Cómo evitar ser bloqueado por Hotmail, Gmail o Yahoo?

10 tips para llegar correctamente a la bandeja de entrada

Llegar via mail masivo a los servidores públicos de HOTMAIL (OUTLOOK), GMAIL o YAHOO, desde siempre ha sido un tema complejo de resolver.
En los últimos años, los 3 casos han reforzado sus plataformas de anti-spam, que actuan como "barrera" en la nube, para analizar cada mensaje que llega a cualquier programa, servicio, soporte o plataforma relacionada a cada empresa: Microsoft, Google o Yahoo.
Si bien es bueno aplicar barreras con bloqueo para evitar casos abusivos, la acción de estos anti-spam muchas veces genera dolores de cabeza a aquellos que quieren enviar correos lícitos, de buena fé, en forma masiva hacia estos 3 servidores.
En esta nota proveemos información específica para entender un poco más cómo resolver este problema.

Dividiremos los tips en 2 grupos: 5 tips de naturaleza técnica, los cuales suelen ser responsabilidad del proveedor de tecnología de la solución de mailing, y 5 tips de prácticas de envío, los cuales están dirigidos al usuario final que efectua los envíos.

Cómo actuan los anti-spam de Hotmail, Gmail y Yahoo?

En los últimos aprox 5 años, los antispam en la nube de estas 3 compañías se han transformado en sofisticadas plataformas online, que trabajan siempre "on the fly" analizando, verificando y aprobando o no cada mensaje que intenta llegar a sus servidores.

Antispam de Microsoft: **x.protection.outlook.com** (reemplazar "x" por distintos subdominios posibles)

Antispam de Google: **mx.google.com** y otros

Antispam de Yahoo: **x.yahoodns.net + mail.x.yahoo.com + postmaster.yahoo.com** (reemplazar "x" por distintos subdominios posibles)

Al indagar en cada uno de ellos, se observa que se subdividen en componentes con varios algoritmos de validación, en funcion a lo que se debe analizar del mensaje recibido:

- Dirección de Email origen
- Dominio origen y sus registros DNS asociados: spf, dkim, dmarc, reverso, etc

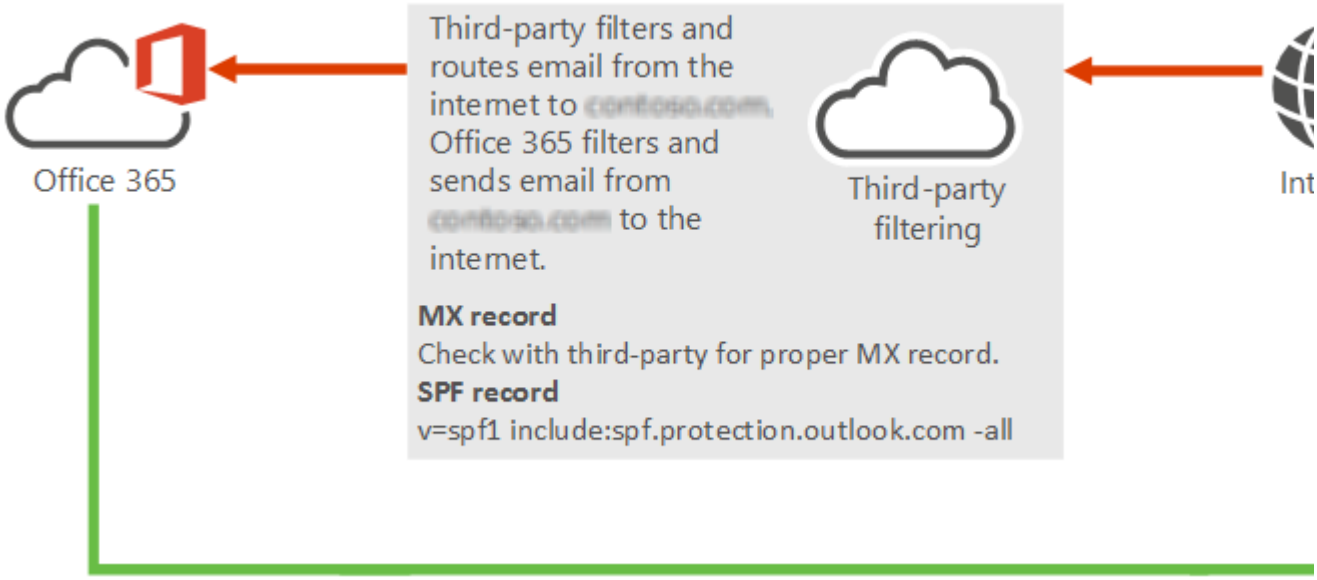
- IP origen
- Hostname origen
- Asunto
- Formato del mensaje
- Links internos en el texto del mensaje
- Textos internos en el mensaje que correspondan a direcciones de email
- Textos internos en el mensaje que correspondan a dominios
- Historial de cantidad de mensajes previos con ese email origen en 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

