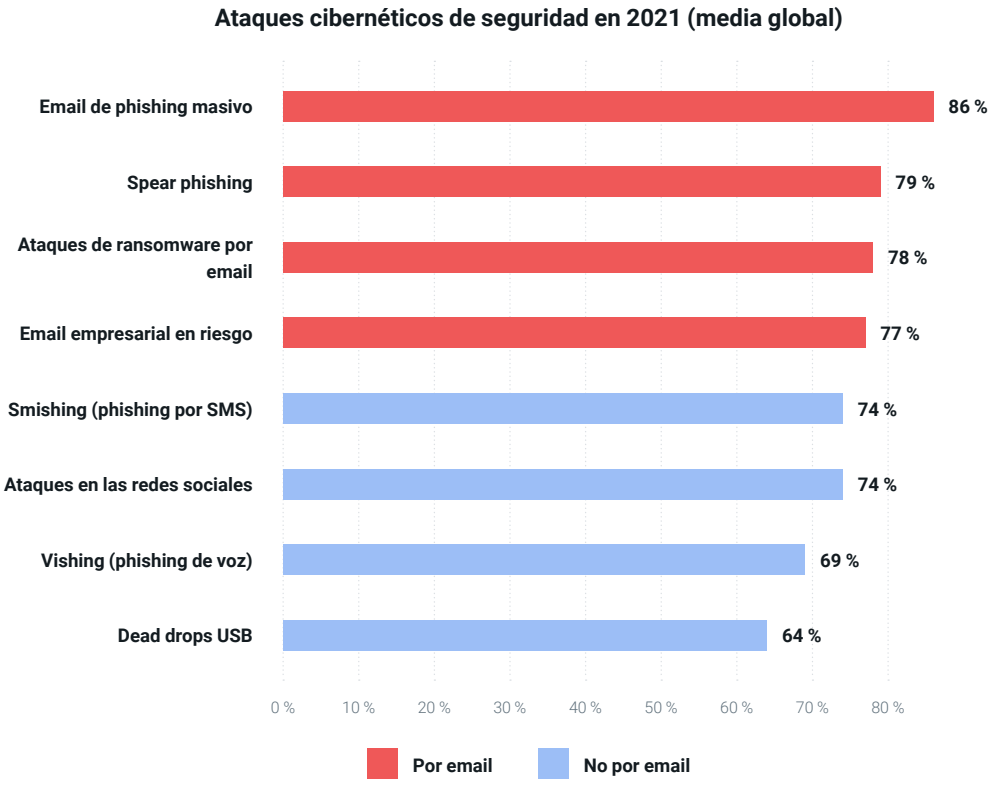
"Desde mi punto de vista, el phishing es el mayor problema. Estoy seguro de que los estafadores piensan en el rendimiento de la inversión como cualquier otra persona, y pueden obtenerlo de los ataques de ransomware. Pero en términos de lo que vemos, la cantidad de ataques de phishing solo está empeorando. Y son buenos en lo que hacen".

Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

Comparación de las amenazas por email y otros canales

El informe de Proofpoint 2022 State of the Phish examinó cómo el email y otras formas de phishing están afectando a las empresas de todo el mundo. En él se encuestó a cientos de profesionales de la informática y a miles de trabajadores de Estados Unidos, Australia, Francia, Alemania, Japón, España y el Reino Unido.

Si bien las empresas de estas naciones experimentaron todo tipo de amenazas a través de diferentes canales, **los ataques por email ocuparon los cuatro primeros puestos**. Un total del 86 % de las organizaciones encuestadas por Proofpoint informaron al menos de un ataque masivo de phishing por email en 2021, convirtiéndolo en el tipo de ataque más común.



De todos los diferentes tipos de intento de phishing, **el 83 % de los encuestados a nivel mundial dijo que al menos uno de esos ataques tuvo éxito en 2021**.

El impacto del phishing

Ya hemos revelado que el impacto monetario potencial de mitigar una brecha de seguridad puede resultar bastante costoso, pero los millones de dólares gastados a raíz de un ciberataque no son las únicas formas en que estos incidentes afectan a las empresas, tanto grandes como pequeñas.

La encuesta de Proofpoint preguntó a los profesionales de TI de todo el mundo sobre cuál fue el mayor impacto que tuvieron los ataques de phishing en sus organizaciones. Los efectos más citados fueron la violación de los datos de los clientes (54 %), las credenciales comprometidas (48 %) y las infecciones por ransomware (46 %).

Principales impactos de un ataque de phishing exitoso

54 %
Violación de datos de los clientes

48 %
Credenciales/cuentas comprometidas

46 %
Infecciones por ransomware

No muy lejos de las infecciones por ransomware, Proofpoint encontró **que el 44 % de los encuestados citó la "pérdida de datos y de propiedad intelectual" como otro impacto negativo de un ataque de phishing exitoso**. Lo cierto es que todos estos factores pueden tener un impacto duradero en un negocio, erosionando la confianza, aumentando los costes e incluso exponiendo los secretos comerciales que dan a las empresas una ventaja competitiva.

Dar prioridad a los proyectos de seguridad

Entonces, ¿en qué centran sus esfuerzos los equipos técnicos cuando se trata de frustrar las brechas de seguridad? Teniendo en cuenta las estadísticas que acabamos de ver, no debería ser ninguna sorpresa que la protección del email **sea una de las principales preocupaciones de seguridad de muchas organizaciones**.

GreatHorn encuestó a cientos de profesionales de TI y ciberseguridad para descubrir qué les preocupaba más. Los tres principales tipos de proyectos citados por los encuestados en 2021 fueron: la seguridad del email (48 %), la seguridad en torno al trabajo remoto y el teletrabajo (41 %) y la gestión de la postura de seguridad en la nube o CPSM (40 %).

Principales proyectos de seguridad en 2021

48 %
Seguridad del email

41 %
Seguridad del teletrabajo

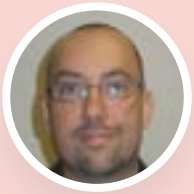
40 %
Gestión de la postura de seguridad en la nube (CPSM)

Un proyecto de TI más específico relacionado con todas estas preocupaciones de seguridad es el paso de una solución de email local a un enfoque nativo en la nube. GreatHorn descubrió que, si bien solo el 24 % de los encuestados sigue utilizando una solución local, **el 77 % de esas organizaciones planeaba pasarse a proveedores con infraestructura de email nativa en la nube**. Esto permite a los remitentes encontrar proveedores con medidas de seguridad más avanzadas, incluyendo asociaciones con servicios de computación en la nube pública de confianza como Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure.

Por supuesto, la mejora de la ciberseguridad en torno al email o a cualquier otra área requerirá una inversión de tiempo, recursos y presupuesto. Así que un déficit en los presupuestos de ciberseguridad puede dejar a los equipos técnicos con las manos atadas.

El informe del 2022 State of Email Security (Estado de la seguridad del email 2022) de Mimecast desveló que **el 95 % de los que tienen deficiencias en el presupuesto de ciberseguridad cree que eso afectó a la resistencia ante ataques y resultó en una preparación inadecuada**. El informe dice que algunos esfuerzos, como la capacitación en concienciación sobre seguridad y nuevas tecnologías, son áreas a las que se dedican fondos insuficientes.

Dan Ross lidera el equipo de Gobernanza, Riesgos y Cumplimiento (GRC) de Mailgun by Sinch. Dan nos dice que el compromiso de nuestra organización de invertir en una seguridad sólida resulta en una ventaja evidente para su equipo, nuestros clientes y todos nuestros empleados.



"El equipo de dirección ha hecho un trabajo realmente bueno dándonos el presupuesto suficiente para proteger los datos de nuestra empresa y de nuestros clientes con la mejor tecnología disponible en la industria. Creo que lo que posiciona a Mailgun como líder en seguridad es la forma en que reaccionamos ante las amenazas conocidas y las herramientas que utilizamos para asegurarnos de que los agentes malintencionados no puedan entrar en nuestra red. Además, internamente tenemos medidas para proteger a los empleados de sí mismos".

Dan Ross, mánager sénior de GRC, Mailgun

PARTE 4

En primera línea de la seguridad del email

Hay varios lugares en los que la seguridad del email podría verse comprometida:

1. En la ubicación donde se almacenan los datos de los emails y la información de los contactos
2. En plataformas compartidas para el envío de correos electrónicos
3. Cuando los mensajes están en tránsito o siendo enviados desde un ESP a los destinatarios
4. Cuando un email llega a una bandeja de entrada para su autenticación y filtrado
5. Después de recibir un mensaje y colocarlo en la bandeja de entrada de un destinatario

Algunas partes implicadas tienen responsabilidades específicas con respecto a la seguridad y la privacidad a lo largo del camino. Analicemos cada una de las áreas anteriores y averigüemos más sobre lo que se necesita para lograr una seguridad sólida en todos los ámbitos relacionados con el email.

Seguridad del email y almacenamiento de datos

Tanto si los datos del correo electrónico se almacenan in situ en las instalaciones como en la nube, estos deben estar protegidos con cifrado cuando no estén en tránsito. Por ejemplo, **Mailgun utiliza el cifrado AES-256 en reposo para todos los datos de cliente**. Esto significa que se requiere una clave de 256 bits para cifrar y descifrar bloques de mensajes.

AES es un método de código abierto utilizado en todo el mundo. Se considera eficaz para evitar los ataques de fuerza bruta, y es lo que utilizan las agencias gubernamentales, como la Agencia de Seguridad Nacional de Estados Unidos (NSA), para el cifrado de datos. Los principales proveedores de nube pública como GCP, AWS y Azure también utilizan el cifrado AES-256.

La mayoría de remitentes que envían un gran volumen de emails han recurrido a soluciones basadas en la nube para el correo electrónico. Al elegir colaboradores que almacenen direcciones de email o cualquier otro dato confidencial en tu nombre, existen otras medidas de seguridad que ayudarán a proteger esa información dentro de los centros de datos. Esto incluye pasos como controlar el acceso a los centros de datos con sistemas de vigilancia y control biométrico las 24 horas del día.

