

# ■ ■ ■ Por qué hay emails que llegan a SPAM (bandeja de correo no deseado)?

Cómo hacer para que lleguen a INBOX (bandeja de entrada). 10 consejos

---

"Por qué un email llegó a SPAM?" es posiblemente la incógnita más popular en el mundo del mailing, tanto masivo como corporativo empresarial. Y lamentablemente la respuesta no es única, sino que las razones posibles son múltiples. Por eso para controlar esta situación deberá atravesarse una instancia de incorporación de conceptos tanto técnicos como más básicos y operativos de usuario final de aplicaciones de e-mail.

Hay algo que podemos estar seguros: cada vez que un correo llega a la bandeja de SPAM es porque un programa "antispam", el cual contiene múltiples algoritmos de análisis, revisó el mensaje de email y dió un veredicto de tipo "dudoso" que condenó al mensaje a caer en esa carpeta.

Esto implica una noticia no del todo negativa: si el veredicto hubiese sido realmente malo, el correo habría rebotado luego del análisis.

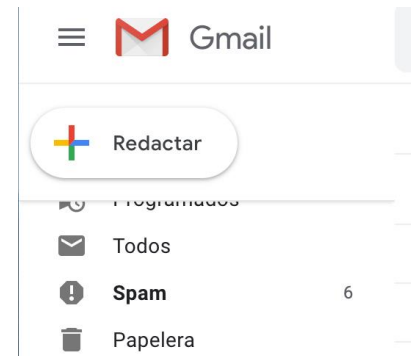
En esta nota proveemos información específica para entender un poco más cómo controlar la operación de emails, buscando el ansiado caso de llegar siempre a **BANDEJA DE ENTRADA**.

Agrupamos esta información en "10 MOTIVOS DE LLEGADA SPAM" y en cada caso, consejos para llegar a BANDEJA DE ENTRADA.

## Cómo trabajan los sistemas Anti-Spam?

Hay distintos tipos de sistemas anti-spam. Hoy en día, los tipos más habituales son:

- **ANTI-SPAMS DE GRAN ENVERGADURA EN SERVICIOS POPULARES**  
Son los utilizados por sistemas populares en la nube, como el de Microsoft para sus dominios de Hotmail, Outlook, Live, Office 365, etc, o el de Google para Gmail, o el de Yahoo.  
Si la idea es investigar estos casos en particular, recomendamos leer la nota [Cómo evitar ser bloqueado por Hotmail, Gmail o Yahoo](#).
- **ANTI-SPAMS CLOUD**  
Son los utilizados en hostings de sitios web, servidores vps y otros servidores en la nube. Hay casos en que el dueño del sitio web y/o el webmaster tiene mayor incidencia en las configuraciones, mientras que en otros casos dependerá del



proveedor del servicio de hosting.

Algunos componentes ejemplo de software para esta finalidad: SpamAssasin, Clamav, Firewalls como CSF o Fail2Ban, etc.

- **ANTI-SPAMS DEL USUARIO FINAL**

Son los configurados por el propio usuario final de email. Ejemplo: Filtros dentro de un webmail, Reglas dentro de Outlook, listas blancas o negras de direcciones de email para pre-autorizar o no autorizar mensajes

- **ANTI-SPAMS DENTRO DE SISTEMAS ANTI-VIRUS**

Hoy en día cualquier solución de anti-virus, sea de pc o de servidor, suele traer incorporada la posibilidad de utilizar un antispam de mensajes de email, como parte de la misma solución. Ejemplo: Avast, AVG, McAfee, Norton, etc

Al indagar en cómo puede trabajar un ANTI-SPAM, se observa que tiene incorporados varios algoritmos de validación, en función a lo que se tenga que analizar del mensaje recibido:

- Dirección de Email origen
- Dominio origen y sus registros DNS asociados: spf, dkim, dmarc, reverso, etc
- IP origen
- Hostname origen
- Asunto
- Formato del mensaje
- Links internos en el texto del mensaje
- Textos internos en el mensaje que correspondan a direcciones de email
- Textos internos en el mensaje que correspondan a dominios
- Historial de cantidad de mensajes previos con ese email origen en la última media hora, hora, día, etc
- Historial de mensajes previos con ese asunto
- Historial de mensajes previos similares hacia el mismo destinatario
- Historial de mensajes previos similares hacia otros destinatarios