NO APROBADO → Rebota con bloqueo "duro"



En esta imágen se observa cómo Microsoft solicita a sus clientes con el dominio en Office 365, les indica cómo configurar el anti-spam ***x.protection.outlook.com***. Es el mismo anti-spam que se aplica en los servidores públicos **outlook.com, live.com, hotmail.com, hotmail.com.ar** y otros peretenecientes a Microsoft.

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 recien mencionadas. Consúltenos para así obtener información actualizada sobre nuestros planes:

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

A CONTINUACIÓN DESARROLLAMOS LOS 10 TIPS

TIPS TÉCNICOS

Estan orientados a ser cumplidos por los proveedores de servidores y soluciones de mailing. Cuando el usuario final recibe las credenciales para acceder a un panel, estos puntos ya deberían estar funcionando por parte de quien ofrece la solución.

1. CONFIGURACIONES TÉCNICAS DEL DOMINIO Y ENTORNO SMTP

Consideramos alrededor de 15 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 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.

Los 3 casos de esta nota: HOTMAIL / GMAIL / YAHOO, 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 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.

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

2. GESTIÓN DE CORREOS REBOTADOS

Parte del análisis que realizan estos servidores estará orientado a crear un perfil de REPUTACIÓN de la direccion de mail y dominio origen. Cuando observan que en un mail masivo estan recibiendo muchos mensajes a direcciones que ya no existen allí, eso baja la reputación y termina perfjudicando a los envíos en general. Para ellos es una mala señal el hecho de tener muchas direcciones inválidas de su servidor en la lista, considerando al enviador como un posible caso de spam abusivo.
Por eso 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

3. CONTAR CON INFORMACION DETALLADA DE LA SALIDA DE EMAILS

Además de poder gestionar los correos rebotados, siempre será importante poder revisar la salida de emails en cualquiera de sus fases desde el momento en que es disparado, especialmente una fase que en muchas herramientas no se muestra y se mantiene oculta al usuario final: **LA COLA DE SALIDA DE MENSAJES**, incluída siempre en el MAIL SERVER.
En casos normales, el email no permanece ni una décima de segundo en la cola de salida, pero no siempre es así. Hay varias razones que pueden hacer que un email permanezca en la cola de salida un tiempo (horas, minutos, o hasta incluso días).
Por eso siempre se deberá contar con una buena interfase para poder revisar "en vivo" la cola de salida de mensajes de mail.

Los casos más comunes para que un email permanezca en la cola de salida son:

- Si el envío es abultado en cantidad de destinatarios y las pausas entre mensajes que establece la aplicación que dispara son breves (short delay), esto generará cierta **congestión** en la cola de salida y se mostrará siempre una lista de mails en la cola de salida.
  Lo ideal es que la aplicación que realiza el disparo de mail y el operador también, sepan que no es bueno que se sumen cientos de emails en la cola, ya que representa que la frecuencia de disparo esta siendo más veloz que la recomendable, y eso puede terminar en una acción de bloqueo y desconfianza por parte de los servidores destino