Procesamiento de datos en Mailgun.

Echa un vistazo a nuestro acuerdo de tratamiento de datos (DPA, por sus siglas en inglés). Profundiza en los detalles legales y descubre cómo gestionamos el tratamiento de datos y el cumplimiento de la normativa tanto para nuestra empresa como en nombre de nuestros clientes.

Seguridad del email y reputación como remitente

Cuando utilices un proveedor de servicios de correo electrónico como Mailgun, a menudo tendrás la opción de elegir planes que utilicen direcciones IP dedicadas o compartidas para el envío de emails.

A menos que seas un remitente con gran volumen de envíos, una dirección IP compartida suele ser suficiente. Pero, ¿qué ocurre si envías correos desde la misma IP que un agente malintencionado? **Eso podría suponer que tu reputación como remitente se viese afectada**.

Los proveedores de buzones de email utilizan diversos factores para calificar la reputación de un remitente. Dos de los más importantes son la reputación del dominio y de la IP.

Parece que los proveedores de buzones como Gmail han comenzado a dar una mayor importancia a la reputación del dominio. Esto se debe a que ese método es más específico para remitentes concretos. Muchos dominios podrían enviar desde una única dirección IP. Por lo tanto, la reputación de un dominio está más estrechamente conectada a un determinado negocio o marca. Sin embargo, la reputación de una IP sigue siendo un factor, especialmente con el cliente de email de Outlook, lo que significa que **la reputación de IP podría tener un efecto extragrande en los correos de negocio a negocio (B2B)**.

Por esta razón (entre otras), Mailgun trabaja duro para evitar que los agentes malintencionados utilicen nuestra plataforma para enviar emails desde IP compartidas. Nick Schafer y el equipo de Entregabilidad y cumplimiento revisan y evalúan a los nuevos usuarios antes de que se les permita usar la plataforma.

"Si los remitentes malintencionados entran en una de nuestras IP compartidas, los proveedores de servicios de email se darán cuenta. La reputación como remitente de otros clientes en la misma IP podría verse afectada negativamente porque ahora el proveedor de servicios de email ve la IP compartida como un sitio desde el que los remitentes llevan a cabo actividades sospechosas. Por eso nos preocupamos por detener a los agentes malintencionados y por hacer que los clientes sigan las mejores prácticas. Así protegemos la reputación de Mailgun como remitente, lo que es realmente importante para los usuarios con direcciones IP compartidas".

Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

Los clientes de Mailgun también deben cumplir con nuestra política de uso aceptable (AUP), que es otra medida que usamos para proteger la reputación de todos los usuarios. **Nuestra AUP incluye, entre otras, las siguientes estipulaciones**:

- Tasa de rebote inferior o igual al 5 %
- Tasa de bajas inferior o igual al 1,4 %
- Tasa de quejas por correo no deseado inferior o igual al 0,8 %
- No se usan listas de contactos compradas, alquiladas u obtenidas por "scraping"
- Se obtiene el consentimiento expreso antes de enviar correos electrónicos no transaccionales
- Se incluye un enlace para cancelar la suscripción en todos los emails
- No se almacena, transmite ni publica contenido prohibido (préstamos sobre el sueldo, apuestas ilegales, material difamatorio, contenido que promueva la violencia, etc.)
- Se evita el uso excesivo de los recursos compartidos de la plataforma

La AUP garantiza que todos trabajemos juntos para seguir las mejores prácticas como remitentes en un entorno digital compartido. No está ahí como amenaza a nadie. La AUP es más bien un código de conducta común.

> *"Estas son las directrices que supervisamos entre los clientes de Mailgun, pero si alguien se pasa de la raya, no necesariamente lo vamos a echar de la plataforma. Sabemos que todos somos humanos. Así que, primero les solicitamos que pongan un poco de orden en sus envíos".*
>
> Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

Cifrado: seguridad de los emails en tránsito

El protocolo simple de transferencia de correo (SMTP) es el protocolo estándar para la transmisión de emails. Los servidores SMTP procesan el correo, enviando, recibiendo y retransmitiendo mensajes de un servidor a otro. Pero el SMTP tiene un gran problema: no es seguro.

El SMTP en su forma básica no admite algoritmos de cifrado o autenticación. Esa es otra razón por la que los spammers y estafadores utilizan el correo electrónico y por la que se crearon protocolos separados de autenticación de emails, como SPF y DKIM.

Los spammers y phishers han explotado a menudo los servidores SMTP configurados con servidores abiertos. Pero los servidores SMTP protegidos por contraseña también pueden ser hackeados, exponiendo los datos que contienen los correos electrónicos. Los agentes malintencionados pueden utilizar SMTP para propagar virus y malware, así como para llevar a cabo ataques de denegación de servicio (DoS). Incluso es posible modificar un mensaje de email mientras este está en camino hacia el destinatario. Por lo tanto, los datos también necesitan protección mientras los emails están en tránsito.

Por eso, los remitentes y los ESP agregan protocolos de cifrado como Transport Layer Security (TLS) y Secure Sockets Layer (SSL) a SMTP. Mailgun dejó de admitir SSL en 2014 debido a una vulnerabilidad conocida como POODLE, que habilitó los ataques de intermediario (MTM).

TLS utiliza un cifrado asimétrico para establecer una sesión segura entre un cliente y un servidor. Acto seguido, utiliza el cifrado simétrico para intercambiar datos dentro de la sesión segura. Esto se conoce como el protocolo de enlace TLS: el proceso por el cual se establece y define la comunicación entre un cliente y un servidor.

Por defecto, Mailgun ahora utiliza lo que se conoce como **cifrado TLS opcional** (TLS versión 1.2) en los emails, método en el que se intenta utilizar TLS con los servidores receptores siempre que es posible, pero cambia a SMTP de texto sin formato si TLS no es compatible, lo que garantiza la entregabilidad.

También puedes añadir marcadores al cifrado TLS opcional para personalizar la configuración de conexión para la entrega de correo. Estos marcadores son `require tls` y `skip verification`.

- `require tls:`
  - Cuando se establece como TRUE, el servidor receptor solo entregará un mensaje si el servidor receptor es compatible con TLS.
  - Si se establece como FALSE, se intentará utilizar TLS; pero se entregará SMTP de texto sin formato si no se consigue.
- `skip verification:`
  - Si se establece como TRUE, no se intentará verificar el certificado y el nombre de host cuando se intente establecer una conexión TLS.
  - Cuando se establece como FALSE, se intentará verificar el certificado y, si no se pudiese, no se establecerá una conexión TLS.

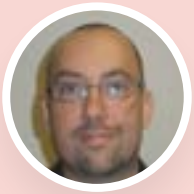
Obtén más información sobre TLS y los emails.

Obtén información esencial sobre el cifrado de la comunicación por email y cómo funciona el control de la conexión TLS en Mailgun.

Mailgun suele recomendar el uso de nuestra API de email en lugar de SMTP. La API es hasta tres veces más rápida, fácil de usar e ideal para envíos de gran volumen por lotes. Además, Mailgun ofrece la posibilidad de utilizar diferentes claves de envío de dominio al gestionar múltiples remitentes. Sin embargo, los hackers pueden acceder tanto a las credenciales SMTP como a las claves API.

Por eso es tan importante rotar regularmente las claves de API y proteger las contraseñas SMTP. Jonathan Torres, de Mailgun, afirma que exponer accidentalmente las claves de API y las credenciales SMTP son dos de las formas más comunes de poner en riesgo la seguridad de los emails.

Dan Ross señala que los datos de emails también necesitan protección cuando se trasladan listas de contactos entre plataformas. Esta es otra situación en la que los datos confidenciales corren peligro durante el tránsito.



"Es importante entender cómo se incorporan las direcciones de email y los contactos a las herramientas que utilizas para enviar mensajes. Mailgun tiene una API segura: un elemento que nos diferencia del resto en el sector. Nuestros clientes utilizan la API para cargar emails y direcciones de email a una velocidad increíble. Si tienes un túnel seguro, reduces el riesgo de que los datos se intercepten durante el tránsito".

Dan Ross, mánager sénior de GRC, Mailgun

Seguridad y autenticación de emails

Si los agentes malintencionados intentan suplantar tu marca mediante emails de phishing, existen algunas formas muy eficaces de impedir que esos correos lleguen a la bandeja de entrada. **Los protocolos de autenticación de email ayudan a los proveedores de servicios de email a decidir si los correos electrónicos son falsos o fraudulentos** antes de que esos mensajes se entreguen a los destinatarios.

Los protocolos de autentificación del email surgieron a principios de la década de los 2000 como una forma de mejorar la seguridad del SMTP y poner freno al aumento del correo no deseado. SPF y DKIM fueron los primeros métodos ampliamente adoptados. Pronto le siguió DMARC como política para confirmar y ampliar lo que ofrecían SPF y DKIM. En la siguiente sección trataremos estos protocolos en profundidad.

En Mailgun, exigimos a los usuarios que configuren registros SPF y DKIM en sus servidores de sistema DNS. Si no lo has hecho o necesitas ayuda, podemos ayudarte. También recomendamos encarecidamente la aplicación de una política DMARC y podemos recomendar proveedores de servicio fiables a nuestros clientes cuando sea necesario. **Configurar registros DNS para la autenticación también mejorará la reputación como remitente y la entregabilidad del email.**

"Los proveedores de servicios de email necesitan formas de identificar quién es realmente un remitente. Sin autenticación de emails, es difícil saber de dónde proviene realmente el tráfico de correo electrónico. Lo que hace la autenticación para los remitentes es que les permite decir: 'Este mensaje es de nosotros, pertenece a nuestro tráfico de emails y estamos autorizados a enviarlo'".

Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

Seguridad y concienciación sobre el email

En materia de seguridad del email, lo que los destinatarios no saben puede *definitivamente perjudicarles*. Una plantilla bien educada y suscriptores con conocimiento sobre el tema tienen muchas más posibilidades de cazar al vuelo a los spammers y estafadores en lugar de cometer un error grave.

Dan Ross, de Mailgun, dice que un **programa de concienciación de los empleados es vital para la seguridad del email**. No olvides lo prevalentes que se han vuelto el phishing dirigido y los ataques por correo empresarial. Estos ataques se dirigen a los empleados dentro de tu organización. Lo ideal sería que, anualmente y con todos los nuevos empleados, se llevasen a cabo acciones de capacitación y las pruebas pertinentes.

A lo largo del año, también puedes poner a prueba los resultados de dicha capacitación enviando tus propios emails de "phishing" a tus empleados a modo de prueba (algo así como "falsificar emails falsos"). Esto te ayudará a evaluar el grado de concienciación de tu plantilla, a la vez que mantiene a los empleados en alerta máxima y te da la oportunidad de recordar a todo el mundo lo que se debe tener en cuenta ante un intento de phishing.

"En Mailgun, enviamos periódicamente pruebas de phishing, y si alguien hace clic en una, tenemos una charla con el empleado correspondiente para explicarle por qué ha de ser más cuidadoso. Hacemos un seguimiento de estas métricas y hacemos todo lo posible para que nuestros empleados estén al tanto del phishing".

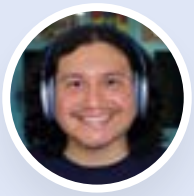
Dan Ross, mánager sénior de GRC, Mailgun

Parafraseando un dicho común... el eslabón más débil es el que define la fortaleza de tu empresa en materia de seguridad del email. Y en casi todas las organizaciones, el eslabón más débil es un ser humano, no la tecnología.

El informe de Mimecast, State of Email Security 2022, afirma que **los empleados con capacitación sobre concienciación cibernética tienen cinco veces más probabilidades de detectar y evitar hacer clic en enlaces maliciosos**. Sin embargo, aunque casi todas las organizaciones encuestadas tienen algún tipo de capacitación, solo el 34 % la ofrece de forma regular. Todo esto a pesar de que cuatro de cada diez encuestados citaron la ingenuidad de los empleados como un grave problema para la seguridad del email en 2022.

La concienciación de los clientes y suscriptores también es importante. Si tu empresa es susceptible a ataques de phishing y suplantación de identidad, o si descubres emails fraudulentos que hacen uso indebido de tu marca, sé proactivo al respecto. No esperes a que haya víctimas. Infórmales y adviérteles sobre estas artimañas. Deja claro qué tipo de información nunca vas a solicitar por email.

Lamentablemente, la mayoría de empresas no piensan en informar a sus clientes sobre los riesgos de suplantación de marca hasta que comienzan a tener mala prensa. Aun así, Jonathan Torres nos explica que un incidente de suplantación de marca es una oportunidad para ser transparente y recuperar la confianza en tu marca.



"Lo último que quieres es que tu empresa sea nombrada en un email que parece legítimo, pero que pone al destinatario en una situación incómoda. Creo que eso es algo de lo que los remitentes suelen darse cuenta cuando ya es demasiado tarde. Y entonces tienen que dar marcha atrás. Por lo tanto, si has sido víctima de un ataque por suplantación de marca, sé transparente. La comunicación es clave. Explica a la gente lo que pasó y lo que estás haciendo para poner las cosas en orden y evitar que vuelva a suceder".

Jonathan Torres, mánager del equipo de TAM, Mailgun

Pero veamos: ¿cómo puedes "poner las cosas en orden", como dice Jonathan? Si tus credenciales se filtran accidentalmente y alguien empieza a enviar correo no deseado desde tu cuenta, es probable que Mailgun lo sepa antes que tú, y nosotros mismos lo detendremos. Mailgun también ayuda a los remitentes a restringir el acceso a las claves de API y a las credenciales SMTP, permitiéndote asignar roles de usuario dentro de la plataforma.

Independientemente de la plataforma de envío de emails que utilices, te recomendamos que restablezcas las claves de API y las contraseñas SMTP de inmediato, así como que verifiques si tu dominio de envío se ha bloqueado debido a la fuga. Configurar la autenticación de dos factores (2FA) también ayudará a evitar que el problema se repita.

Pero, ¿hay algo más que los remitentes puedan hacer para luchar contra la suplantación de marcas? Sí, lo hay. **Se trata de la autenticación del email** y vamos a abordar este tema tan importante a continuación.

PARTE 5

Autenticación: la última línea de defensa

El momento de la verdad en la transmisión del correo electrónico se produce cuando un proveedor de servicios de email como Gmail o Outlook debe decidir cómo filtrar un mensaje. ¿El remitente de este email es realmente quien afirma ser? ¿Es correo no deseado? ¿Es peligroso? ¿Debemos bloquear este mensaje, enviarlo a la carpeta de correo no deseado o entregarlo en la bandeja de entrada?

Como Kate Nowrouzi mencionó anteriormente en esta guía, no siempre es fácil responder esas preguntas, incluso si eres un especialista antispam. Por esa razón la industria del email desarrolló **protocolos de autenticación de emails** y otras especificaciones técnicas para pedir esencialmente la identificación de un remitente antes de permitir que sus mensajes lleguen a la bandeja de entrada del destinatario.

Para cada protocolo o especificación, hay un registro TXT de DNS que se debe agregar y formatear correctamente en los servidores de nombres de dominio. Echemos un vistazo a cuatro áreas clave en la autenticación del email, incluyendo cómo dichas áreas ayudan, cómo funcionan y cómo trabajan juntas.

1. Marco de directivas de remitente (SPF)

El marco de directivas de remitente (SPF) es un protocolo que enumera las direcciones IP de los servidores de email y los nombres de dominio que están autorizados a enviar correo en tu nombre. El registro SPF actúa como un portero en un club nocturno. Si no estás en la lista, no puedes pasar.

Por ejemplo, si envías emails transaccionales a través de Mailgun, usas un ESP diferente para los emails de marketing y utilizas Google Workspace para los emails internos, los tres deben estar identificados en tu registro SPF. De este modo, si los proveedores de servicios de email observan que el correo procede de un remitente no autorizado, pueden optar por bloquear esos mensajes o enviarlos a la carpeta de correo no deseado.

Los detalles técnicos

Este es un ejemplo de registro DNS de SPF:

```
v=spf1
ip4:61.949.100.188 ip6:98.422.200.766 a:smtp.ejemplo.com -all
```

A continuación se muestra un desglose del ejemplo de registro TXT de DNS para SPF anterior:

La versión de SPF utilizada:

Esto siempre debe ser "`v=spf1`" (la primera versión) porque todas las demás versiones están obsoletas.

La lista de remitentes autorizados:

Se debe incluir cualquier dominio que envíe correos en tu nombre utilizando mecanismos como direcciones IP, nombres de host o registros "`a`". Puedes optar por utilizar para todos mecanismos del mismo tipo o combinarlos.

Hay varios mecanismos diferentes entre los que elegir:

1. El mecanismo `ip4` o `ip6` enumera las direcciones IP exactas autorizadas para enviar en tu nombre.
2. El **mecanismo** "`a`" permite al servidor entrante hacer referencia a los registros "`a`" de un dominio, en lugar de usar una IP específica. Siempre que la IP desde donde se origina el email se encuentre entre los registros "`a`", el email pasará la autenticación SPF.
3. El mecanismo `MX` indica las direcciones IP que utiliza tu dominio para recibir correo; si se envía un email desde una de esas direcciones IP, el servidor de correo entrante debe aceptarlo.
4. El mecanismo "`include`" también se utiliza para incluir el registro SPF del dominio en cuestión. Esto es lo que Mailgun utiliza como medio para que los clientes agreguen todas las IP de Mailgun a su SPF.

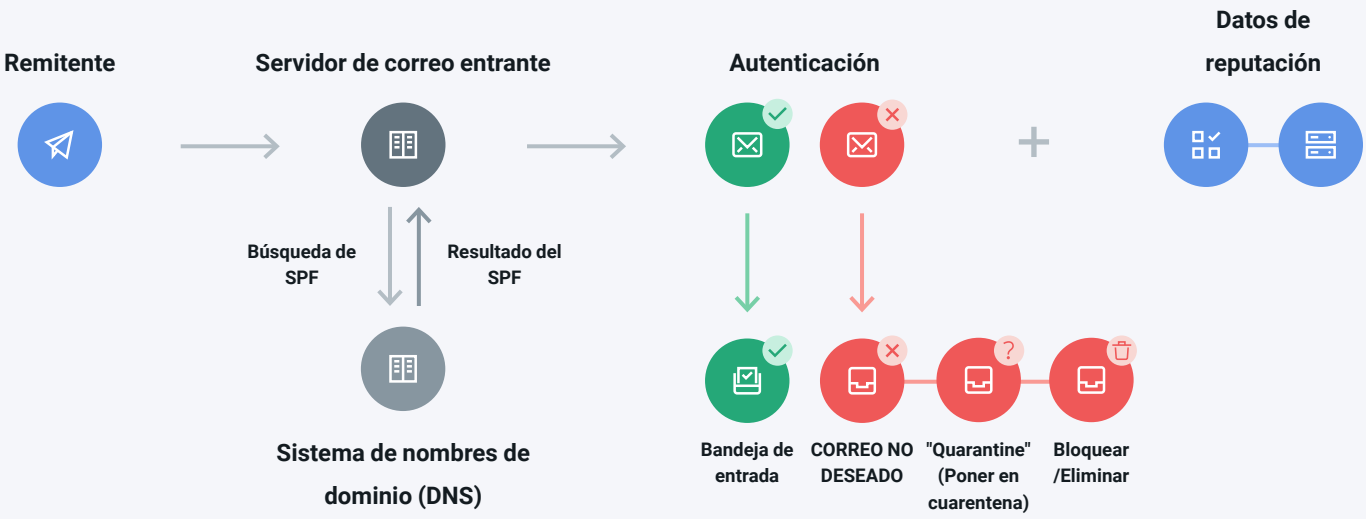
El mecanismo "all" (todo) o calificador de fallo:

Al final de cada registro SPF se encuentra un mecanismo "all". Informa a los servidores de correo entrante sobre qué hacer si un mensaje falla en la autenticación.