Luego de aplicar el análisis y validación, se llega a un veredicto que puede determinar 3 posibilidades:

**APROBADO OK** → Llega a bandeja de Entrada

**REPUTACIÓN DUDOSA** → Llega a bandeja de SPAM, caso que analizaremos en esta nota

**NO APROBADO** → Rebota con bloqueo "duro"

Aclaremos que gran parte del contenido de esta nota es muy técnico, pero si no se mencionaran los temas técnicos, se estaría dejando afuera información fundamental relacionada a los motivos reales que llevan a redireccionar un email hacia la carpeta de SPAM.

---

Cualquiera de los programas, servidores y plataformas de mailing que ofrecemos en **webmatter** permiten revisar toda esta información en detalle, y tener configurado el SMTP origen de acuerdo lo necesario para aprobar estas validaciones recién mencionadas sumando conceptos de control de la reputación de parte de quien realiza los envíos. Consúltenos para así obtener información actualizada sobre nuestros planes:

Chat	Teléfono	WhatsApp
Botón de CHAT ubicado abajo a la izquierda	<b>5411 47982212</b> (lun/vie 10/19 hs)	<b>54911 54594979</b> (lun/vie 10/19 hs)

---

## A CONTINUACIÓN DESARROLLAMOS LOS 10 MOTIVOS MAS HABITUALES

### 1. SMTP ORIGEN con errores, mal configurado

ACLARACIÓN: Este motivo de llegada a Spam es responsabilidad 100% del proveedor de la solución de mail, no es necesario que un usuario final de envíos y campañas se involucre. Para aquel más interesado en cuestiones técnicas y se transforme en nuestro cliente, siempre será bienvenido a aclarar estos conceptos ya que brindamos capacitación inicial a los clientes como parte de los planes de SMTP y mailing en general.

Consideramos alrededor de 20 configuraciones a cumplir aplicadas al dominio. Por ejemplo: registros DNS sincronizados con el servidor, como dkim / spf / dmarc / google-postmaster / reversos de ip / etc.

Todas estas variables técnicas recién mencionadas, podrán ser correctamente mensuradas online en sitios como *MxToolbox* por lo cual, además de la palabra del proveedor, es recomendable revisar estas variables por nuestros propios medios para saber si están

















correctamente configuradas.





Si se trata de mail masivo, es importante configurar el parámetro **List-Unsubscribe** que proporciona el link o email de desuscripción: esto se ha incorporado en los principales servicios de email públicos hoy en día (hotmail,gmail, yahoo, etc). Si este parámetro no se informa, estos servidores aumentarán la desconfianza en el mensaje y posiblemente lo direccionen a la bandeja de SPAM.

Los anti-spams de los servidores de direcciones de mail destino verifican al máximo detalle que estas variables sean configuradas correctamente, ya que sino, ellos suponen que podría tratarse de servidores con sustitución de identidad (phishing), o publicidad excesiva, o virus e intrusión quienes envían los mensajes. Cuando los principales de estos parámetros no son configurados, habría que descartar que se llegará bien a la bandeja de entrada, y con suerte se llegaría a spam en el caso de no rebotar.

### IMPORTANCIA DE TENER TODOS LOS "SEMÁFOROS" EN VERDE

Todos los parámetros de los SMTP que entregamos configurados estarán siempre en perfecto estado, esto es analizable desde sitios externos como *MxToolbox*. Hoy en día es fundamental para la buena llegada de los correos, y la calidad del mail server a través del tiempo transcurrido.