- Si la casilla del destinatario está llena, en algunos casos el email estará **retenido en la cola de salida** unas horas, buscando una nueva oportunidad para probar llegar (reintento)

- La más habitual: Servidores destino como yahoo, hotmail y gmail detectan alto volumen desde la misma dirección origen, y entonces crean bloqueos temporales de 4 u 8 hs, que hacen esperar al mensaje en cola hasta finalmente dejarlo llegar a destino. Esta **dosificación forzada** puede terminar bien, llegando a destino más tarde, o podría terminar mal: rebotando en forma definitiva por anti-spam (rebote "duro")

4. PAUSA ENTRE DISPAROS BIEN CONFIGURADA

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.

5. SOPORTE CON ASISTENCIA AL INSTANTE

Como bien se sabe, cada envío presenta una situación dinámica online, que debería ser siempre monitoreada: por ejemplo supongamos que mientras se está realizando un envío, un virus externo reusa la dirección origen del envío, y causa un caos en internet con envíos fraudulentos reusando dicha dirección. Eso podría repercutir al instante en el envío que se estaba realizando, haciendo caer la reputación y generando rebotes duros por parte de los anti-spam.
La ventaja de contar con un soporte asistido al momento, es que quien envía, ante los primeros correos rebotados o sospecha de virus/fraude, avisa al proveedor, y todo podrá ser detenido a tiempo para restaurar el sistema evitando poner en riesgo su reputación en futuros envíos.
Cuando este tipo de tareas de soporte no se atienden a tiempo, podría ser tarde luego de restaurarse el entorno, ante el nivel de errores acumulados.

TIPS PARA EL USUARIO FINAL

Estan orientados a ser cumplidos por la o las personas que realizarán los envíos. Lo primero será tomar conciencia de lo importante que serán estos puntos para lograr envíos saludables a través del tiempo y llegar correctamente a los 3 servidores mencionados en esta nota. Las prácticas de hoy al enviar implican un tratamiento muy distinto al de hace unos años, ya que antes los anti-spam y sus algoritmos eran muchísimo más débiles, y se podía llegar a destino con mayor facilidad.

6. CRITERIO PARA ARMAR LISTAS

Además de lo mencionado en el TIP 4 (PAUSA ENTRE DISPAROS), la dosificación tambien debería estar al armar las listas. Asumiendo que se trabaja con 1 solo SMTP de salida, sugerimos que cada lista o lote:

- No pase las 10.000 direcciones destino
- No tenga más de 1500 de hotmail
- No tenga más de 1500 de yahoo
- No tenga más de 1500 de gmail
- Validar el formato y ortografía de las direcciones destino antes de enviar

Si alguno de los 3 servidores presenta una proporción mayor, convendría separar el excedente y enviarla al día siguiente, o en tal caso enviarlo con un plan que incluya multi-smtp de salida que nos dará la posibilidad de ampliar el volumen en paralelo.
Al aplicar las pausas, sumadas a este criterio de reparto, se darán las condiciones ideales para evitar inconvenientes en el envío.

7. PAUSA CONFIGURADA POR EL USUARIO

Hay casos en que la pausa entre disparos será configurada por el usuario final. Ejemplos:

- Programas de PC como Sendblaster o GroupMail
- Aplicaciones propias como sistemas de facturación
- Aplicaciones propias en la nube, desarrollos propios

El tema de la pausa deberá ser tenido en cuenta al tratar con el proveedor de SMTP. Por ejemplo en nuestro caso, cuando el parámetro ***pausa*** (delay) no puede ser configurada del lado del aplicativo, simplemente indicándonos que es así podremos configurarla del lado de nuestros Servidores SMTP, para que el envío pueda funcionar como corresponde para la llegada correcta.

Los 3 anti-spam mencionados (el de hotmail, de gmail y de yahoo), cuando reciben muchos mails tipo "ametralladora" en un período corto de tiempo, aplican un BLOQUEO TEMPORAL (temporary deferred). Y luego de la instancia de bloqueo temporal, pasan a la instancia de bloqueo total, como una pared que no deja pasar mensajes. Esto obligará a que al menos con ese servidor se tenga que trabajar de otro modo: aplicando pausas muy espaciadas, como de 15 segundos o más entre disparos. esto podría hacer recobrar la reputación a través de los días siguientes.

