Seguridad y buenas prácticas del correo

- Añadir a correo de confianza en Microsoft
- Cambiar la contraseña de tu Webmail
- Buenas prácticas de correo

Añadir a correo de confianza en Microsoft

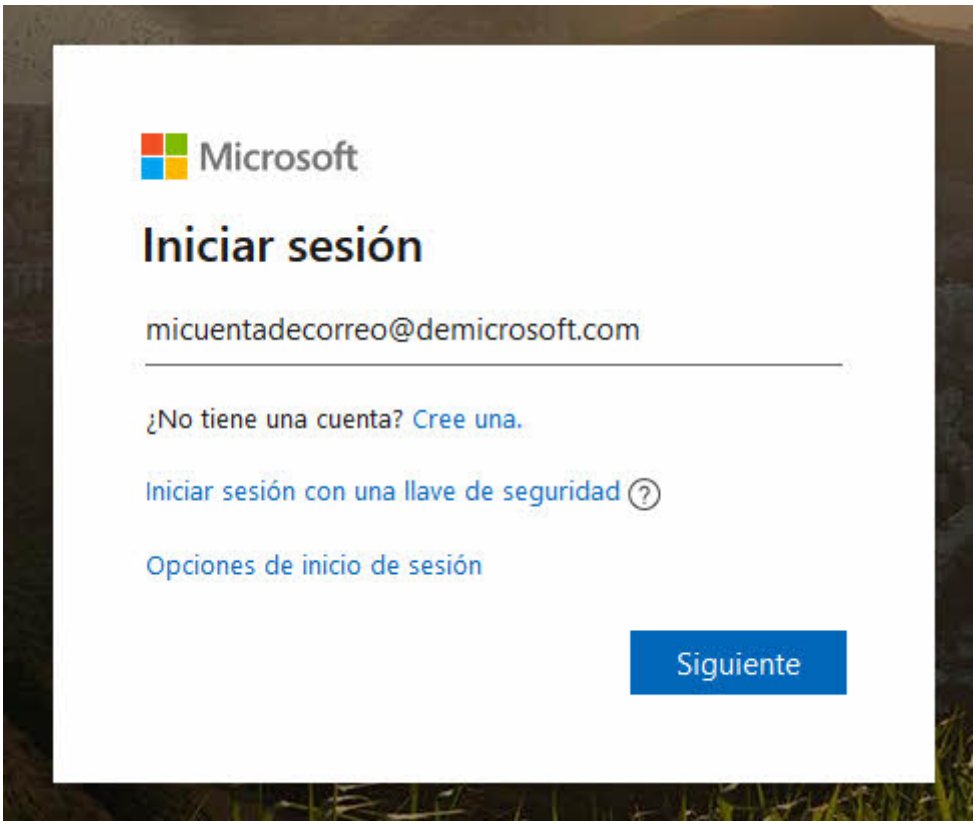
Correo seguro en Microsoft (Hotmail, Outlook...)

En una empresa, ya sea del sector hotelero o de cualquier otra, es necesario separar su dirección de correo de aquellas que está catalogadas como «spam». Para ello, la principal tarea es indicar a los proveedores de correo más relevantes que nuestro correo no es «correo basura».

En este caso, vamos a ver cómo hacerlo con las cuentas de Microsoft.

1. Acceda al Smart Network Data Service de Microsoft

https://sendersupport.olc.protection.outlook.com/snds/whoelse.aspx?wa=wsignin1.0



Si no tiene una cuenta, cree una, le llevará tan sólo 10 segundos.