 DKIM Domain Keys Identified Mail	 SPF Sender Policy Framework	 MX Registro MX del dominio	 DMARC Registro DMARC
 DNS Registros DNS del dominio	 BLACKLISTS IPs fuera de listas negras	 PTR Reverso DNS de cada IP	 SOA Start of Authority del dominio
 SMTP AUTH SMTP c/ autenticación	 SSL/TLS Autenticación cifrada opcional	 DOMAIN HEALTH Estado general del dominio	 Not an OPEN RELAY Seguridad/Privacidad del SMTP
 YAHOO FEEDBACK LOOP Seguimiento y	 HOTMAIL SNDS Seguimiento y	 GMAIL POSTMASTER Seguimiento y	 SENDERSCORE.ORG Seguimiento y monitoreo p/reputación

monitoreo p/reputación	monitoreo p/reputación	monitoreo p/reputación	
 LIST- UNSUBSCRIBE Link o Email de desuscripción	 BOUNCES Poca proporción de rebotes	 VOLUMEN Volumen no excesivo en períodos acotados	 ACEPTACION Acciones positivas de confianza de usuarios

**EJEMPLO DE RESULTADOS DE EVALUACIÓN DE MENSAJE DE EMAIL:**

## Mensaje original

ID de mensaje	<dd1229f37019aa77850ad4209330725@psantibaries.com>
Creado a las:	4 de junio de 2021, 17:36 (entregado en 422 segundos)
De:	facturacio...@psantibaries.com.ar
Para:	agru@psantibaries.com
Asunto:	Prueba 1 del 04-06-2021
SPF:	PASS con la IP 200.85.157.124 <a href="#">Más información</a>
DKIM:	'PASS' con el dominio psantibaries.com.ar <a href="#">Más información</a>
DMARC:	'PASS' <a href="#">Más información</a>

[Descargar original](#)

```
Delivered-To: agru@psantibaries.com
Received: by 2002:aa6:c0c6:0:b029:fa:174f:933d with SMTP id o6csp1678891lkp;
  Fri, 4 Jun 2021 13:43:19 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJwuOFLXfoc1qeeW3cMAHsy05LQ6eNAfY4V0lOHE60grUuxOz4aKEj
X-Received: by 2002:ae9:f001:: with SMTP id l1mr6130410qkg.117.1622839399440;
  Fri, 04 Jun 2021 13:43:19 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1622839399; cv=none;
  d=google.com; s=arc-20160816;
  b=oyBqI18279KQf/Jof3eL0TRrgCv0Q6jS7GuZUMP4DH1W15z6AWgL0klGzi15N072f+
  79CnN01RaNhX1DuTXn5nFW3HVp5wRfWJd/8F37A0ua63T9h79mci0NY27I8xw7pnt0SA
```

Normalmente al recibir un mensaje de email y abrir el encabezado, se muestran parte de los resultados de la evaluación realizada por los antispam y controles del servidor de email que recibe. Por ejemplo en GMAIL esta información se obtiene clickeando la opción "Mostrar original" una vez abierto el mensaje. Observar la presencia de los registros de control SPF, DKIM y DMARC. Junto a información básica como el hecho de que el email sea autenticado en el smtp con contraseña, los reversos de ip y reputación en general, esto está entre lo más importante a tener en cuenta del lado del proveedor SMTP.

Esta información puede evaluarse abiertamente en plataformas como **mxtoolbox.com** y **mail-tester.com**