8. PREPARACION DE LA CUENTA DE E-MAIL ORIGEN ANTE HOTMAIL / GMAIL / YAHOO

Apenas una dirección de email de envío origen es creada, existirán algunas tareas iniciales que podrán ayudar a lograr una buena reputación en el corto y mediano plazo, además tambien ayuda a clarificar algunas cuestiones en las pruebas iniciales de envíos.
Estas tareas son:

- Ingresar a la cuenta de email origen con el WEBMAIL del servidor smtp, y enviar un correo básico a 3 direcciones propias de prueba de hotmail, luego a 3 de gmail, luego a 3 de yahoo
- En cada caso, si el correo hubiese llegado a la bandeja de "no deseado", marcar el correo como "deseado", y asegurarse que se visualizan bien imágenes y links. Cabe aclarar, que en estos casos de reputación inicial, Yahoo suele permitir llegar a la bandeja de entrada, pero Hotmail al contrario: facilmente como primera medida al ser un correo origen nuevo, enviará el mensaje a la bandeja de Spam (Gmail mostró siempre comportamientos variados respecto a este punto)
- Una vez recibido el correo, marcado como seguro y visualizado bien en la bandeja de entrada, se debe agregar el contacto orígen en la Agenda de Contactos, tal como si fuera el mail de una persona.

Estas acciones lograrán un efecto positivo ante los 3 servidores. Ademas: desde ese momento, siempre el correo debería llegar a la bandeja de entrada de esas direcciones de prueba. Si alguna vez esto no se cumple, se deberá revisar y focalizarse en el MENSAJE, descartando otros motivos de dominio, mail y servidor.

9. ASUNTO Y MENSAJE BIEN CONFECCIONADOS

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.

10. MANEJO DE SUSCRIPTORES UTILIZANDO SERVICIOS DE HOTMAIL/GMAIL/YAHOO

Ademas de las cuestiones ya obvias como incluir un link de desuscripción para quien recibe el mensaje, hoy existen mecanismos que permiten un mayor control, que es brindado por cada servidor destino.
Resumiendo, se trata de lo siguiente:

- **HOTMAIL**
  Registrandose en su programa **Microsoft SNDS**, se puede dar de alta una o más IP origen del servidor, y luego solicitar notificaciones cada vez que un usuario destino marca a un mensaje como spam.
  Con esta información, será recomendable desuscribir esa dirección manualmente, para no seguir enviando a quien ya ha marcado al mensaje manualmente como "no deseado".
  Este mismo programa permite visualizar el nivel de carga que esta recibiendo Microsoft desde el SMTP, y cómo lo está catalogando: se basa en 3 colores segun la cantidad recibida (verde ok, amarillo dudoso y rojo negativo por alta carga)
- **YAHOO**
  Registrandose en su programa **YAHOO FEEDBACK LOOP**, se puede dar de alta uno o más DOMINIOS origen del servidor, y luego solicitar notificaciones cada vez que un usuario destino marca a un mensaje como spam.
  Con esta información, será recomendable desuscribir esa dirección manualmente, para no seguir enviando a quien ya ha marcado al mensaje manualmente como "no deseado".

- **GOOGLE**
  Registrandose en su plataforma **Google Postmaster** a traves de un registro de DNS, se puede dar de alta uno o más DOMINIOS origen del servidor, y luego visualizar el nivel de carga que esta recibiendo Google desde el SMTP, y cómo lo está catalogando.

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 recien mencionadas.
Consúltenos para así obtener información actualizada sobre nuestros planes:

Chat	Teléfono	WhatsApp
Botón de CHAT ubicado abajo a la izquierda en https://web-matter.com.ar	**5411 47982212** (lun/vie 10/19 hs)	**54911 54594979** (lun/vie 10/19 hs)