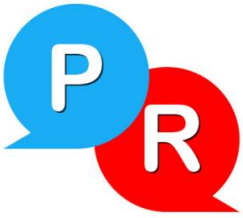
Preguntas y Respuestas sobre Emails - Parte 1

Recopilamos varias PREGUNTAS-RESPUESTAS que en los últimos años fueron surgiendo de parte de clientes e interesados en nuestros servicios. Aquí van las primeras 5. Próximamente seguiremos publicando más P/R como parte de esta serie.



P "Por qué me rebotó esta dirección de email, si es correcta?"

R Esta situación tiene más de un motivo posible:

- **REPUTACIÓN DE LA DIRECCIÓN ORIGEN**
  Lo más habitual en un caso así en el cual la dirección de e-mail existe y es válida, es que el servidor de e-mail y dominio origen están teniendo un problema de REPUTACIÓN, el cual hace que el anti-spam del servidor del destinatario rechace el mensaje y sea devuelto con un código de error.
  Este problema podría ser de naturaleza técnica, por ejemplo si se ha omitido configurar algún registro de importancia en el servidor de email (ej: DKIM, SPF, DMARC, REVERSO IP, HOSTNAME, PTR).
  También podría darse por haber enviado una alta carga de mensajes a ese servidor sin pausa entre los emails disparados, lo cual también deteriora la reputación.

- **ASUNTO Y TEXTO DEL MENSAJE**
  Hay algunas premisas que conviene considerar en los mensajes de emails hoy en día para evitar el rechazo de los antispams de los destinatarios. Por ejemplo, no conviene que el texto del asunto este todo en mayúsculas si se ha enviado un mensaje masivo.
  Se debe cuidar que el asunto no contenga palabras sospechosas que sugieran ventas o promoción, sino que se vea como un mensaje informativo o de una operación de usuario como por ejemplo registración o pago.
  En los textos del mensaje se debería cuidar que no se haya pegado código de programación no visual, por ejemplo de *Javascript*, el cual generaría rechazo seguro por sospecha de virus.

- **VÍNCULOS DEL MENSAJE**

  Para cada vínculo, dominio o dirección de correo de un mensaje se deberá cuidar:
  - El vínculo debe ser *https*, jamás incluir *http* en un mensaje de email.
  - El dominio incluído en el link o texto del mensaje no debe estar en ninguna lista negra.
  - La ip del dominio incluído en el link o texto del mensaje no debe estar en ninguna lista negra.

- **FILTRO ESPECÍFICO CREADO POR EL DESTINATARIO**

  El destinatario o su administrador de e-mails, pudo haber creado algún filtro por medio del cual si se cumple determinada condición el mensaje sea rechazado. Por ejemplo la inclusión de un texto puntual en el asunto o como parte del mensaje.

- **PROBLEMAS TÉCNICOS DEL DOMINIO DESTINO**

  La validación y detección del dominio destino dependerá de la calidad de su configuración de DNS y obviamente que el dominio este vigente. Si en el momento de enviar el e-mail al destinatario su dominio no estuviese disponible, también se generaría un mensaje rebotado: esta situación se detecta en el instante mismo del disparo del e-mail, aunque lo habitual es que el servidor origen realice reintentos hasta confirmar la no disponibilidad del dominio destino.

- **PROBLEMAS TÉCNICOS DEL SERVIDOR DE E-MAIL DESTINO**

  La validación y detección del servidor de e-mail destino dependerá de la calidad, configuración y disponibilidad de su servidor de e-mail SMTP.

  También dependerá de las configuraciones y disponibilidad de Networking en general: red, proveedor de conexión isp del mail server destino, etc. Si en el momento de enviar el e-mail al destinatario su e-mail y servidor no estuviesen disponibles, se generaría un mensaje rebotado: esta situación se detecta en el instante mismo del disparo del e-mail, aunque lo habitual es que el servidor origen realice reintentos hasta confirmar la no disponibilidad del servidor destino.

- **PROBLEMAS TÉCNICOS DE NETWORKING DEL SERVIDOR DE E-MAIL ORIGEN**

  Si en el momento de disparar el e-mail, el servidor origen no tuviese una conectividad normal a internet, el correo rebotaría al instante.

- **CASILLA DEL DESTINATARIO LLENA**
  Si bien hoy en día es menos usual que antes, el caso de una saturación de espacio por mensajes acumulados en el destinatario podría ocurrir. Hoy cuando esto sucede, probablemente se trata de una casilla de email "abandonada" por el usuario.