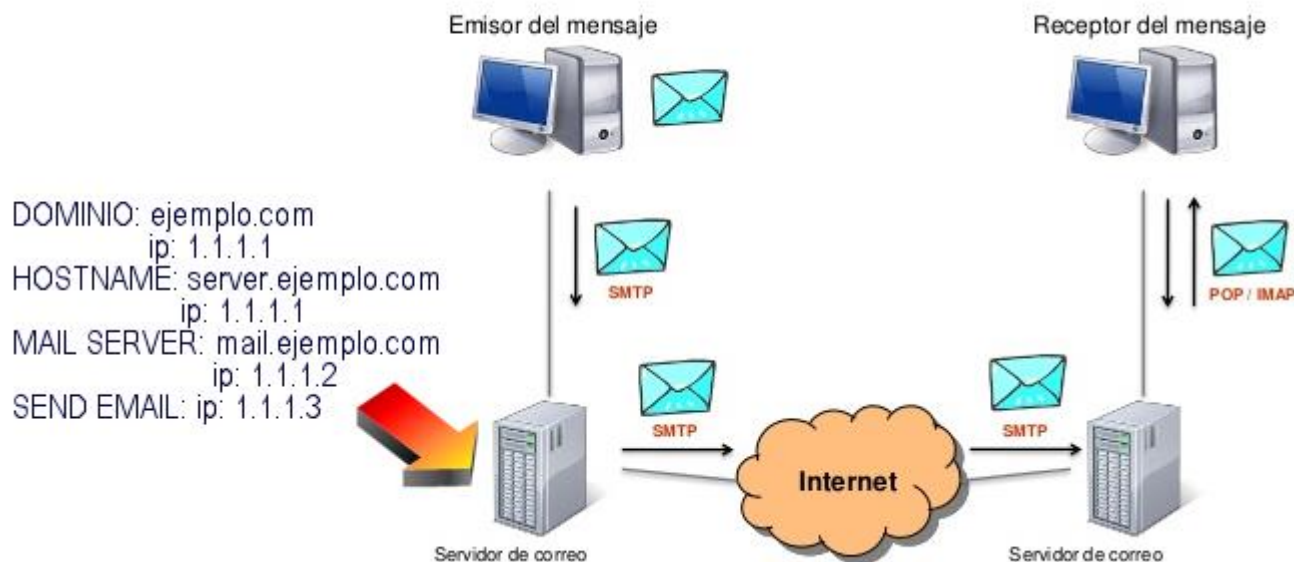
## 2. REPUTACIÓN DE DOMINIO ORIGEN E IPS RELACIONADAS

**ACLARACIÓN:** Este motivo de llegada a Spam también es responsabilidad 100% del proveedor de la solución de mail, no es necesario que un usuario final de envíos y campañas se involucre. Para aquel más interesado en cuestiones técnicas y se transforme en nuestro cliente, siempre será bienvenido a aclarar estos conceptos ya que brindamos capacitación inicial a los clientes como parte de los planes de SMTP y mailing en general.

Este motivo consiste en evaluar no sólo el servidor de mail, por ejemplo *mail.dominio* y su correspondiente dirección IP, sino también la ip que corresponda a sólo el dominio, la cual puede ser o no la misma que la del SMTP. Y también otras cuestiones relacionadas, como la ip del hostname del servidor, la ip de disparo del mensaje, y los reversos de todas ips recién mencionadas.

Para comprender mejor esto, veamos la arquitectura posible al enviar el correo:

### EJEMPLO DE ARQUITECTURA DE ENVÍO DE MENSAJE DE EMAIL:



El dominio "ejemplo.com" podría apuntar a una web en una dirección ip 1.1.1.1 y tener un servidor de mail que sea "mail.ejemplo.com" apuntando a otra ip, por ej 1.1.1.2. Cuando se envíe un email desde @ejemplo.com el anti-spam y mail server destino podría analizar la reputación y la presencia en listas negras de ambas ips y según el resultado de ese análisis,

decidir o no que el email llegue a la bandeja de SPAM o a la de ENTRADA. este mismo análisis se extiende al HOSTNAME del servidor donde esta funcionando el e-mail y a la ip del disparo de email (SEND EMAIL ADDRESS). A su vez en cada ip recién mencionada se analiza el REVERSO DE IP, o sea que no se trate de una ip "fantasma" sino que tenga un nombre válido, relacionado al mismo entorno.

Al igual que se mencionó en el punto 1 de esta nota, parte de esta información también se visualiza en el encabezado del mensaje recibido, lo que asegura que esta información es analizada por el servidor que recibe.