2. Completar su perfil

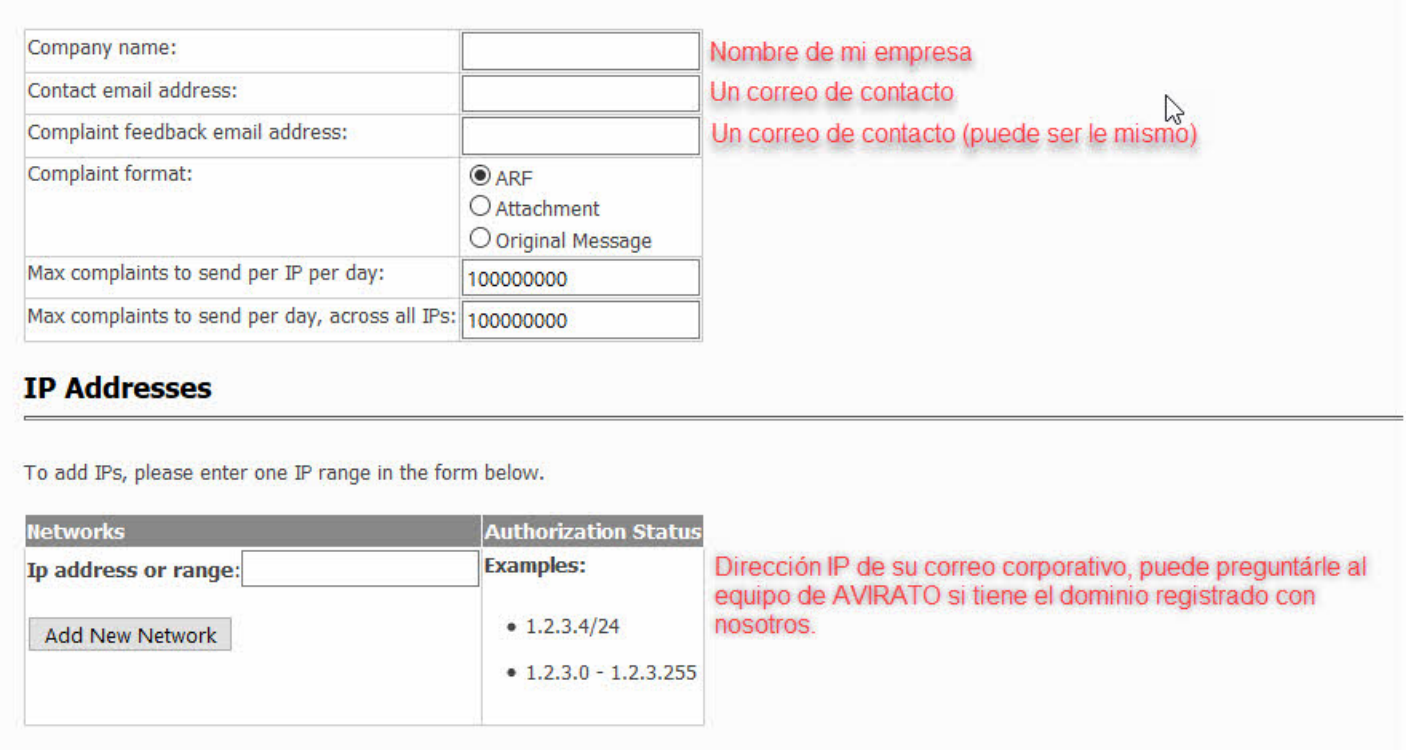
Con añadir el nombre y el apellido es suficiente



3. Junk Mail Reporting Program



En esta sección, rellene los campos que le solicitan, como el nombre de la empresa o el correo electrónico.



Cuando añada la IP y de a «Add New Network», le solicitará una autorización por correo, indique la primera opción «**abuse@[sudominio].com**«. Si tiene su dominio registrado con AVIRATO, la información de dicho correo debería estar en su conocimiento.

4. ¡Listo!, ya tiene registrado su dominio



¿No ha encontrado lo que busca? Contacte con nuestro equipo y le ayudaremos.

