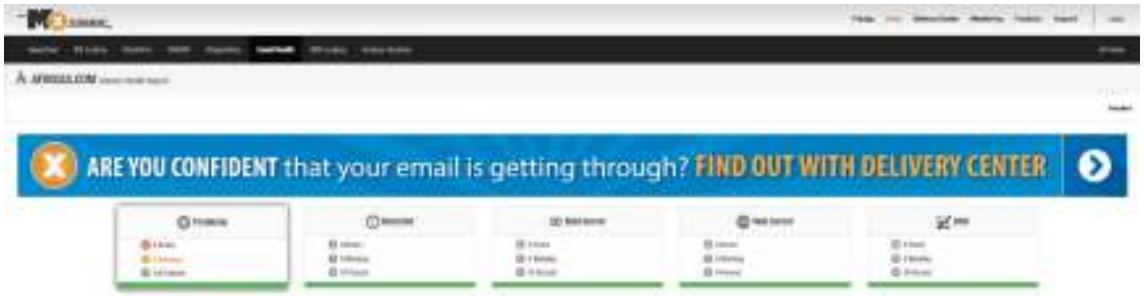
RECOMENDACIONES SOBRE EL USO ADECUADO DE LAS CUENTAS DE CORREOS Y MANEJO DE INCIDENCIAS

Durante muchos años hemos disfrutado de nuestras cuentas de correo electrónico sin apenas problemas. Nos entregaban una cuenta y sin necesidad de nada más, recibía y entregaba correos electrónicos durante años sin apenas incidencias. Esto ha cambiado**. La lucha contra el delito informático, contra correos no deseados (spam), suplantaciones de identidad (phishing), etc. han obligado a añadir NUEVOS PROTOCOLOS de seguridad en los últimos tiempos para que pueda ser entregado o recibido un correo. Quienes no hayan añadido esos protocolos o no los hayan configurado bien, simplemente no recibirán algunos de estos correos**. **También se han MULTIPLICADO las inclusiones en listas negras por circunstancias menores por las que hace unos años no habría mayor problema.**

En resumen, los algoritmos de los proveedores de servicios de correo son cada vez más estrictos (en especial en la lucha contra el SPAM) y eso nos obliga a entender que la situación ha cambiado radicalmente, implica a la responsabilidad de todos y no tiene una solución fácil.

En el caso de los colegiados de afincas sus cuentas de correos **cumplen con todos los protocolos de seguridad exigidos y el estado de salud de la cuenta es excelente**, por lo tanto, las incidencias que puedan ocurrir serán, casi con seguridad, fruto de un problema en los correos de los destinatarios (bien por configuración de los correos o por estar en listas negras) o por haber sido incluido específicamente la IP del colegiado en alguna lista negra.



Estado de salud de la cuenta de afincas.com a 15/03/2023 (146 puntos revisados: 0 errores y 0 advertencias. Esto es común, en principio, para cada una de las cuentas de correo de los colegiados)

El correo electrónico es un servicio fundamental e indispensable para todos los usuarios de internet. La frecuencia con la que se emplea el correo corporativo (cuenta_de_usuario@afincas.com) y su utilización por centenares de usuarios, provoca obviamente, que este sea el servicio con el mayor número de incidencias.

En este documento vamos a revisar las más habituales y realizar algunas recomendaciones:

1. Cuota excedida

A pesar de que la modalidad recomendada en la creación de una nueva cuenta corporativa es con el protocolo POP (los correos se descargan localmente en el ordenador y se eliminan del servidor pasado un número de días determinado, que en Outlook se puede establecer hasta en 99 días) muchas de estas se han creado con el protocolo IMAP (se accede a los correos almacenados en el servidor y solo se eliminan de este si el usuario decide borrarlos manualmente). Esto provoca un aumento continuo del espacio de la cuenta hasta provocar que la cuenta se exceda del tamaño predeterminado a la hora de su creación. Se asigna a cada cuenta en su creación espacio suficiente para albergar más de 4 meses de correos electrónicos. Obviamente ese espacio es insuficiente cuando una cuenta IMAP se prolonga en el tiempo y provoca que la cuenta quede suspendida al excederse la cuota asignada. Nuestra recomendación es siempre crear cuentas de tipo POP para evitar estos inconvenientes y si tiene una cuenta IMAP le recomendamos ponerse en manos de un informático para que traslade los correos de su cuenta IMAP a una cuenta POP.

