Publicado en América Latina el 24/09/2024

# [DigiCert y las Nuevas Normativas para Remitentes Masivos que se deben Conocer](http://www.notasdeprensa.es)

## Más de 4.260 millones de usuarios de correo electrónico enfrentan crecientes amenazas de phishing y filtraciones de datos

 Desde su invención en 1965, el correo electrónico ha experimentado una evolución significativa. Según datos de Statista, en 2022 se registraban más de 4.260 millones de usuarios de correo electrónico, con un volumen de correos enviados que alcanzó los 330 mil millones. Se espera que este número crezca un 17,8% para 2026. Sin embargo, el aumento en el uso del correo electrónico ha llevado a una mayor vulnerabilidad, con más de 3,4 mil millones de correos electrónicos de phishing generados diariamente, responsables del 90% de las filtraciones de datos, según Techopedia. Con el objetivo de mejorar la seguridad y combatir los mensajes maliciosos, los principales proveedores de servicios de correo electrónico (ESP, por sus siglas en inglés), han implementado nuevas políticas para los remitentes de correos electrónicos masivos. Dean Coclin, director senior de desarrollo empresarial de DigiCert, explicó: "El objetivo es frustrar la suplantación de dominios y facilitar que los ESP como Google, Yahoo y Microsoft detecten contenido malicioso". Google y Yahoo fueron los primeros ESP importantes en imponer estos nuevos requisitos, que entraron en vigor en febrero de 2024. Microsoft anunció posteriormente sus planes de unirse a esta iniciativa. Para las empresas que dependen del envío de correos electrónicos de marketing a clientes actuales y potenciales, es fundamental entender los nuevos requisitos para los remitentes masivos. ¿Cómo se Define un Remitente Masivo? La definición de remitente masivo varía según el ESP: Google: Considera a los remitentes masivos aquellos que envían más de 5000 mensajes por día a cuentas de Gmail. Estos remitentes deben cumplir con estándares de cumplimiento y autenticación más estrictos. Yahoo: Aplica el término a quienes envían grandes volúmenes de correos electrónicos y se enfoca en asegurar que todos los remitentes masivos implementen una autenticación sólida y opciones fáciles para cancelar la suscripción. Microsoft: Al igual que Yahoo, clasifica a los remitentes masivos como aquellos que envían grandes volúmenes de correos electrónicos, exigiendo el cumplimiento de estrictos protocolos y mejores prácticas de autenticación. Para aquellos que no envían miles de correos electrónicos diarios, los nuevos requisitos para remitentes masivos pueden no ser aplicables. No obstante, si una empresa califica como remitente masivo, deberá cumplir con los requisitos de los ESP para evitar que sus mensajes lleguen a las carpetas de correo no deseado de los destinatarios. Nota Importante: Los ESP pueden clasificar los mensajes como spam, incluso si el dominio no es clasificado como remitente masivo. Intentar evadir la clasificación de remitente masivo no evitará el filtrado de protocolos y contenidos por parte de los ESP. 4 Mejores Prácticas para Evitar Convertirse en Remitente Masivo Cumplir con los requisitos de los ESP implica adoptar medidas que los remitentes masivos ya deberían estar implementando. Las prácticas recomendadas incluyen: Autenticación de Dominio: Siempre Google y Yahoo exigen que los remitentes de correos electrónicos masivos configuren registros de autenticación de correo electrónico para sus dominios de envío. Se recomienda configurar tres protocolos clave: SPF, DKIM y DMARC. Registros SPF: Especifican qué servidores de correo pueden enviar correos electrónicos en nombre de un dominio, ayudando a prevenir la suplantación de dominio. Firmas DKIM: Añaden una firma digital a los mensajes para verificar que provienen del dominio reclamado y que no han sido modificados durante el tránsito. Políticas DMARC: Permiten a los propietarios de dominios especificar cómo deben manejarse los mensajes que no pasan las comprobaciones de SPF o DKIM. Se aconseja comenzar con una política "ninguna" para monitorear el tráfico de correo electrónico y luego avanzar a "cuarentena" o "rechazo" para bloquear correos no autenticados. Facilitar la Cancelación de Suscripción Es fundamental no poner obstáculos para que los usuarios se den de baja de los correos electrónicos de marketing. Implementar una opción de "cancelación de suscripción con un clic" ayuda a mantener una buena reputación y reduce el riesgo de que los correos sean marcados como spam. Evitar el Envío de Spam Los ESP aplican umbrales estrictos para las tasas de spam reportadas. Para cumplir con las normas: Gobernar la Base de Datos de Correos Electrónicos: Supervisar los rebotes permanentes, respetar las preferencias de suscripción y confirmar las suscripciones de usuarios inactivos. Aislar la Infraestructura de Envío: Separar los sistemas de correos electrónicos de marketing de los correos individuales y transaccionales. Enviar Buen Contenido: Asegurarse de que el contenido enviado no sea irrelevante o de bajo valor para los destinatarios. No Olvidar las Mejores Prácticas de DNS para la Seguridad del Correo Electrónico Es esencial que los sistemas de correo electrónico cuenten con registros DNS válidos. Configurar los protocolos SPF, DKIM y DMARC es clave. También es necesario monitorear y auditar periódicamente los registros DNS para detectar cambios no autorizados. El uso de Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) ayudará a proteger contra la suplantación de DNS. Además, se recomienda alojar el DNS con un proveedor confiable que ofrezca protección DDoS y redundancia para garantizar la seguridad y disponibilidad de la infraestructura DNS. Comenzar Ahora Coclin concluye: "Estos movimientos de los principales ESP crean un modelo de responsabilidad compartida entre los remitentes de correos electrónicos y los proveedores de buzones de correo. Si aún no se han tomado medidas para mantener al día el estado de remitente masivo, es fundamental comenzar ahora revisando las estadísticas de los registros de autenticación del dominio utilizando herramientas en línea." Además, sugiere considerar la ampliación del dominio autenticado con un Certificado de Marca Verificada (VMC) DigiCert, que muestra el logotipo de la marca antes de que los destinatarios abran el mensaje. Un VMC actúa como un sello de garantía de que se ha realizado la debida diligencia para configurar SPF, DKIM y DMARC, y representa una medida de marketing que beneficiará a la marca.

**Datos de contacto:**

PR DIGICERT

PR

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/digicert-y-las-nuevas-normativas-para](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Inteligencia Artificial y Robótica Marketing Emprendedores Software Ciberseguridad Dispositivos móviles



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)