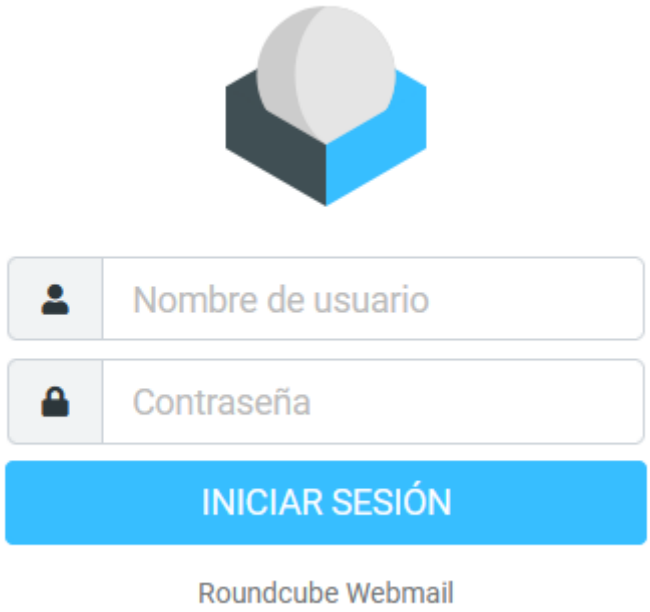
Cambiar la contraseña de tu Webmail

Cambiar la contraseña en https://webmail.*midominio.com*

Acceda a su buzón de correo

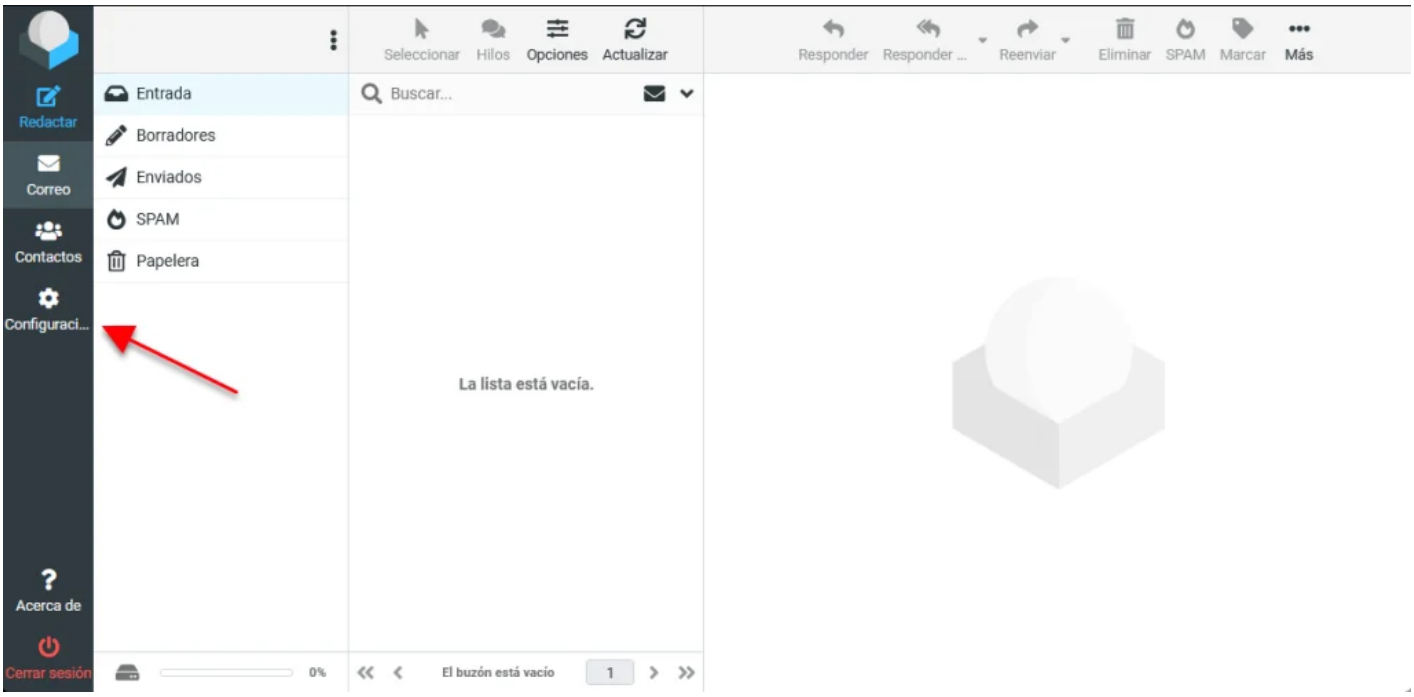
Su buzón de correo (su buzón real, donde se almacena su correspondencia digital), está en la URL