- `-all`: Si no se encuentra una coincidencia exacta, el email ha fallado. El mensaje se bloqueará y no llegará a la bandeja de entrada. Esta es la mejor manera de usar SPF para detener la suplantación de identidad.
- `~all`: Si no se encuentra una coincidencia exacta, el email falla pero aun así se entregará. Sin embargo, se marca como sospechoso y probablemente irá a la carpeta de correo no deseado.
- `+all`: Esta opción permite que cualquier servidor envíe desde tu dominio. Rara vez debería usarse porque todo pasará la autenticación SPF. Eso significa que cualquiera podría suplantarte como remitente.
- `?all`: Esta es una configuración neutral. Los mensajes no pasan o fallan la autenticación SPF si la IP no está en la lista. Deja la decisión en manos del proveedor de servicios de email.

> ***Ten en cuenta que un dominio sólo puede tener un registro SPF:*** *Tener varios registros SPF en un dominio hará que los mensajes fallen la autenticación. Aunque los proveedores de buzones de email no siempre toman medidas ante los fallos de SPF, es una parte importante de la conformidad con DMARC, algo que exploraremos más adelante*

Cómo funciona la autenticación SPF



Cuando los proveedores de servicios de email utilizan la autenticación SPF, el servidor de correo entrante comprueba la ruta de devolución en el encabezado del email. A continuación, verifica que el correo electrónico se haya originado en una de las direcciones IP enumeradas en el registro TXT de DNS.

Si el servidor de correo entrante verifica el remitente, se entregará el email a la bandeja de entrada. Si el remitente no se encuentra, el correo se bloqueará o se enviará a la carpeta de correo no deseado, dependiendo de cómo se defina el calificador de fallo (mecanismo `all`).

El SPF tiene un par de inconvenientes. Por un lado, no funciona cuando se reenvía un email. Esto se debe a que en ese caso se realiza el envío desde una IP que no figura en el registro. **El SPF también está limitado a 10 mecanismos (o IP aprobadas)**, lo que puede que no sea suficiente para organizaciones de gran tamaño y remitentes que envíen un gran volumen de correos con muchas personas o equipos enviando en nombre del dominio principal.

2. Autenticación de mensajes, informes y conformidad basada en dominios (DKIM)

DomainKey Identified Mail (DKIM, autenticación de mensajes, informes y conformidad basada en dominios) es un protocolo de autenticación que combina dos métodos diseñados para evitar la falsificación de emails: "DomainKeys" de Yahoo e "Identified Internet Mail" de Cisco.

Al igual que con SPF, la autenticación DKIM implica un registro TXT de DNS que los servidores de correo entrante consultarán para verificar la autenticidad de un remitente, pero es un poco más avanzado. DKIM también ayuda a determinar si un mensaje se modificó en tránsito. Hoy en día, todos los principales proveedores de servicios de email revisan los correos electrónicos en busca del DKIM.

Como su nombre en inglés sugiere, DKIM implica el uso de claves cifradas, también conocidas como firmas digitales. La clave secreta se agrega a un encabezado del email para asociar el mensaje con un determinado dominio y verificar el remitente. La clave DKIM cifrada se empareja con una clave pública que se encuentra en el registro TXT de DNS.

Los detalles técnicos

Este es un ejemplo de registro DKIM de DNS:

```
dk1024-2012._domainkey.ejemplo.com TXT "v=DKIM1; t=y; k=rsa;
p=MIGfMA0GCSqGSiuTHjQWercnvEr54A2CA;"
```

Aquí hay un desglose del registro TXT de DNS de muestra para una firma DKIM:

- `v=` La versión del protocolo utilizada
- `t=` Esta etiqueta opcional indica que el dominio de envío está *probando* DKIM
- `k=` El tipo de clave, que suele ser RSA
- `p=` La clave pública, que se empareja con la firma DKIM cifrada
- La única etiqueta obligatoria en el registro DNS es la clave pública (`p=`). El registro DKIM también incluye el dominio de envío y el selector, este último siendo un nombre o número que el remitente utiliza para indicar a los servidores de email receptores dónde encontrar la clave pública. **El encabezado de firma DKIM** se agrega a los mensajes de email e incluye la información que los servidores receptores necesitan para verificar la autenticidad de un mensaje.

Este es un ejemplo de un encabezado DKIM:

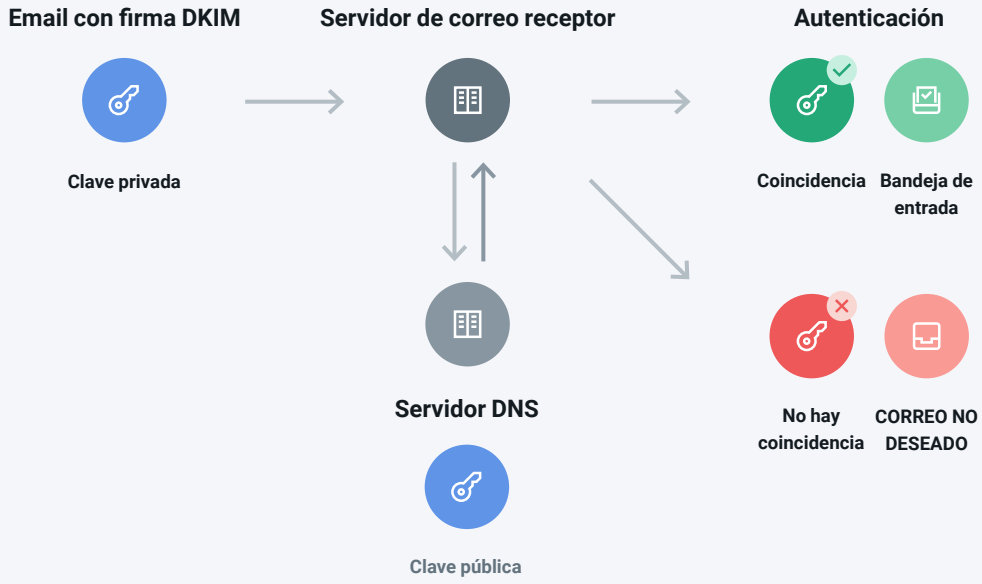
```
DKIM-Signature v=1; a=rsa-sha256; q=dns;
d=ejemplo.com;
s= dk1024-2012; t=1117574938; x=1118006938;
h=Content-Type: Mime Version: Subject: From: To: Sender; Date: List-
Unsubscribe
bh=PV3AoaeTApQYJwe3qgbuUFFTVhjwhv1q2gGNBL+KHU=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

A continuación vemos un desglose de las etiquetas que se encuentran en el ejemplo anterior de información de encabezado DKIM:

- `v=` La versión de DKIM
- `a=` El algoritmo de firma
- `q=` El método de consulta por defecto
- `d=` El dominio de firma asociado a un registro selector para localizar una clave pública
- `s=` El selector, que se utiliza para buscar la clave pública y permite múltiples claves en un dominio
- `t=` La marca de tiempo de la firma
- `x=` El tiempo de caducidad
- `h=` La lista de encabezados que se utilizarán en el algoritmo de firma
- `bh=` El hash el cuerpo después de ser canonizado en Base64, lo que convierte el código binario en texto
- `b=` La firma DKIM real de los encabezados y el cuerpo, que está codificada con Base64

También hay algunas etiquetas DKIM opcionales que se pueden añadir a la información del encabezado. Algunas etiquetas del encabezado DKIM son obligatorias: `v`, `a`, `d`, `s`, `h`, `bh` y `b`. Otras, como `t` y `x`, son opcionales pero recomendables.

Cómo funciona la autenticación DKIM



Una firma DKIM permite a los proveedores de servicios de email y a los agentes de transferencia de correo (MTA, por sus siglas en inglés) saber de dónde extraer la clave pública. Si la clave pública coincide con la firma cifrada, es más probable que los proveedores de servicios de email entreguen el correo en la bandeja de entrada. Si no hay coincidencia, o si no hay ninguna firma DKIM, lo más probable es que el email sea rechazado o enviado a la carpeta de correo no deseado.

El DKIM en sí mismo no filtra los emails. Sin embargo, ayuda a los servidores de correo a decidir cómo filtrar mejor los mensajes entrantes. Una verificación DKIM exitosa a menudo significa una puntuación de correo no deseado reducida para un mensaje.

3. Informes de autenticación de mensajes de dominio (DMARC)

Estrictamente hablando, el sistema de informes de autenticación de mensajes de dominio (DMARC) no es un protocolo de autenticación. Es una especificación técnica que define una directiva para la autenticación del correo electrónico. DMARC ayuda a los remitentes y a los proveedores de servicios de email a sacar el máximo provecho de SPF y DKIM, a la vez que proporciona informes que permiten conocer quién intenta enviar desde tu dominio.

El objetivo principal de una directiva DMARC es verificar la conformidad con SPF y DKIM, y se considera la forma más eficaz de evitar que los agentes malintencionados suplanten a tu marca por email. Cuando se implementa DMARC, los proveedores de buzones de correo comprueban tanto SPF como DKIM y luego se remiten a la directiva que el remitente defina en el registro DMARC de DNS.

Las opciones para la directiva DMARC son:

- **Rechazar:** los mensajes que fallen en DMARC no se entregarán (`p=reject`).
- **Cuarentena:** los mensajes que fallen en DMARC se filtrarán y enviarán a la carpeta de correo no deseado (`p=quarantine`).
- **Ninguno:** Permite que los mensajes pasen independientemente de si aprueban o fallan la comprobación. Solo se utiliza para informes o durante la configuración y las pruebas de DMARC (`p=none`).

Los detalles técnicos

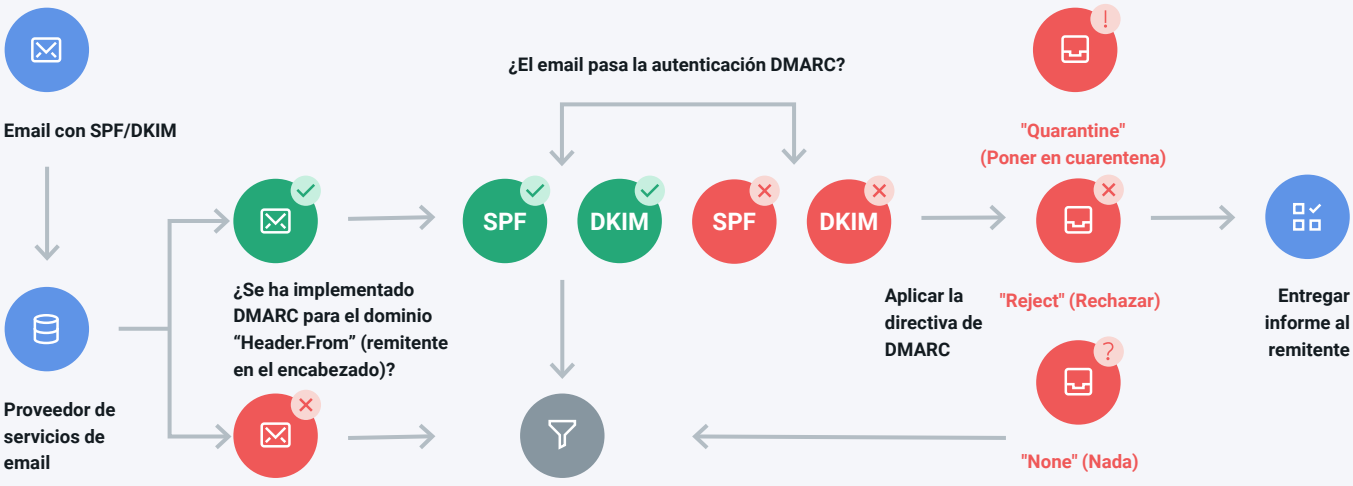
```
1  v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@ejemplo.
   com; pct=100; aspf=s; adkim=s
```

Los registros DMARC pueden ser más sencillos o más complicados, dependiendo de cuántas etiquetas decida utilizar un remitente. Aquí hay una lista completa de las posibles etiquetas DMARC con sus explicaciones correspondientes:

- `v=` La versión de DMARC utilizada.
- `p=` La directiva a aplicar de DMARC: ninguna (none), cuarentena (quarantine) o rechazar (reject).
- `rua=` Una lista de direcciones de email a las que se envían los informes globales de DMARC.
- `pct=` El porcentaje de mensajes que están sujetos a la directiva a aplicar. Por defecto es pct=100.
- `aspf=` Define el modo de conformidad con SPF, que puede ser estricto o relajado con los escenarios de aprobación/fallo.
- `adkim=` Define el modo de conformidad con DKIM, que puede ser estricto o relajado con los escenarios de aprobación/fallo.
- `sp=` Representa diferentes directivas a aplicar para los subdominios.
- `ruf=` Enumera las direcciones de email para el envío de informes forenses/de fallos de DMARC, que son más detallados que los informes globales.
- `fo=` Indica las opciones para crear un informe forense/de fallo de DMARC.
- `rf=` Declara el formato de informe forense para los informes de fallos específicos de los mensajes.
- `ri=` Establece el intervalo de envío de los informes DMARC, que se define en segundos pero suele ser de 24 horas o más.

En nuestro ejemplo de registro TXT de DNS, el remitente tiene una directiva DMARC establecida en "cuarentena" sin diferencia para ningún subdominio. Hay una dirección de email para recibir informes globales. El 100 % de los mensajes están sujetos a la directiva de DMARC, y los modos de conformidad con SPF y DKIM están configurados como "estrictos". Cuando se establecen como "estricto", si uno solo entre SPF o DKIM falla la autenticación, la comprobación DMARC completa falla.

Cómo funciona una directiva DMARC



Cuando un remitente ha implementado DMARC, el proveedor de servicios de email comprueba si pasa SPF y DKIM. A continuación, aplica la directiva indicada en el registro DNS y filtra el email en consecuencia. Por último, se entrega un informe al remitente con información sobre el tráfico de email enviado en nombre del dominio y cómo se ha gestionado.

Informes DMARC

Los informes DMARC proporcionan valiosa información estratégica sobre cómo están transitando los mensajes a través del ecosistema de emails, así como con qué frecuencia los agentes malintencionados intentan falsificar emails y hacerse pasar por tu marca. Como habrás notado, hay dos tipos de informes DMARC: globales y forenses.

Los informes DMARC globales se envían diariamente, a menos que se especifique lo contrario. Incluirán:

- Todos los dominios que envían correo usando tu dominio en el campo "De" (remitente).
- La dirección IP de envío de cada dominio en el informe
- Los resultados de la autenticación SPF y DKIM
- Emails en cuarentena (si tu directiva es `p=quarantine`)
- Emails bloqueados (si usaste `p=reject`)
- Información sobre el tráfico diario de emails

> ***Nota:*** *Probablemente querrás configurar una dirección de email específica para recibir tus informes DMARC. Esto se debe a que se envían emails diarios desde cada ISP que recibe mensajes con tu dominio en el campo "De" (remitente). Estos emails pueden acabar siendo muchos para algunos remitentes.*

Los informes DMARC forenses se envían cada vez que un email falla la autenticación DMARC porque SPF o DKIM no están alineados. También conocidos como **informes de fallo**, estos informes son muy útiles cuando se investigan casos de suplantación de identidad y se necesitan detalles adicionales sobre ciertos mensajes concretos. Por ejemplo, los informes forenses de DMARC incluirán la línea de asunto de los mensajes fallidos, los campos `Para:` y `De:`, así como información sobre los archivos adjuntos y las URL incluidas en esos emails.

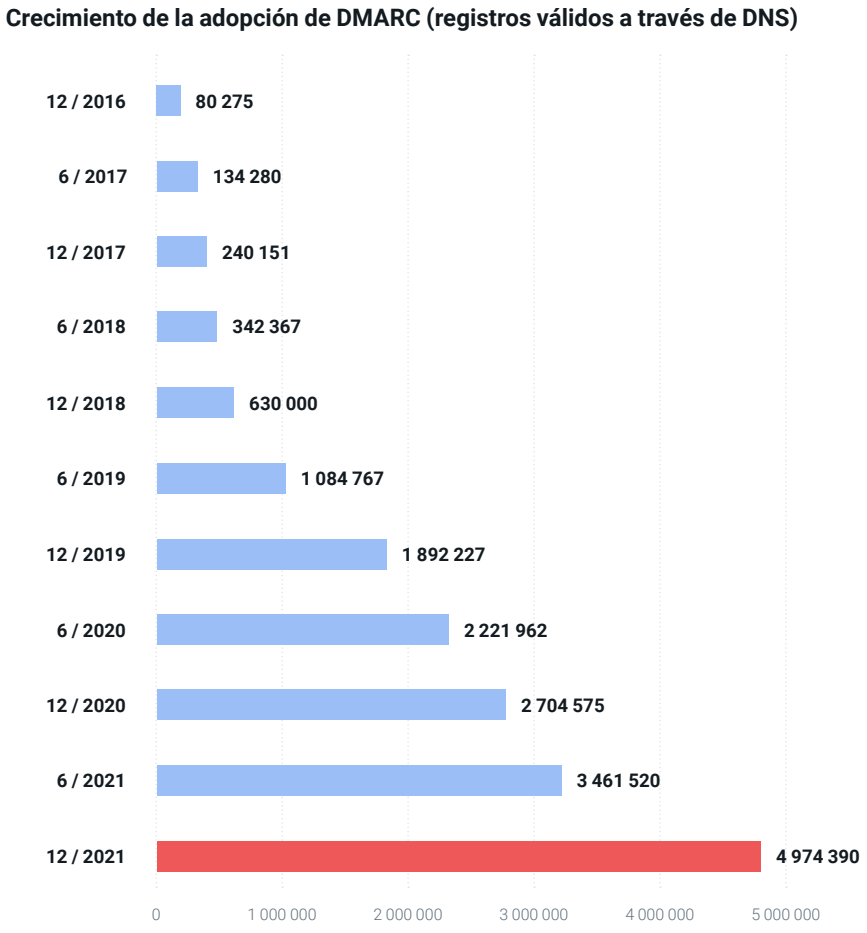
Si tu equipo supervisa la seguridad del email, los informes DMARC son como sesiones informativas periódicas que te ayudan a detectar y detener los problemas antes de que estos se desborden.

"Cuando establecimos por primera vez políticas DMARC para Mailgun, nos pareció muy interesante recibir esos informes y ver todo el tráfico. Empezamos a darnos cuenta de todos estos sitios que usaban Mailgun. com como dominio de envío. Gran parte era realmente tráfico nuestro, pero sencillamente no éramos conscientes de ello. Por ejemplo, nuestro equipo de marketing podía probar un nuevo servicio con los protocolos mal alineados. Pero al menos, con los informes de DMARC podemos ver lo que está sucediendo".

Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

¿Cuál es la mejor directiva DMARC?

Cada vez más remitentes ven el valor que tiene DMARC. Los números recientes de DMARC.org indican que la adopción de la especificación aumentó un 84 % en 2021 con casi 5 millones de registros únicos a final del año.



Sin embargo, DMARC.org también afirma que **cerca de dos tercios de estos registros (65,6 %) han establecido directivas relajadas con p=none**. Esto podría deberse a que algunos remitentes solo quieren ver sus informes DMARC, y dudan en aplicar una política estricta que rechace o ponga en cuarentena mensajes fallidos. Usar una directiva p=none te dará los beneficios de recibir informes, pero no hará absolutamente nada para detener los ataques de phishing y la suplantación de identidad de marca.

Kate Nowrouzi dice que Mailgun anima a sus usuarios a aplicar políticas DMARC más estrictas. Aunque es perfectamente aceptable empezar con una política relajada, en algún momento los remitentes deben dar el siguiente paso para mejorar la seguridad del email.

La etiqueta `pct=` de tu registro DMARC te permite **especificar un porcentaje de mensajes a los que debe aplicarse tu directiva**. Esto significa que puedes evaluar el impacto que una directiva `p=quarantine` o `p=reject` podría tener en la entregabilidad de los correos sin que DMARC afecte a todo tu correo saliente. A continuación, puedes solucionar cualquier problema utilizando los informes DMARC y aumentar gradualmente el porcentaje al que se aplica la directiva.