Enlace con información para trasladar una cuenta IMAP a una POP: https://www.vorealis.com/Portals/1/GuiaConvertirIMAPaPOP.pdf

2. IP baneada

El baneo o denegación de un servicio (acceso al correo electrónico o a la web) es una medida de seguridad del servidor como respuesta a que este detecta en una cuenta algún tipo de actividad sospechosa. Esto sucede comúnmente cuando no se ha configurado correctamente el correo corporativo en el gestor de correo de su computadora, lo que ocasiona que el sistema intente acceder varias veces a la base de datos del correo sin éxito, por lo que el Firewall lo detecta como una amenaza a la seguridad del servidor y bloquea la IP de donde proviene esta acción. También es habitual que dichos baneos ocurran por errores en repetidos intentos de acceso con una contraseña equivocada. En ocasiones, hemos detectado que errores en la bandeja de salida del gestor de correo del cliente, provoca distintos reintentos que generan que el servidor proteja la cuenta baneando lo que entiende que es una IP atacante. En este caso, póngase en contacto con la secretaría del colegio, y se le desbaneará en pocos minutos.

3. Problemas en la entrega y devoluciones de correos

Desgraciadamente, **la proliferación exponencial de amenazas en el entorno de internet, han provocado que los servidores mundiales en su intento de combatirlo, hayan habilitado distintos filtros o defensas que en ocasiones provocan efectos colaterales indeseables**; se evalúa la estructura del mensaje, el encabezado, los archivos adjuntos o el número de destinatarios para dilucidar si el mensaje electrónico supone

una amenaza o no. En ocasiones el listón de lo “aceptable” se pone tan alto en algunos servidores que se rechazan correos electrónicos absolutamente inocuos.

Las devoluciones de correos, cuando se producen, pueden estar causadas:

a) Por problemas de seguridad del correo del destinatario. Esto es lo más habitual. La mayoría de cuentas de correo no tienen mantenimiento desde que se crearon. La lucha contra spam y resto de delitos de internet, provoca que se devuelvan correos si no tienen habilitados o bien configurados nuevos protocolos de seguridad de reciente aparición. También podría ocurrir que el destinatario estuviese inscrito en alguna lista negra que nuestro servidor detecte. Y ahí poco se puede hacer, salvo comunicar esto al destinatario para que lo corrija.

b) Porque la IP del remitente (el colegiado) esté en listas negras y sea rechazado por el servidor del destinatario.

Recomendaciones para evitar entrar en listas negras:

a) **No hacer click en mensajes de dudosa procedencia**. Podría instalarse un troyano o malware en el ordenador y enviar spam o suplantarle la identidad sin ser conscientes de ello. Le recomendamos que antes de clicar en el enlace o en el archivo adjunto, sitúe el ratón encima: suele aparecer una ventanita emergente o bien en la barra inferior del navegador con la dirección real a la que se dirigirá. Si tiene la menor duda de que esa dirección le parece sospechosa o no tiene nada que ver con el motivo del enlace, evite cliquear y póngase en contacto con el cliente o proveedor por otro medio y confirme la autenticidad del mensaje.