Sumando todo lo recién detallado, el consejo sería revisar 9 datos puntuales:

- el estado de reputación de la **ip del dominio** en listas negras, por ejemplo en *whatismyipaddress.com*
- existencia de Reverso de ip válido de la ip del dominio
- el estado del **nombre de dominio** en Spamhaus DBL
- el estado de reputación de la **ip del servidor de email MX** o sea del servidor smtp que dispara el email
- existencia de Reverso de ip válido de la ip del MX
- el estado de reputación de la **ip de disparo de email (send email address)**, la cual puede ser distinta a la ip del mx, se asocia al SEND puntual de ese mensaje
- existencia de Reverso de ip válido de la ip de disparo del email
- el estado de reputación de la **ip del hostname** donde se encuentra el servidor de email
- existencia de Reverso de ip válido de la ip del hostname del servidor de email

Esta información puede evaluarse abiertamente en plataformas como **mxtoolbox.com** y **mail-tester.com**

### 3. REPUTACIÓN DE DIRECCIÓN DE EMAIL ORIGEN

Si una dirección de email origen ha generado sospechas debido a un historial de muchos mensajes, o de mensajes marcados como spam por los usuarios de un servidor, claramente podría generar una desconfianza que redireccione mensajes hacia la carpeta de SPAM. Cuando esto ocurre la solución más drástica sería el reemplazo de cuenta de email o de dominio origen. Esta misma situación de desvío a spam se da cuando una dirección origen fue marcada como spam previamente por la persona que recibe, e incluida en su lista de direcciones de desconfianza.



#### 4. ALTA CARGA DE MENSAJES IGUALES en tiempo breve (aplicar pausas)

Si hay un parámetro que adquirió relevancia en los últimos tiempos es el de aplicar una PAUSA en segundos entre cada disparo de mail.

Este dato normalmente se configura en la plataforma o programa que se utilice para realizar el envío.

Cuando no se aplican las pausas al disparar, la primera medida que pueden tomar los anti-spam y servidores destino, es volcar el mensaje a la carpeta de SPAM, para luego incluso llegar al punto de aplicar bloqueos temporales o definitivos.

Nuestro consejo respecto a la pausa entre cada disparo es: para servidores grandes como yahoo / gmail / hotmail, establecer una pausa de alrededor de 10 segundos o más. Para otros casos: una pausa de aprox 5 segundos. Si en algún caso se detectara un bloqueo "duro" por antispam y se estaba enviando con pausa de 5 segundos, es recomendable que para ese servidor destino @dominio también se aplique una pausa de alrededor de 10 segundos o más.

En relación a las pausas, muchas veces cuando las pausas son cortas por ejemplo menores a los 5 segundos, los servidores destino aplican bloqueos temporales: no llegan a ser bloqueos "duros", sino que los mails quedan retenidos en la *mail queue* de salida unas horas, hasta que más tarde se observa que el correo sale y llega correctamente a destino. A esto se la podría llamar una dosificación forzada, y es un comportamiento muy habitual en los servidores de yahoo y de gmail.

#### 5. ANTISPAM EXCESIVO EN EL SERVIDOR DESTINO

Cuando del lado del SMTP que dispara el email se han hecho todos los deberes configurando correctamente cada detalle, y además se tiene una buena reputación medible en internet, además de haber cuidado el asunto y contenido del mensaje, no debería existir un motivo para considerar "No deseado" a un correo. Pero así y todo, esto a veces ocurre: se da cuando en el servidor destino el Anti-Spam está configurado excesivamente alto, con reglas imposibles, como por ejemplo: "que de antemano exista la dirección origen de un mensaje en la lista de contactos de quien recibe". Otro motivo excesivo: filtrar mensajes basándose en Blacklists de poca importancia, cuando lo lógico sería basarse sólo en las blacklists mundialmente conocidas y más importantes para tomar de referencia.

Estos casos son los más difíciles, porque sólo se podrá avanzar comunicándose con el destinatario para informarle el caso. A veces se resuelve cuando la persona agrega la dirección de mail origen a sus contactos lista blanca de pre-aprobación. Pero a veces esto no es suficiente, y implicará que la persona se comunique con su proveedor de hosting y/o servidor de mail, para que no apliquen un filtro excesivo sobre ese email origen.

## 6. ASUNTO DEL MENSAJE (medir score)

El asunto del mensaje enviado no debería estar todo en mayúsculas, no debería incluir caracteres como \*\*\*,!!!, palabras como "vendemos", "promoción", etc etc.

