Cómo enviar mailing masivo sin problemas

10 Tips fundamentales para hacer buenos envíos masivos.

En los últimos años han cambiado mucho los criterios automáticos que adoptan los servidores de mail para aceptar o no los correos que reciben. Por eso se hace fundamental comprender cómo es que hoy funcionan las cosas.

Como proveedor de soluciones de mailing, muchos de nuestros servicios son para mail masivo de alto volúmen.

Por eso podemos asegurar con conocimiento de causa, que en muchos casos, quienes contratan nuestros servicios, vienen inicialmente con una "mentalidad" relacionada a cómo se enviaba correo masivo hace unos años, lo cual marca una gran diferencia respecto a los stándares de hoy en día.

Si tuvieramos que resumir las principales diferencias entre aquellas prácticas y lo que implica el mail masivo hoy, podríamos resumirlo en las siguientes:

PRE-2018

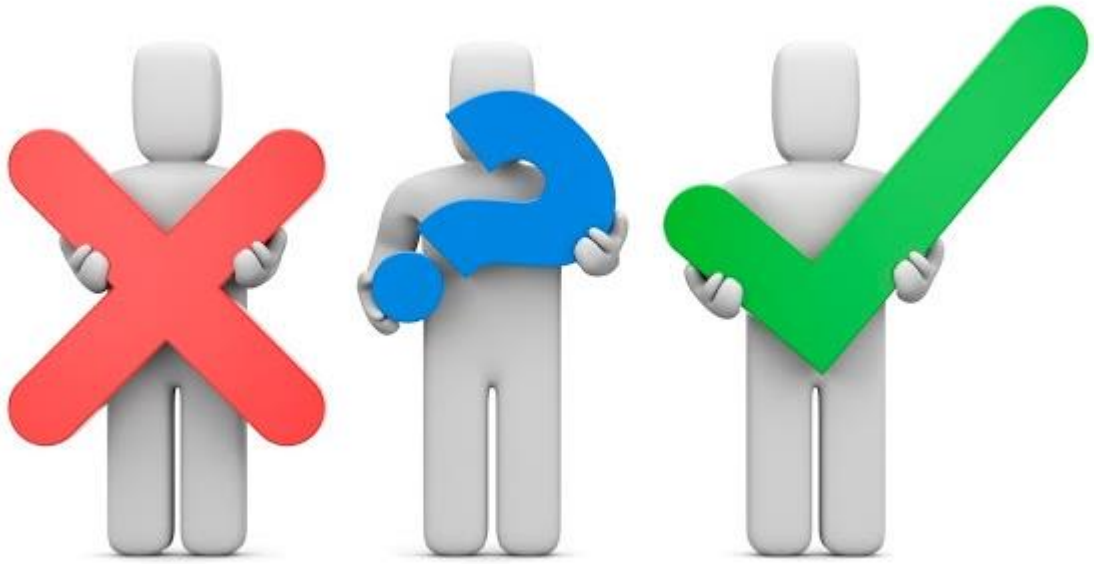
1. Quien enviaba mail masivo de newsletters/e-mail marketing sin control con envíos sin pausa de 5 segundos o más entre mensajes, a pesar de ello podía llegar a tener resultados en sus campañas.
2. Quien enviaba mail masivo de newsletters/e-mail marketing sin control con bases de datos voluminosas sin saber la procedencia, a pesar de ello podía llegar a tener resultados en sus campañas.
3. Quien enviaba mail masivo de newsletters/e-mail marketing sin un DOMINIO Y SERVIDOR SMTP correctamente autenticado y configurado en sus registros DNS, con spf, dkim, dmarc, reverso de DNS, MX correcto, etc, a pesar de ello podía llegar a tener resultados en sus campañas.
4. Antes: Quienes enviaban mail masivo promocional con prácticas hoy inimaginables de aplicarse, buscaban métodos de esquive como dominios volátiles o no existentes, envíos bulk sin smtp, direcciones origen no autenticadas autoreemplazadas, rotación constante de direcciones IPs y anonimato en general.