Kate cree que el objetivo final de DMARC es implementar una directiva que realmente ayude a los proveedores de servicios de email a verificar los remitentes legítimos y que proteja a los destinatarios de los agentes malintencionados que intenten hacerse pasar por tu empresa. Pero primero, los remitentes deben superar su miedo al DMARC.

"Muchas marcas reconocidas y tradicionales todavía consideran que el DMARC es algo nuevo, y tienen sus dudas. Les preocupa, por ejemplo, que si la directiva está configurada como p=reject, sus emails sean bloqueados porque DMARC no está bien configurado. Veo a muchas marcas jactándose de que han implementado DMARC. Pero si su directiva se establece en p=none, es básicamente como no hacer nada".

Kate Nowrouzi, vicepresidenta de Entregabilidad y desarrollo de producto, Mailgun

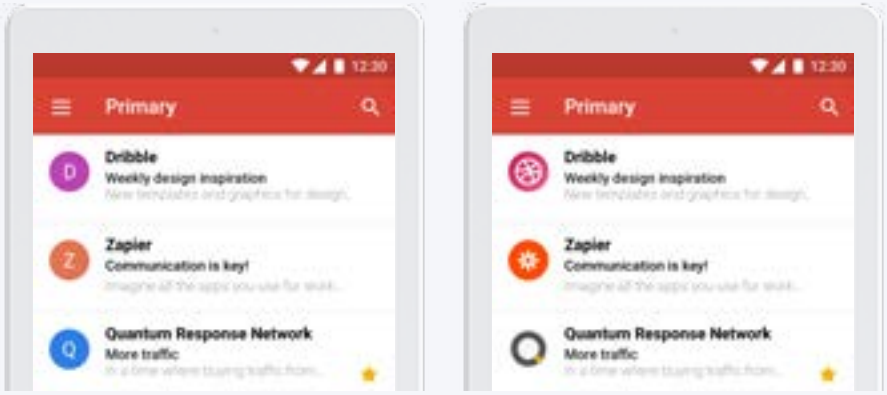
4. Indicadores de marca para la identificación de mensajes (BIMI)

Otra razón por la que algunos remitentes dudan en aplicar una directiva DMARC es que puede parecer que no hay demasiado beneficio para ellos. Es fácil suponer que solo existe la desventaja de que emails legítimos se bloqueen o envíen a la carpeta de correo no deseado debido a una configuración defectuosa de tus registros de autenticación de email.

Para fomentar una adopción más sólida de las directivas DMARC, la industria del email introdujo los indicadores de marca para la identificación de mensajes (BIMI). El resultado de la implementación de BIMI es un logotipo de marca que aparece en la bandeja de entrada y a nivel de mensaje. Pero para estar "listo para BIMI", se debe tener DMARC implementado con una directiva establecida para rechazar o poner en mensajes cuarentena.

Este es un prototipo de cómo se ven los logotipos de BIMI:

Antes de BIMI **Después de BIMI**



Cuando un proveedor de servicios de email recibe un mensaje de tu marca, primero utiliza el registro DMARC para repasar la autenticación SPF y DKIM. Si el mensaje pasa el DMARC, el proveedor de servicios de email puede buscar un registro BIMI de DNS, que es donde se almacena un archivo de imagen SVG con el logotipo de la marca.

Los logotipos de BIMI son algo que interesa y mucho a los profesionales del marketing y cualquier otra persona que se preocupe por la marca. Sin embargo, son los equipos técnicos los que han de configurar los registros BIMI. Y el primer paso es asegurarse de tener todos los demás protocolos de autenticación de emails configurados correctamente, incluida una directiva de DMARC implementada.

Por esa razón, se podría considerar que BIMI es una especie de recompensa para los remitentes que se toman en serio la autenticación de emails. Jonathan Torres, de Mailgun, dice que la industria del email "dio en el clavo" usando BIMI como factor motivador para la implementación de DMARC.

Gmail comenzó a admitir el estándar en 2021, lo que lo convirtió en un incentivo mucho más atractivo aún. Ahora Apple planea introducir compatibilidad con BIMI para su cliente de email, Apple Mail, cuando se lancen las próximas versiones de sus sistemas operativos (se espera que Ventura llegue en octubre de 2022).

Sin embargo, Jonathan también cree que es posible que los proveedores de servicios de email puedan pasar de recompensar a los remitentes con autenticación DMARC a hacer que sea un requisito para asignar mensajes a la bandeja de entrada.

"En algún momento, los proveedores de servicios de email pueden decidir priorizar los mensajes de remitentes que tengan directivas de DMARC establecidas para rechazar o poner en cuarentena, porque esos remitentes los pueden verificar y por lo tanto pueden confiar en ellos. Aún no hemos visto a nadie dar ese paso, pero las bases necesarias para exigir que los remitentes tengan una directiva DMARC establecida en algo además que p=none ya están ahí. Es posible que este sea el paso necesario para lograr una verdadera adopción global".

Jonathan Torres, mánager del equipo de TAM, Mailgun

Autenticación y reputación de emails

Seamos sinceros. Aunque hacer que tu logotipo aparezca en la bandeja de entrada de tus destinatarios es algo que mola, es poco más que un símbolo que hace sentir orgullosos a los directores de marketing y profesionales del email marketing. Existen razones más importantes para centrarse en la autenticación del email: **la reputación como remitente y de la marca**.

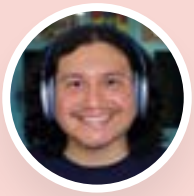
La reputación como remitente es como una calificación de crédito para las organizaciones que envían emails. Básicamente, es una medida de tu fiabilidad y de la calidad de tus comunicaciones por email.

Los proveedores de servicios de email prestan atención a estas cosas y toman notas. Utilizan trampas de spam para encontrar a los remitentes que obtienen contactos de forma sospechosa. Saben con qué frecuencia tus suscriptores abren e interactúan con lo que les envías. Saben si los mensajes son ignorados, eliminados o marcados como correo no deseado. Por eso, **cuanto mejor sea tu reputación como remitente, mejor será la entregabilidad de tus emails**.

Esa es la razón de que Mailgun incluya métricas como las bajas y las quejas por correo no deseado en la política de uso aceptable, y también es por eso que la plataforma incluye herramientas y servicios para supervisar tu reputación como remitente. Queremos remitentes fiables en nuestra plataforma, y queremos ayudar a los usuarios a mejorar su reputación como remitentes de email.

El uso o la ausencia de autenticación de emails también afectará a la reputación y la entregabilidad del remitente. Si utilizas la autenticación de emails correctamente, aumentarás las probabilidades de que tus mensajes se entreguen correctamente. Pero si pasas por alto la autenticación, es menos probable que los proveedores de servicios de email te vean como un remitente fiable. Esa es una de las razones por las que Mailgun exige el uso de DKIM y SPF, a la vez que recomendamos encarecidamente la implementación de DMARC.

Es posible que los equipos técnicos no consideren la **reputación de la marca** parte de sus responsabilidades. De ahí que puedan sentirse algo desconectados de problemas como la suplantación de marca. Sin embargo, si su función está relacionada con la ciberseguridad, una de las principales cosas que estarán protegiendo es la reputación de la marca. No son solo los profesionales de marketing los que se preocupan por la marca.



"Creo que la importancia de proteger la marca de un remitente se está convirtiendo en un tema más acuciante en el área del email debido a la forma en que el sector está cambiando. La marca lo es todo. Si la gente pierde la confianza en tu empresa porque no está segura de si los emails que parecen proceder de tu empresa son seguros o no, eso puede dañar tu reputación de forma permanente".

Jonathan Torres, mánager del equipo de TAM, Mailgun

PARTE 6

Cómo elegir a los socios adecuados

La confianza es, sin duda, un factor crucial en cuestiones de seguridad. Es crucial para todo tipo de relaciones y asociaciones. Del mismo modo que los proveedores de servicios de email necesitan formas de identificar a los remitentes fiables, tú necesitas formas de encontrar proveedores fiables en el área de los servicios de email.

Los expertos en seguridad del email y cumplimiento normativo de Mailgun ofrecieron su perspectiva sobre qué buscar en un socio SaaS que se adhiera a las mejores prácticas.

Auditorías y certificaciones

Tal vez una de las formas más obvias de evaluar a un socio potencial es examinar los estándares a los que se adhieren y las certificaciones que han obtenido. El destino quiso que Dan Ross, director principal de Gobernanza, riesgo y cumplimiento de Mailgun, estuviera pasando por varias auditorías de importancia en ese momento.

Dan tiene una comprensión estratégica de lo que son estas auditorías y certificaciones, y de lo que significan para ti como remitente de emails.

Auditorías SOC 2 Tipo I y II

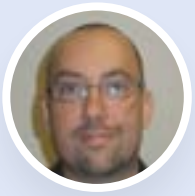
Un informe SOC 2 te proporcionará certeza sobre la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y los controles de privacidad de una organización. Se basa en el cumplimiento de los criterios de servicios de confianza (TSC) del American Institute of Certified Public Accountants (AICPA).

- **La auditoría SOC 2 Tipo I** evalúa el diseño de los procesos de seguridad y examina si los controles de seguridad están en vigor en un momento determinado.
- **La auditoría SOC 2 Tipo II** evalúa cómo de bien funcionan esos controles de seguridad mientras se observan las operaciones a lo largo de un periodo de seis a doce meses.

Por ejemplo, cuando los auditores elaboraron el informe SOC 2 Tipo II sobre Mailgun, evaluaron aspectos como la formación en ciberseguridad de los empleados. Los auditores eligieron a 25 empleados y comprobaron si habían recibido formación y habían aprobado el examen.

Los auditores también examinaron 25 cambios de código diferentes en la plataforma Mailgun para ver si cada uno de esos cambios seguía las mejores prácticas, lo que incluía si Mailgun realizaba un control de calidad (QA) sobre el mismo, y si el nuevo código era revisado para detectar posibles vulnerabilidades de seguridad.