- **ALTO NIVEL DE ANTISPAM EN EL SERVIDOR DESTINO**
  A veces sucede que el servidor destino o el mismo usuario adopta un criterio de antispam muy muy alto, el cual puede generar un rechazo. Cuando esto sucede será necesario establecer contacto por otro medio, para avisarle que baje el nivel de protección, ya que el mismo podría ser exagerado y mayor al necesario. Por ejemplo, hay casos en que se permite llegar correos que pertenezcan a contactos previamente creados en su servidor, y hasta que el contacto no exista, el primer email no llegará.

Más info relacionada a esta respuesta:
» **Gestión de Correos Rebotados - Casos más habituales y cómo resolverlos**
» **Cómo enviar mailing masivo sin problemas**

P "No sé que pasó pero me desapareció un mensaje de email, dónde puede estar?"

R

Lo primero que nos muestra esto es que para mucha gente es posible que no se cuente con la certeza sobre qué ha ocurrido con un mensaje de email, y ha vivido así años, acostumbrado a que esto puede suceder peródicamente como si fuera algo normal...

...En estos tiempos, en los cuales el e-mail se utiliza para cuestiones importantes como confirmar registros de usuario, enviar facturas, autorizar cuentas, confirmar un pago al comprar un pasaje de avión o automóvil, etc, sería asumir que a pesar de su importancia real, enviar un email es menos exitoso que enviar una carta postal hace más de 100 años...

Evidentemente su proveedor anterior no le mostró la información completa, ni le explicó cómo verificar bien el problema.

Con la abultada información que se cuenta hoy en cualquier sistema tecnológico como programas, reportes, archivos de log, estadísticas, etc, sólo se trata de armar bien las cosas como para que quien hace esta consulta cuente en su pantalla con lo necesario para rápidamente resolver la incógnita del mensaje de email "desaparecido".

Cuál es el ciclo completo de un envío de email? Cómo verificar el problema del "mail desaparecido"?

En cualquier envío de email, sea masivo o individual, para cada email a enviarse existen las siguientes fases posibles:

FASE 1

CREACIÓN

Existencia
Formato
Ortografía

FASE 2

DISPARO

Aplicación de Envío
Conexión de Red local o Wi-Fi
Conexión a Internet

FASE 3

EN COLA DE SALIDA DEL SMTP

Congestión?
Retenido temporalmente?
Dosificación forzada?

FASE 4 ERROR

REBOTE

Dirección inválida?

Casilla Llena?
Dominio destino inválido?
Bloqueo Anti Spam?

FASE 4 EXITO

LLEGÓ!

Inbox?
Junk?
Otra carpeta?

Conocer estas fases en detalle permitirá saber siempre donde puede encontrarse un determinado mensaje.

Para leer info detallada de cada una de estas fases, ingresar a la siguiente nota:
» **Derribando el mito del "EMAIL DESAPARECIDO"**

P "Estan llegando miles de emails basura extraños y rebotados. Por qué?"

R

Asi como en los últimos años creció exponencialmente la activación de Antispams, también creció exponencialmente el volumen de virus dañinos tanto locales como remotos que suelen atacar o intentar adueñarse de los servidores de e-mail...

...El motivo por el cual se observan miles de correo basura, es porque estos virus intentan reutilizar cuentas de email del servidor para enviar fraudulentamente mensajes de email a miles de destinatarios.

El formato de estos miles de mensajes es de correos rebotados, porque al dispararse de a miles, en gran parte de los destinatarios de las listas los correos rebotan y no llegan a destino.

Debido a que hoy en día las configuraciones correctas de SMTP siempre previenen estos casos, normalmente estos emails generan un caos solo en la *mail queue*, pero no son disparados en la realidad, sino que eso queda en el intento sin poder ejecutarse.

La acción de este tipo de virus podría provenir desde distintos orígenes a revisarse:

1. **DESDE EL PROPIO SERVIDOR DONDE SE ENCUENTRA EL SERVIDOR DE E-MAILS**
   Cuando se ha detectado un virus en el mail server, una de las primeras acciones es revisar la "mail queue" (cola de salida/entrada de mensajes) y como segundo paso ejecutar un programa en el server local, por ejemplo realizar un scanneo con *clamscan* o con programas anti-malware como por ejemplo Maldet.
   Se deberán barrer todas las carpetas del servidor, tanto las relacionadas a mensajes de cuentas de e-mail, como así tambien a las carpetas de páginas web almacenadas en el mismo servidor, si es que existiesen: no olvidemos que una de las variantes más comunes es que usen formularios web para potenciar los disparos de emails.