2018 EN ADELANTE

1. Quien envía mail masivo de newsletters/e-mail marketing sin control con envíos sin pausa de 5 segundos o más entre mensajes, es bloqueado a los pocos minutos por los principales servidores destino.
2. Quien envía mail masivo de newsletters/e-mail marketing sin control con bases de datos voluminosas sin saber la procedencia, es bloqueado a los pocos minutos por los principales

servidores destino debido la prescencia de *spam-traps* y de alto volúmen de correos rebotados.
3. Quien envía mail masivo de newsletters/e-mail marketing sin un DOMINIO Y SERVIDOR SMTP correctamente autenticado y configurado en sus registros DNS, con spf, dkim, dmarc, reverso de DNS, MX correcto, etc, es bloqueado a los pocos minutos por los principales servidores destino.
4. Hoy: Sólo adquirir una buena REPUTACIÓN me permitirá operar a largo plazo llegando correctamente a los servidores destino. Intentar aplicar métodos previos implicaría una importante pérdida de tiempo y dinero.

Para ver nuestras propuestas y servicios actuales de MAILING y SMTP, clickea aquí



Las tareas de mailing hoy en día, para subsistir en el tiempo, deberían ir siempre acompañadas de un buen CONTROL DE REPUTACIÓN. Al inicio, tanto los servidores como dominios arrancan con una reputación neutra (azul), y se deberá ir trabajando día a día para llegar a una REPUTACIÓN POSITIVA, para luego conservarla en el tiempo.

---

10 TIPS PARA UN MAILING MASIVO EXITOSO

1. Acerca de listas y pruebas antes de un envío masivo

Aun hay casos en que se saltean algo tan básico como "ver uno mismo para saber y creer".
Un buen envío masivo hoy debería tener las listas separadas en lotes (no más de 10.000 correos por lote).
Antes de enviar a cada lote de direcciones, es fundamental enviarse el mismo mensaje a una lista propia de PRUEBAS.

Esta lista debería tener al menos 2 direcciones de yahoo, 2 de gmail, 2 de hotmail, algun correo de otro servidor (por ejemplo una casilla de una página web propia), y otra muy importante: una dirección falsa, erronea, que permitirá verificar el funcionamiento de la gestión de correos rebotados: en las pruebas esa dirección errónea debería rebotar, y debería ser visualizada en la gestión de correos rebotados que tenga la herramienta/plataforma que se esté utilizando en ese momento para enviar.

2. El dominio y el servidor SMTP, estan correctamente configurados?

Cuando se asigna un dominio a un servidor SMTP de mail, hay muchas variables técnicas a analizar antes de realizar envíos.

Para el dominio

- Debería asegurarme que esté al día, bajo mi propiedad, con los name servers (servidores de dns) correctos.
- Es recomendable que el dominio tenga una antiguedad de al menos 30 días, ya que hay blacklists como *SEM FRESH* que sino podrían marcar al dominio, creando desconfianza a los servidores destino.
- Los registros DNS del dominio deberían estar correctamente configurados: Registros A, NS, SOA, y TXT (dkim, dmarc, spf y otros)

Para el servidor SMTP

- El proveedor de SMTP debería asegurarme que se trata de un servidor smtp preparado y configurado para mail masivo.
  Los servidores más habituales son, sobre Linux: *Postfix* y *Exim* ; sobre Windows: *MS Exchange* y *MailEnable*.
- La casilla de correo origen a utilizar en el envío debería estar bien configurada en el servidor, con una contraseña de tipo seguro
- El servidor smtp debería tener la opción de conexión con *SSL/TLS* a las cuentas de correo.

Para dominio + servidor SMTP

- Hay muchas configuraciones que involucran al dominio y al servidor SMTP: DKIM, SPF, REVERSO DE DNS (HOSTNAME DEL SERVIDOR), DMARC, VERIFICACION GOOGLE POSTMASTER

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

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 monitoreo p/reputación	HOTMAIL SNDS Seguimiento y monitoreo p/reputación	GMAIL POSTMASTER Seguimiento y monitoreo p/reputación	SENDERSCORE.ORG Seguimiento y monitoreo p/reputación

3. Dosificación: Pausa entre mensajes

Si hay un parámetro que adquirió relavancia 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.
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 algun 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.