Otro aspecto de SOC 2 Tipo II es la capacidad de agregar controles HIPAA a la auditoría, algo que Mailgun hace. Encontrar un proveedor de servicios de email con un informe SOC 2 Tipo II es relativamente infrecuente. Sin embargo, Dan dice que ese informe es lo que realmente necesitas si te preocupas por encontrar socios que respeten las leyes de protección de la privacidad. Su equipo es acribillado a preguntas por los auditores mientras elaboran el informe completo.



"La auditoría SOC 2 Tipo II audita realmente si los controles de seguridad funcionan de forma eficiente. Cuando Mailgun pasa por una auditoría SOC 2 Tipo II, las jornadas laborales pasan a ser de 12 horas diarias durante un par de semanas. La cosa se pone intensa".

Dan Ross, mánager sénior de GRC, Mailgun

Certificaciones ISO 27001 y 27701

Las normas internacionales (ISO) ayudan a los consumidores y a los compradores B2B a calibrar la calidad y la seguridad de los productos y servicios. ISO 27001 e ISO 27701 son estándares internacionales que evalúan la seguridad de la información y los controles de privacidad.

Si un socio potencial cuenta con la **certificación ISO 27001**, eso demuestra que ha establecido e implementado un sistema de gestión de la seguridad de la información (SGSI), y que lo mantiene y mejora continuamente. Básicamente, la norma certifica que un socio cuenta con los procesos y las políticas adecuadas, y que está mejorando la seguridad de la información año tras año. En una asociación de SaaS, esto significa que la plataforma es cada vez más segura para los clientes y usuarios.

Dan dice que eso incluye factores como un presupuesto y un equipo de seguridad que siguen creciendo anualmente en lugar de reducirse.

Una **certificación ISO 27701** amplía lo cubierto en el estándar ISO 27001 abarcando áreas de control de la privacidad en un sistema de gestión de información de privacidad (PIMS). Este estándar se introdujo en 2019 para ayudar a valorar el cumplimiento de una organización con leyes como el RGPD y la CCPA, evaluando los factores incluidos en estas y otras normativas de privacidad.

Aunque estas dos certificaciones ISO no garantizan que un socio potencial cumpla con la normativa en su totalidad, es una señal sólida de que la organización está haciendo todo lo posible para proteger los datos de los clientes. Y encontrar un socio que cumpla con las leyes sobre emails es importante, porque eso está directamente relacionado con el cumplimiento de tu propia organización.

"No existe una certificación específica sobre el RGPD, porque el RGPD es la ley en sí. No puedes obtener una certificación al respecto, porque la ley está para cumplirla. Pero la forma en que demostramos que la estamos cumpliendo es mediante certificaciones como ISO 27701, que podemos ofrecer a nuestros clientes y demostrar así que realmente estamos haciendo lo que decimos que hacemos".

Dan Ross, mánager sénior de GRC, Mailgun

Otras certificaciones y políticas de seguridad

Más allá de preguntar sobre las principales auditorías y estándares de seguridad, hay otras preguntas que querrás hacerle a tus socios potenciales. Dan dice que puedes incluir cosas como de qué manera administran el acceso a tus datos, cómo responden a las violaciones de seguridad cibernética, cómo realizan copias de seguridad de los datos, o cuestiones sobre redundancia geográfica y recuperación ante desastres.

También puedes hacer preguntas sobre la seguridad de los usuarios, incluidas cosas como el inicio de sesión único (SSO) y la autenticación multifactor (MFA). Puede que tengas dudas específicas sobre la certificación PCI o sobre la seguridad en las oficinas físicas, o tal vez quieras ver un diagrama de la red de sistema. **Un socio de confianza responderá a todas tus preguntas sobre seguridad y te entregará toda la documentación que solicites.**

Obtén todos los detalles sobre la seguridad de Mailgun.

En Mailgun, proporcionamos un portal de seguridad integral que alberga todo tipo de documentación que nuestros clientes y clientes potenciales podrían solicitar.

Protegiendo el producto

Steve Proud es director de Ingeniería de seguridad en Mailgun, lo que significa que está a cargo de proteger nuestra plataforma y mantenerla segura para los remitentes. Dice que los controles que cubrimos en la sección anterior (ISO 27701 y SOC 2 Tipo II) son factores importantes independientemente del tipo de socio tecnológico que evalúes. Eso es porque los ciberdelincuentes son implacables.

> *"Los piratas informáticos atacan constantemente las aplicaciones expuestas a internet. Tanto si se trata de una plataforma de envío de emails como de una red social, las organizaciones deben recurrir a socios que cuenten con un sólido programa de seguridad para asegurarse de que existe una gobernanza y una estructura adecuadas en la forma en que se aplica la seguridad en el personal, los procesos y la tecnología".*
>
> Steve Proud, director de Ingeniería de seguridad, Mailgun

Antes de firmar un contrato con un socio que proporcione servicios de email, obtén detalles sobre cómo protegen ellos su aplicación contra las amenazas de ciberseguridad. El equipo de seguridad de Mailgun aplica una estrategia triple en la protección de nuestra plataforma.

Enfoque "triple amenaza" de seguridad del producto

1. **Pruebas de seguridad internas:** ¿Tiene el socio potencial expertos en seguridad internos que prueban las actualizaciones del producto antes de su implementación final?
2. **Pruebas de penetración externas:** ¿Utiliza el socio potencial un servicio de pruebas de ciberseguridad de terceros que va más allá de las auditorías e informes estándar?
3. **Programas de recompensa "bug bounty":** ¿Se invita a los investigadores de seguridad y a los hackers de sombrero blanco o "buenos" a buscar vulnerabilidades de seguridad desconocidas en la plataforma del socio potencial?

En esta guía, ya has conocido a algunas de las personas involucradas en la seguridad de los productos de Mailgun. Entre estas se encuentra Dan Ross, quien dice que preguntar sobre la "gestión de cambios" es una parte importante de la evaluación de un socio tecnológico potencial. **¿Los equipos de productos y seguridad ponen a prueba el código nuevo para detectar vulnerabilidades antes de pasar el código a producción?** En Mailgun, siempre lo hacemos.

Steve Proud dice que una vigilancia constante es algo necesario en su línea de trabajo, e igualmente importante es que sus socios potenciales tengan un plan para remediar situaciones de seguridad de forma rápida y eficiente.

"Los remitentes de correo electrónico deben considerar cuidadosamente con quién eligen asociarse cuando evalúen herramientas de marketing por email y entregabilidad... La cuestión no es si se descubrirán vulnerabilidades y errores de configuración; la cuestión es cuándo se descubrirán. Y es importante asegurarse de que tus socios cuenten con una metodología que permita tomar medidas rápidamente para crear y poner en marcha código nuevo y más seguro en el entorno, mitigando así el efecto de esa vulnerabilidad".

Steve Proud, director de Ingeniería de seguridad, Mailgun

Seguridad y automatización

Incluso con el mejor y más brillante equipo de seguridad de la información, es difícil mantenerse al día de las tendencias y estar un paso por delante de los agentes malintencionados. Es por eso que un socio sólido también **debería contar con medidas de seguridad automatizadas para poder responder a las amenazas de manera rápida y eficaz**.

Dan Ross explica que, aunque Mailgun cuenta con un equipo de gran talento, todos somos humanos y a veces a los seres humanos se nos escapan cosas que a las máquinas no. Por eso, Dan y sus colegas han trabajado para que "en cuestiones de seguridad no sea necesario pensar". Eso puede sonar algo raro, pero sencillamente significa que existen herramientas automatizadas que alertan al equipo de seguridad casi instantáneamente si surge un problema.

Mailgun utiliza herramientas de seguridad internas que nos permiten supervisar las amenazas en la red y en los puntos de conexión en tiempo real con personal dedicado a investigar cada alerta que se genera. Por ejemplo, si el ordenador de un empleado remoto se comporta de forma extraña, el equipo de seguridad tendrá conocimiento de ello y lo solucionará antes de que el empleado mismo sepa que algo va mal.

Nick Schafer dice que ese tipo de automatización se extiende a lo que ocurre dentro de la aplicación Mailgun, porque queremos asegurarnos de que los emails que salen de nuestra plataforma son seguros y legítimos.

"Si tuviéramos que confiar exclusivamente en acciones humanas y manuales, no daríamos abasto. Aunque pensemos que estamos actuando con diligencia y rapidez, podrían estar saliendo miles de mensajes potencialmente dañinos. Por lo tanto, contamos con todo tipo de alertas y automatizaciones que nos envían notificaciones y nos ayudan a evitar que se perpetren actividades maliciosas".

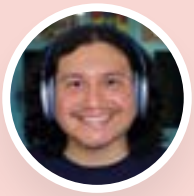
Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

Educación del cliente

Por último, un buen socio en materia de seguridad del email compartirá sus conocimientos y experiencia contigo. Como hemos visto, las amenazas de ciberseguridad están en constante evolución y el email está en el centro de la acción. Por lo tanto, un proveedor de soluciones de email que te mantenga a ti y a tu organización al día es algo muy valioso.

En Mailgun, llevamos a cabo una gran cantidad de formación para asegurar que nuestros clientes no están haciendo accidentalmente algo que vaya en contra de las mejores prácticas o que, potencialmente, viole las leyes.