https://webmail.sudominio.com



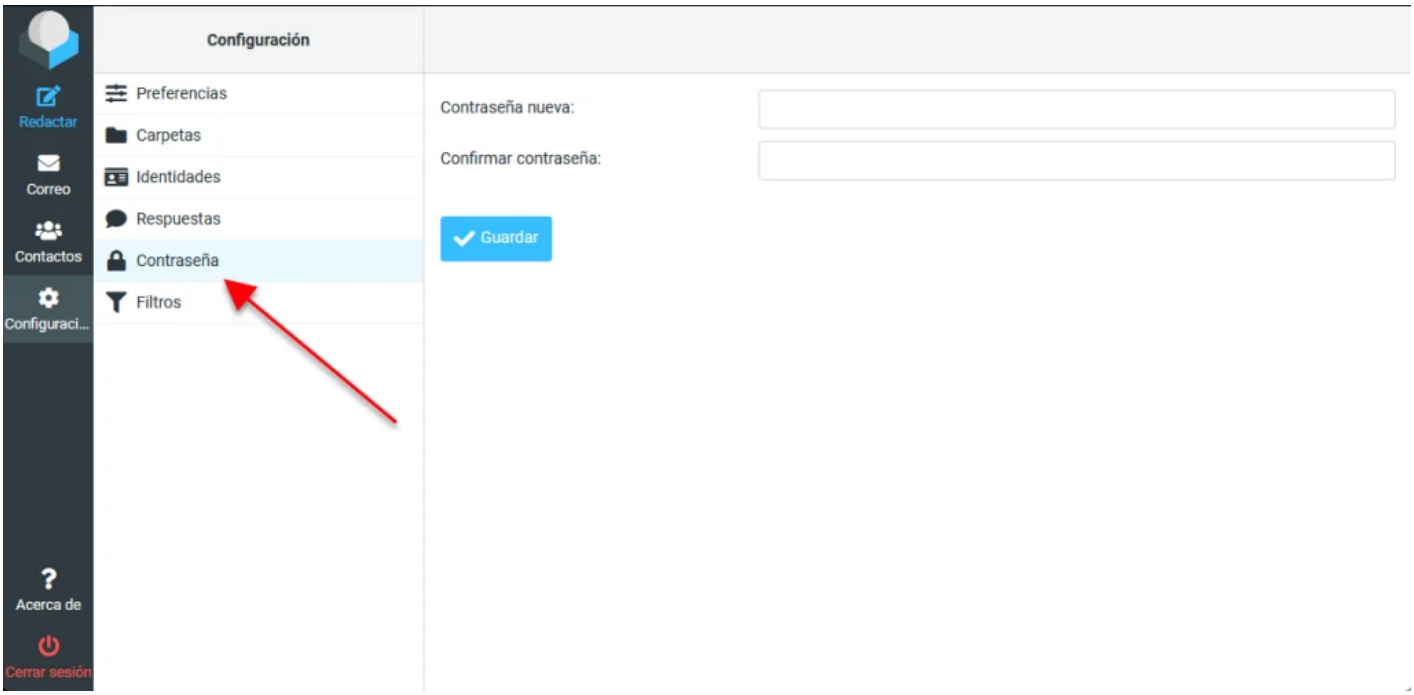
1. Acceder a la configuracion del correo

Lateral izquierdo de la pantalla



2. Seleccionar en el menú de configuracion "Contraseña"

En el aparecera un formulario de dos campos desde el que podrá establecer una contraseña nueva



Le recomendamos usar una contraseña que tenga, al menos, 8 caracteres alfanuméricos, tanto en mayúsculas o minúsculas; además de, algún símbolo. De este modo se hará exponencialmente más difícil que se apropien de ella.

¡Importante! Tenga en cuenta que esté es su buzón real, y que todas las configuraciones de terceros tendrán que adaptarse si cambia la contraseña.
Por ejemplo, la configuración de su PMS si lo usa para la automatización de correo:
Configurar el correo eletronico en el PMS

¿No ha encontrado lo que busca? Contacte con nuestro equipo y le ayudaremos.