Para una mejor lectura en todos los dispositivos como el caso de celulares, sugerimos en el asunto sólo incluir letras mayúsculas, minúsculas y números. En lo posible no incluir ni acentos ni caracteres especiales como comillas.

Los anti-spams, cuando miden el score de un asunto, se fijan en que no sea corto, sino que tenga una longitud de más de 50 caracteres en lo posible. Sugerimos que los asuntos sean detallados, no genéricos.

En tareas de mailing masivo, lo ideal es que los asuntos vayan cambiando para cada destinatario, por ejemplo incluyendo su nombre o dato particular como número de socio o similar.

Desde hace años, los anti-spam aplican un score para el mensaje de e-mail en el cual evalúan estos aspectos. Este score suele ser un número entre 0 y 10 (cuanto más alto, más spam se considera). Normalmente para llegar a bandeja de entrada el resultado de esta evaluación debe dar 5 o menos.

También existe otro tipo de score, el que proporciona **mail-tester.com** el cual evalúa muchísimas variables, y se basa en lo contrario: un 10/10 es lo ideal.

Algunos evaluadores de spam score conocidos en el mercado: **SpamAssasin, Barracuda, MessageLabs, Outlook**, antivirus como **McAfee, Avast, AVG, Norton** y otros

## 7. TEXTOS DEL MENSAJE Y LINKS PRESENTES (medir score)

Respecto al formato y textos del mensaje, es importante asegurarse que si el mensaje se armó con código HTML, sea el html para email ("HTML EMAIL"), el cual es muchísimo más acotado que el html de las páginas web. Este punto es un error recurrente en quienes envían newsletters.

Para perfeccionar el mensaje HTML de email lo máximo posible, sugerimos validarlo y corregirlo ingresando a: <https://www.htmlemailcheck.com/check/>

Entrando en temas del mensaje más relacionados a la posibilidad de ser considerado spam, es importante que cualquier DOMINIO, EMAIL o URL incluido en el mensaje, antes pase por el análisis indicado en el punto 2 de esta nota.

Si por ejemplo se incluye un link hacia una página web con reputación baja, eso perjudicará sistemáticamente a ese envío, haciendo que los mensajes lleguen a bandeja de SPAM o

incluso directamente reboten.

Hay una prueba que siempre sugerimos realizar a nuestros clientes, la cual es muy útil para saber si se da este problema, consiste en los siguientes pasos:

1. Enviarse el mensaje hacia una dirección propia por ejemplo de @gmail.com
2. Una vez que el mensaje llegó, asegurarse que se consideró "deseado". En el caso de que llegue a SPAM, marcarlo como seguro, hasta llegar al punto en que se muestre en la carpeta "Recibidos" o "Prioritarios" si fuera hotmail.com
3. Luego agregar el contacto origen del mensaje en la agenda de CONTACTOS de ese email
4. De ahí en más, cualquier mensaje enviado desde ese email origen hacia ese email destino debería llegar a esa carpeta. En el caso de que el mensaje aparezca en la carpeta SPAM, evaluar si tiene un link adentro del texto que cause ese problema, y volver a probar sin incluirlo para confirmar.

Desde hace años, los anti-spam aplican un score para el mensaje de e-mail en el cual evalúan estos aspectos. Este score suele ser un número entre 0 y 10 (cuanto más alto, más spam se considera). Normalmente para llegar a bandeja de entrada el resultado de esta evaluación debe dar 5 o menos.

También existe otro tipo de score, el que proporciona **mail-tester.com** el cual evalúa muchísimas variables, y se basa en lo contrario: un 10/10 es lo ideal.