Mantenga su antivirus actualizado y asegúrese que monitoriza los correos electrónicos en tiempo real, si no es así, adquiera una solución de pago que lo incluya. Consulte con su informático.
Más Información sobre correos fraudulentos y phishing:
https://www.mcafee.com/blogs/es-mx/internet-security/ejemplos-de-correos-electronicos-de-phishing-y-como-reconocerlos/

b) **No enviar correos masivos o a muchos destinatarios a la vez**, ya que las empresas vigilantes que monitorizan el tráfico de correos, pueden entender que se está enviando spam e incluir en lista negra la ip de sus equipos e incluso su propia cuenta.
Para el envío masivo de correos, se recomienda buscar una solución de marketing o de listas de distribución.
Hay muchas en el mercado, pero las opciones más populares entre otras son:
MailChimp (https://mailchimp.com/es/)
Sendingblue (https://es.sendinblue.com/)
ActiveCampaigne (https://www.activecampaign.com/)

Tampoco conocemos los criterios en cuanto al número de destinatarios máximos en un solo correo, porque son cambiantes y dependen de los muchos servicios anti-spam que "vigilan" en tiempo real nuestros correos y que podrían considerar que estamos enviando spam, pero como norma general lo ideal es enviar un único correo al menor número de destinatarios posibles o podría terminar con la IP en listas negras.
Enviar, por ejemplo, un solo correo a 30 o 40 destinatarios de una comunidad de propietarios, es algo que convendría evitar o al menos no hacerlo con asiduidad porque podrían ser incluidos en listas negras (blacklist). Cuando esto ocurre, los servidores de destino que revisen alguna de las listas negras en la que la IP del colegiado se encuentre, rechazarán los correos.

c) **Pedir al cliente que te agregue a la libreta de direcciones** suele ayudar a entregar el correo.

d) **Descargar malwarebytes** (hay una versión gratuita) y analizar los ordenadores frecuentemente, para prevenir o detectar el problema cuánto antes.

e) **Depurar la lista de contactos** para que no envíe correos a destinatarios que ya no existan o no tengan actividad. Este es otra circunstancia arquetípica de los spammers, que envían una cantidad ingente de correos, pero las cuentas están sin depurar y lo hacen muchas veces a cuentas no activas.

Procedimiento para quitar una IP de una lista negra

Si ya estamos en una lista negra, podemos seguir secuencialmente estos pasos:

1. **Descargar malwarebytes** (https://es.malwarebytes.com). Se debería pasar a todos los equipos que utilicen esa IP un antivirus (completo) y el malwarebytes, por si el origen del problema estuviese ahí.
2. **Solicitar que lo quiten de la lista negra**. Esto es algo que no siempre es fácil, y es recomendable que lo haga un informático. Aunque algunas listas negras deslistan bajo demanda en pocos minutos, otras marcan un tiempo de días para hacerlo, y algunas otras no deslistan a demanda, sino cuando vuelven a revisar la situación de la cuenta de correo. Por ello, dependiendo de la lista negra, esto no siempre será posible.
3. Si el punto 2. no es posible, **apagar router durante diez minutos y volver a encender**. En ocasiones este procedimiento proporciona una nueva IP. Una nueva IP limpia solucionará el problema, siempre que se hayan tomado medidas para evitar la causa que lo originó.
4. Si 2. y 3. no funciona, **hablar con su proveedor de internet**, contarle el caso y solicitar que le cambien la IP desde el servicio técnico.

Cualquier colegiado puede tener un diagnóstico del estado de salud de una cuenta de correo (la suya o la del destinatario) mediante el siguiente procedimiento:

1. Ir a https://mxtoolbox.com/emailhealth/
2. Añadir en el cuadro de texto la cuenta de correo o el dominio (el texto que aparece tras la @), que se quiera analizar.

Para saber si está en una lista negra:

1. Ir a https://mxtoolbox.com/blacklists.aspx
2. Añadir en el cuadro de texto la IP. (Puede encontrar su IP en https://miip.es)

Algunos enlaces de interés con más información sobre el tema:

Listas negras

https://www.aulatina.com/que-son-las-listas-negras-rbl/

https://linube.com/blog/blacklist-que-es/

Protocolos seguridad correo

https://www.simla.com/blog/spf-dkim-y-dmarc