Jonathan Torres explica que lo hacemos de forma proactiva, asegurándonos de que los problemas de seguridad del email se abordan durante la bienvenida e introducción, así como con el gestor de cuentas (TAM) del cliente de forma continua.



"No todos los proveedores sacan a colación los temas de seguridad y cumplimiento de las normativas. Nosotros queremos hablar con los clientes sobre estos problemas, y estamos más que dispuestos a asesorarlos sobre las mejores prácticas, incluso cuando un problema no esté directamente conectado con nuestro producto".

Jonathan Torres, mánager del equipo de TAM, Mailgun

PARTE 7

Mailgun puede ayudarte

Esperamos haberte convencido de que una plataforma segura para el envío de emails es de extrema importancia. Desde las medidas de seguridad del usuario para detener a los malhechores hasta nuestra estricta adhesión a las normas de cumplimiento, todo eso es el pan nuestro de cada día aquí en Mailgun by Sinch. Llámanos raros si quieres, pero nos encanta lo que hacemos.

"Nuestro equipo tiene una enorme pasión por lo que hacemos, y contamos con una amplísima experiencia. Disfrutamos genuinamente de nuestra labor de mantener a los agentes malintencionados fuera de la plataforma de Mailgun. Es divertido. Es como algo que haría un superhéroe. Me gusta decirles a mis hijos que somos los héroes que protegen la plataforma".

Nick Schafer, mánager de Entregabilidad y cumplimiento, Mailgun

A estas alturas, también deberías entender que contar con un socio que sitúe la seguridad del email y el cumplimiento normativo en lo más alto de su lista de prioridades es un activo valioso para cualquier organización. En Mailgun by Sinch estamos preparados y dispuestos a ser ese socio para ti.

Este es un resumen de cómo nos asociamos con nuestros usuarios en materia de seguridad y cumplimiento del email:

- **Centros de datos seguros:** Los servicios basados en la nube de Mailgun se basan en la infraestructura GCP líder en la industria. Todos nuestros centros de datos están equipados con vigilancia las 24 horas del día y sistemas biométricos de control del acceso.
- **Redundancia, recuperación de datos y copias de seguridad:** Nuestros centros de datos están equipados con al menos redundancia N+1 para las infraestructuras de energía, redes y refrigeración. Dentro de una región, el procesamiento de datos ocurre en al menos tres zonas de disponibilidad distintas. En todas las bases de datos principales se llevan a cabo copias de seguridad diarias de los datos de cuenta con recuperación cifrada incremental/puntual a tu disposición.
- **Cifrado:** Mailgun utiliza cifrado AES-256 en reposo para proteger los datos de los clientes y aplica cifrado TLS opcional para proteger los mensajes enviados desde la plataforma en tránsito.
- **Cumplimiento normativo:** En Mailgun cumplimos o superamos el cumplimiento del RGPD y la CCPA para proteger la privacidad e integridad de los datos de nuestros clientes. Los derechos y responsabilidades para el cumplimiento de la HIPAA se definen en un anexo para socios empresariales. Usamos Stripe, empresa que cumple con PCI, como procesador de pagos.
- **Informes y certificaciones:** Contamos con las certificaciones ISO 27001 y 27701. Mailgun también tiene informes SOC 2 Tipo I y SOC 2 Tipo II, lo que significa que nuestros controles de seguridad se valoran evaluando los factores incluidos en normativas como RGPD, CCPA e HIPAA. Además, todos nuestros proveedores cuentan con certificaciones SOC 2 Tipo II e ISO 27001.
- **Acceso y concienciación de los empleados:** Mailgun limita el acceso a los datos y sistemas en función de las funciones laborales. El acceso administrativo a los sistemas y servicios de Mailgun sigue el principio de mínimo privilegio. Todos los empleados deben someterse a una capacitación anual sobre concienciación cibernética, incluida una evaluación individual anual.
- **Seguridad de las aplicaciones:** SAML y 2FA están disponibles para los inicios de sesión de cliente. Existe un sistema de detección de intrusiones (IDS) para detectar accesos no autorizados a las cuentas. Los cambios en el código del producto se ponen a prueba para detectar vulnerabilidades de seguridad, y un programa externo de recompensas "bug bounty" ayuda a Mailgun a identificar problemas desconocidos.
- **Protección de la plataforma:** Mailgun cuenta con herramientas, sistemas automatizados y empleados dedicados a mantener a los agentes malintencionados lejos de la plataforma y a supervisar nuestra red en busca de actividades sospechosas. Una política de uso aceptable describe lo que esperamos de los usuarios.
- **Autenticación del correo electrónico:** Al usar la plataforma de Mailgun es obligatorio implementar la autenticación SPF y DKIM. Además, recomendamos encarecidamente aplicar una política DMARC.

La seguridad, el cumplimiento y la autenticación del email son problemas complejos. Por ello, Mailgun proporciona gestores de cuentas (TAM) para ayudar durante el proceso de bienvenida e introducción y a lo largo del contrato del cliente. Incluso podemos ayudar con tareas como la implementación de DKIM y SPF. Además, estamos más que dispuestos a hablar de estos temas y a darte consejos de lo más útiles.

"Mantenemos una relación muy estrecha con nuestros clientes, algo que incluye una formación a fondo sobre las mejores prácticas en aspectos como la autenticación del email y el cumplimiento normativo. Luego, cada año nos reunimos con nuestros clientes para volver a educarlos e informar a las nuevas personas que han llegado a bordo. Hacemos todo esto porque realmente nos preocupamos por su éxito como remitentes y por asegurarnos de que conozcan los riesgos".

Kate Nowrouzi, vicepresidenta de Entregabilidad y desarrollo de producto, Mailgun

¿Todavía tienes preguntas? Obtén más información sobre la seguridad y el cumplimiento en Mailgun by Sinch visitando nuestro portal de seguridad dedicado. No dudes en ponerte en contacto con nosotros si tienes preguntas sobre seguridad, cumplimiento normativo o cualquier otra cuestión. Estaremos encantados de explicarte cómo desde Mailgun mantenemos el email de nuestros clientes sano y salvo.

PARTE 8

Recursos

Profundiza en la seguridad, el cumplimiento y la autenticación del email con información detallada, los artículos del blog de Mailgun, los estudios citados en esta guía y otros recursos externos útiles.

Recursos en Mailgun.com

- El portal de seguridad de Mailgun: Consulta o solicita acceso a nuestras políticas, certificaciones e informes. Entre ellos se incluyen los informes ISO 27001, ISO 27701 y SOC 2 Tipo I y II.
- Centro de recursos sobre el GDPR: Descubre cómo Mailgun cumple con la ley sobre la privacidad de los clientes de la Unión Europea.
- Anexo para socios empresariales (BAA) de HIPAA: Obtén información sobre los derechos y las responsabilidades relacionados con la protección de la información sanitaria privada.
- Acuerdo de procesamiento de datos: Obtén detalles sobre cómo Mailgun gestiona los datos de los clientes.
- Política de uso aceptable (AUP): Repasa las directrices exigibles a los usuarios en la plataforma Mailgun.

Contenido útil de Mailgun (en inglés)

- Las mejores prácticas en seguridad del email: Cómo mantener tu programa de email a salvo
- Glosario de estafas por email
- ¿Cómo mantiene Mailgun tus emails protegidos?
- Gestión de la vulnerabilidad: Trabajando con la comunidad para parchear las amenazas a la seguridad
- Conceptos básicos de TLS: ¿Qué es el control de conexión TLS?
- Entender el DKIM: Cómo funciona y por qué es necesario
- Implementación de DMARC: Una guía paso a paso
- ¿Qué puerto SMTP debería usar?
- Emails de phishing: Cómo identificarlos y protegernos
- Estudio de caso: Optimizando la privacidad de los datos para un email escalable y seguro

Recursos de autenticación del email

- Open-SPF.org: Obtén más información sobre el proyecto Sender Policy Framework (marco de directivas de remitente).
- DKIM.org: Obtén más información sobre la autenticación DKIM.
- DMARC.org: Obtén más información sobre DMARC.
- BIMIGroup.org: Obtén más información sobre BIMI.
- El camino hacia la implantación de BIMI: Obtén más información sobre la configuración de BIMI en Email on Acid by Sinch.

Fuentes externas incluidas en esta guía

- IBM: Informe sobre el coste de una filtración de datos en 2021
- Cisco: Tendencias de las amenazas a la seguridad en 2021
- Mimecast: Estado de la seguridad del email en 2022
- Proofpoint: Estado del phishing en 2022
- GreatHorn: Informe de referencia sobre la seguridad del email en 2021

Más de 100 000 empresas de todo el mundo utilizan Mailgun by Sinch para crear experiencias de email integrales para sus clientes mediante una infraestructura de primera clase. Marcas como Vodafone, Etsy, la NHL o McKinsey confían en la tecnología innovadora de Mailgun y en su fiable infraestructura para enviar miles de millones de emails cada año. Creada pensando en los equipos de desarrollo, Mailgun hace que enviar, recibir y realizar el seguimiento de los emails resulte sencillo para remitentes de correo de todos los tamaños.

Mailgun fue fundada en 2010 como respuesta a la falta de servicios pensados para desarrolladores y basados en APIs. Desde entonces, Mailgun se ha unido a **Sinch**, un proveedor líder de plataformas de comunicación como servicio (CPaaS), para convertirse en la solución de email de referencia para desarrolladores de todo el mundo. Al cumplir con el RGPD, la HIPAA y con los SOC I y II, Mailgun aspira a proporcionar el mejor servicio de email posible, poniendo especial atención en la seguridad y la privacidad.

Para más información, visita **mailgun.com/es**.