Algunos evaluadores de spam score conocidos en el mercado: **SpamAssasin, Barracuda, MessageLabs, Outlook**, antivirus como **McAfee, Avast, AVG, Norton** y otros

## 8. IMÁGENES Y LINKS VÁLIDOS EN MENSAJE (probar siempre antes de enviar)

Los anti-spams suelen medir la validez de los links presentes en un mensaje:

- Las IMÁGENES, que tienen un link interno de origen, deberían poder visualizarse siempre. TIP UTIL: Los nombres de archivo de imágenes crearlos sin espacios en blanco, ya que hay visualizadores de email que sino pueden fallar no reconociendo el archivo, y mostrar una cruz roja con fondo blanco en su lugar
- Es recomendable que el mensaje no sea sólo una imagen, muchos configuran esto como candidato a spam, por eso debería tener al menos un párrafo de TEXTO.
- Los LINKS deben ser vínculos hacia URL válidas, de sitios web online que no presentan error
- Todos los LINKS de URLs de sitios web externos o internos, de imágenes, y de archivos adjuntos como PDFs, deberían ser con SSL (https://), ya que servidores como

gmail desconfían fácilmente cuando el link es no seguro (http://), y probablemente se envíe el mensaje a la carpeta de **spam**

- Como se indicó en el punto anterior, si en el texto se incluyen DOMINIOS, DIRECCIONES DE E-MAIL o LINKS, asegurarse que todos tienen buena reputación antes de enviar

La información de imágenes y validez de links puede evaluarse abiertamente en plataformas como **mail-tester.com** (resultado "Not broken links")

## 9. DENUNCIAS DE DESTINATARIOS (configurar bien vías de desuscripción)

Cuando un mensaje de email masivo es enviado y no presenta un mecanismo simple y rápido de desuscripción, y lo que es peor, cuando una persona llegó a pedir desuscripción pero igual vuelve a recibir un mensaje, se está poniendo en riesgo que la persona realice una denuncia "Reportar como Spam" de su lado, lo que perjudicará muchísimo a la reputación del e-mail y servidor origen. Por eso no nos cansamos de insistir en la necesidad de incluir los 2 mecanismos necesarios:

- LINK DE DESUSCRIPCIÓN DE LA PLATAFORMA: Normalmente se puede configurar indicando la Lista en la cual quedará guardada la dirección desuscripta. Por ejemplo nuestra plataforma de envíos *wmEmails* incluye esta funcionalidad
- LIST-UNSUBSCRIBE: Dirección de e-mail para recibir desuscripciones, mediante la función "Unsubscribe" generalizada, que hoy ya es usada por Yahoo / Gmail / Hotmail entre otros

## 10. CORRESPONDENCIA ENTRE EMAIL SENDER Y CUENTA DE SMTP (muy importante y descuidado)

En tiempos actuales de phishing y sustitución de identidad, es fundamental que cuando se envía un e-mail, la dirección que ve la persona, sea exactamente la misma dirección que se configuró y autenticó en el servidor SMTP. En muchos casos nos pasó que los clientes suelen reemplazar la dirección de sender, la que ve la persona, por otra de otro dominio y servidor, lo cual hoy en día no es para nada recomendable. Cuando esto se realiza, se rompe automáticamente todo lo que se pudo haber logrado aplicando los puntos 1 a 9 de esta nota, creando una desconfianza innecesaria en el servidor de email destino.

Por otro lado, cabe aclarar que la dirección de e-mail que sí se podrá manipular libremente es la llamada **DIRECCION DE RESPUESTA**, que es la que el destinatario verá al clicar "Responder" en su programa de e-mail.

Este punto en particular es un diferencial importante a favor en soluciones como la nuestra, que implica tener un SMTP propio con dominio propio configurado.

---

**Esperamos que esta nota te haya resultado útil!**  
**Para más información detallada, aguardamos tu contacto.**

Cualquiera de los programas, servidores y plataformas de mailing que ofrecemos en **webmatter** permiten revisar toda esta información en detalle, y tener configurado el SMTP origen de acuerdo lo necesario para aprobar estas validaciones recién mencionadas sumando conceptos de control de la reputación de parte de quien realiza los envíos.

Consúltenos para así obtener información actualizada sobre nuestros planes:

#### Chat

Botón de CHAT ubicado  
abajo a la izquierda en  
<https://web-matter.com.ar>

#### Teléfono

**5411 47982212**  
(lun/vie 10/19 hs)

#### WhatsApp

**54911 54594979**  
(lun/vie 10/19 hs)