4. Cuidado con las *SPAM TRAPS* y las bases de dudosa procedencia

Cuando se adquieren grandes bases de datos sin saber su procedencia, suelen tener adentro direcciones de mail que no corresponden a personas, sino que son direcciones "testigo" de que se estan realizando prácticas de spam. Esto actuará como una auto-denuncia y tanto las principales blacklists como servidores de importancia, pasarán de un momento a otro a bloquear por completo los envíos.
Cuando se envía a grandes bases de datos de procedencia dudosa, otra gran problema que se da, es que el nivel de correos rebotados es muy grande en relación a lo habitual. Por ejemplo si la cantidad de rebotados por direcciones inválidas es mayor al 30% eso tambien suele derivar en bloqueos "duros" generados por los anti-spam de los servidores destino.
Por eso es que no nos cansamos de insistir con la necesidad de contar con datos confiables, además de cuidar mucho la operación de mail masivo.

5. Gestionar día a día los correos rebotados

Cada envío que se realice debería estar acompañado de un estricto control de correos rebotados, esto me permitirá saber con exactitud lo que está ocurriendo al enviar. Lo ideal es que cada lista o lote de direcciones destino, no supere las 10.000, de ese modo, luego de haber enviado a cada lote, hay que acceder a la gestión de correos rebotados, la cual siempre tiene que estar dentro del programa o plataforma de mailing que se utilice.
La gestión de rebotados debería discriminar claramente los e-mails segun motivo de rebote:

- Las direcciones inválidas (dadas de baja, inexistentes) -> en nuestras herramientas se marcan en ROJO. Estas direcciones deberían eliminarse de las listas
- Las direcciones válidas pero que rebotaron x casilla llena -> en nuestras herramientas se marcan en AMARILLO
- Las direcciones en las que no se puede determinar si son válidas, normalmente por caídas temporales del servidor destino -> en nuestras herramientas se marcan en GRIS
- Las direcciones en las que el destinatario ha aplicado un nivel de seguridad alto, y no pudo llegar -> en nuestras herramientas se marcan en NEGRO. Cuando esto sucede en gran escala, deberían informarnos para resolver el problema del lado del servidor, a partir del análisis de reputación, listas negras, etc

6. El Mensaje también importa

Es fundamental que al armar el mensaje de mailing se tengan en cuenta algunos puntos de importancia:

- El asunto no debería estar todo en mayusculas, no debería incluir caracteres como ***,!!!, palabras como "vendemos", "promoción", etc etc
- Para una mejor lectura en todos los dispositivos, sugerimos en el asunto sólo incluir letras mayúsculas, minúsculas y números. En lo posible no incluir ni acentos ni caracteres especiales como comillas
- Siempre será mejor recibido un mensaje que incluye texto, y que no se trata de una única imágen con link
- Asegurarse que cada url, email, dominio, etc incluído en los textos, cuenta con buena reputación en internet. Si un sitio web funciona con https cuidar no ponerlo con http o viceversa

- Asegurarse que la tabla o set de codificación de caracteres según el lenguaje, por ejemplo "iso-8859-1" para español, fue correctamente referenciada en el encabezado.
- Asegurarse que los estilos visuales de los elementos HTML, escritos en CSS, son asignados "in-line" por elemento y no a través de clases referenciadas (*class*).
- Asegurarse que si el mensaje se armó con código HTML, sea el html para email ("HTML EMAIL"), el cual es muchisimo 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 corregrilo ingresando a: *https://www.htmlemailcheck.com/check/*
  Al contratar cualquiera de nuestros planes inicialmente damos mucha ayuda al cliente en estos detalles de programación HTML para que cuente con mensajes "tipo" bien construídos, los cuales servirán de plantilla para mensajes siguientes.