2. **DESDE LAS MÁQUINAS (PC, NOTEBOOKS) DONDE SE ENCUENTRAN CONFIGURADAS CUENTAS DE E-MAIL POP3 O IMAP DEL @DOMINIO**
   Si hubiera que hacer un ranking, esta opción se lleva el primer puesto, porque los virus más habituales son aquellos que reusan una cuenta de email de una pc, normalmente configurada en Outlook o Thunderbird. Por eso es sumamente importante hoy en día trabajar con CONTRASEÑAS ULTRASEGURAS, de modo de minimizar el posible accionar de estos virus.

3. **VIRUS REMOTOS**
   Los virus remotos pueden ser prevenidos por Firewalls que protejan el servidor de e-mail. Pero aquellos más invasivos, pueden combinarse con formularios web que generen un alto volumen de tráfico en poco tiempo, logrando que enseguida se afecte la operatoria del resto de las cuentas de e-mail del servidor.

Hay que tener en cuenta que este tipo de virus podría tener distintos propósitos abusivos. Los más comunes son:

:: Reusar cuentas de e-mail existentes para enviar mail masivo tipo spam (propagandas)
:: Reusar cuentas de e-mail existentes para enviar mail masivo saturando a un servidor externo
:: Generar caos en el servidor de e-mail para afectar la operatoria normal de las cuentas de los usuarios
:: Reusar una cuenta de e-mail puntual para un objetivo específico (normalmente accionado y ejecutado por un tercero)

Cuando este tipo de virus actua, la operación de los usuarios se ve afectada hasta el momento en que la *mail queue* se limpie y se normalice, además de haber detectado la forma de prevenirlo a futuro.

Más info relacionada a esta respuesta:
» **Cuál es la mejor estrategia anti-spam posible para aplicar en un servidor de mail?**

P "Puedo tener una dirección que sea @subdominio.dominio?"

R Si, el formato es válido, tanto los servidores de dominio como los servidores de e-mail estan preparados para este tratamiento...

Cuando se crea un servidor de e-mail deberá definirse en cada detalle que todo será configurado para el formato @subdominio.dominio: los registros TXT del servidor como SPF, DKIM y DMARC, asi como también el reverso de ip, y cada mínimo detalle del SMTP contemplarán siempre el formato de @subdominio.dominio de modo de que adquiera la independencia necesaria en el uso posterior: será muy importante que no se superponga a configuraciones de otros subdominios relacionados al dominio principal.

Ejemplo de una dirección con este formato: *facturacion@admin.abc.com* -> en este caso, el usuario "facturacion" tiene su cuenta en el subdominio "admin" dentro del dominio "abc.com".

P "Qué significa si un email enviado a *@gmail.com* es rechazado con *OverQuota*?"

R

Hoy en día cuando se envía un mensaje a una dirección de *@gmail.com* que fue abandonada por el usuario o sino que ha dejado llenarse al tope su espacio de almacenamiento, la misma suele devolver el siguiente mensaje como parte del texto de "rechazado":

(host alt1.gmail-smtp-in.l.google.com[64.233.x.x] said: 452-4.2.2 The recipient's inbox is out of storage space. Please direct the 452-4.2.2 recipient to 452 4.2.2 support.google.com 5b1f17b1804b1-4217ab2ab41si45927805e9.190 - gsmtp (in reply to RCPT TO command))

Y esta situación, entre el servidor de gmail al rechazar y el servidor origen del mensaje al recibir la devolución, suele estar acompañada del identificador *p=OverQuotaPerm* o sino *p=OverQuotaTemp*.

De acuedo a lo expermimentado hasta el momento, en los casos en que se recibe *p=OverQuotaPerm* estará casi garantizado que la dirección fue abandonada, y en los casos en que el identificador es *p=OverQuotaTemp* podría tratarse de una situación temporal.

Cabe aclarar que observamos que la situación de devolución con *p=OverQuotaTemp* puede extenderse mucho en el tiempo (días, meses), dándose en la mayoría de esos casos que el usuario también abandonó la cuenta pero gmail se demora en confirmarlo del todo.

Si el servidor origen está bien configurado y el sistema de correos rebotados tambien, cuando se trate de un caso temporal, se volverán a realizar reintentos para ver si es posible llegar a destino luego de un período más tarde. Y luego de x cantidad de reintentos, devolver la situación de "correo rebotado" a los reportes de información que lee el usuario final.

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