7. Un mecanismo de control interesante

Una vez que ya se tenga todo listo para enviar, y que ya se realizaon las pruebas a direcciones propias, no está de más ingresar a *https://www.mail-tester.com/* y seguir los pasos de pantalla: se generará automáticamente una dirección de envío a la cual tambien enviaré el mensaje a modo de prueba, y tendré una PUNTUACIÓN segun varias cracterísticas: del servidor, del mensaje, del asunto, etc etc

8. Blacklists: En cuáles NO se puede estar?

A continuación informamos aquellas listas negras que consideramos de mayor importancia.
Si tu dominio o ip de servidor se encuentra en alguna de estas listas, implicaría que la reputación está muy baja, y hasta no solucionarlo, no tiene sentido realizar envíos masivos (sería perder el tiempo)

- SORBS SPAM
- SPAMHAUS (de IP)
- SPAMHAUS DBL (de DOMINIO)
- SPAMCOP
- SEM FRESH
- ivmSIP

Cuando alguno de nuestros clientes se ve complicado por un tema de reputación, normalmente se debe esperar 24 hs hasta regularizar el tema de la blacklists asociada al problema deslistando la dirección ip.
En el caso de que se trate de haber caído en la blacklist de dominio SPAMHAUS DBL, el problema es mayor ya que el desliste no es fácil. Por eso insistimos mucho con la necesidad de tener un dominio que constantemente tenga buena salud para utilizarse en envíos.

9. Ganar buena reputación en yahoo / gmail / hotmail

Cuando se empiezan a realizar envíos, una de las primeras cosas que surgen es tomar conciencia del alto control que hoy en día aplican los grandes servidores como yahoo / gmail / hotmail, y lo

fácil que pueden desconfiar al recibir correos con características de newsletters informativos o promocionales.

Qué se puede hacer para mejorar mi reputación en yahoo / hotmail / gmail?

Además de aplicar los puntos de esta nota, para estos 3 servidores en particular, se justifica aplicar algunas acciones adicionales:

1. Al enviar a direcciones propias de yahoo / gmail / hotmail, si el mensaje llegó a la carpeta de "no deseado", marcar el correo como deseado
2. Una vez que fue marcado como "deseado", clickear el link "siempre mostrar imágenes" dentro del mensaje
3. En cada dirección, agregar el contacto origen en la Agenda de Contactos. En el contacto el mail origen es el mail que proviene del servidor smtp contratado. Para cada casilla origen del SMTP, convendría repetir este proceso

Por qué la validación de reputación que realizan GOOGLE con *gmail.com* y MICROSOFT con *hotmail.com/live.com/outlook.com* se ha vuelto especialmente importante?

Actualmente muchas entidades, empresas, instituciones y compañías contratan para sus propios dominios servicios corporativos provistos por Google y Microsoft. Por ejemplo Google G-Suite o Microsoft Office 365. En cada empresa estas plataformas en la nube, utilizan sus propios sistemas de análisis de reputación integrados. En el caso de Microsoft suele utilizar su red de servidores anti-spam ***x.protection.outlook.com***. En el caso de Google, utiliza sus sistemas anti-spam configurados en ***gmail.com***. Por eso hay que tener en cuenta que al probar la reputacion enviando a gmail o a hotmail, hoy en día esa validación puede ser la misma que se efectúe para otros dominios.

10. Lo más importante: criterio que se aplica en los envíos

Cada vez que sumamos un nuevo cliente para operar con nuestros sistemas y servidores, aclaramos que lo más importante será adaptarse a operar mail masivo siguiendo la necesidades actuales de ganar REPUTACIÓN.
Esto implicará sumar tareas, costumbres y tiempos que quizás antes no se contemplaban al enviar mailing.
Al principio, incluso podemos admitir algun error menor debido a que hay personas que pueden tener costumbres similares a cómo se operaba antes de 2018.
Luego habitualmente quien realiza envíos se va adaptando a los nuevos criterios existentes para operar este tipo de plataformas y programas.

Para más información detallada, aguardamos su llamado al (011) 4798-2212 o via WhatsApp al **+54911 54594979**