Buenas prácticas de correo

Como evitar que tus mails acaben en SPAM

Hoy en día, todos recibimos y enviamos correos electrónicos prácticamente a diario, y entre este tráfico de correo, es común que muchos vayan a la carpeta de SPAM. Por regla general, estos correos que acaban en SPAM son, bueno... eso, SPAM, pero también es frecuente que un correo que no es *correo no deseado* acabe en dicha carpeta. Y Aunque la mayoría de las veces se puede evitar, existen muchos factores relevantes que pueden provocar esto. En Avirato te facilitamos algunas recomendaciones para, en la medida de lo posible, evitar que tus correos empresariales acaben en SPAM

1. ### Usa solo tu correo corporativo para asuntos corporativos

   Resulta evidente decir esto, pero nunca uses tu correo de empresa, con el que gestionas tu negocio y depende tu *modus vivendi*, para registrarte en **NINGÚN** sitio web. Hacer eso, es abrir una puerta a recibir SPAM, y otros visitantes menos deseados, como virus y ataques de malware

2. ### Evita los gestores de correo

   Resulta muy tentador emplear un gestor de correo como Outlook o Thunderbird para ver tu correo, pero estos gestores son el punto de mira de la mayoría de virus que rastrean tus contactos y envían correos masivos en tu nombre, ya que son un elemento en el que los constructores de malware pueden basarse. Si esto ocurre, no solo puede ocurrir que los sistemas de seguridad de nuestros servidores bloqueen tus envíos para evitar que mandes correo basura, sino que da una imagen muy poco profesional para tu negocio de cara a tus clientes. Así pues, desde Avirato siempre recomendamos utilizar directamente tu buzón de correo Webmail, el cual te mandamos cuando te creamos los correos. Para más información, contacte con nuestro equipo.

3. # La importancia del *Asunto*

   Los filtros antispam están parametrizados para detectar correos no deseados en base a una serie de factores y palabras clave. Es por ello por lo que, si empleas mayúsculas en tus asuntos, o usas palabras que todos asociamos a correo no deseado, como “gratis”, “oferta” o “descuento” (entre otras), tus correos acaben, no llegando a la bandeja de entrada.

4. # Prestar atención al cuerpo del correo

   Del mismo modo, también es arriesgado utilizar palabras que tradicionalmente se asocian con correo basura, dentro del propio cuerpo del mensaje. Evita emplear demasiadas exclamaciones, referencias a gratuidades en productos o servicios, o expresiones que induzcan a comprar o generar confianza en el lector. Un correo sobrio e informativo, a menudo es lo mejor, e incluso lo más producente en un correo corporativo.

5. # No uses enlaces acortados

   Una de las prácticas más comunes en los ataques de phishing (ser engañados para dar nuestras credenciales) es usar acortadores de enlaces para camuflar dominios y que el usuario no considere que está accediendo a un sitio no legítimo. Esto hace que los enlaces acortados estén en el punto de mira de los filtros antispam. Muchas veces tratamos de adjuntar enlaces muy engorrosos y largos en nuestros correos, pero eso es mejor al hecho de que el recetor nunca reciba nuestra comunicación

6. # No abuses de las imágenes

   Utilizar imágenes aligera la lectura y da un toque estético en nuestros correos. Pero en muchas ocasiones, se utiliza para ocultar información, como las palabras clave anteriormente mencionadas, por lo que es frecuente que se sospeche de correos con un número muy alto de imágenes. Aun así, eso no quiere decir que no podamos valernos de ellas en nuestros correos, únicamente tener en cuenta que un correo con 400 palabras y 15 imágenes puede resultar “sospechoso”. ¿Qué recomienda Avirato? Que emplees imágenes únicamente para completar información. Añadir una imagen que aporta la misma información que el texto ya incluido, no es buena idea.

7. # Los límites de envíos son muy importantes

Nuestros sistemas de software y almacenamiento establecen unas limitaciones en el envío de correo. Esto es muy importante para evitar que la IP de su dominio acabe en una lista negra de correo en caso de que sus equipos se infecten con un malware, o lo más común, que alguien se haga con sus credenciales y envíe correos en su nombre. Uno de los errores más comunes es usar la propia IP del dominio para el envío masivo de correos. Esto puede hacer que no solo un correo, sino todos los correos asociados a ese dominio (lo que va después del @), se vean perjudicados. Es por ello que, si planea hacer campañas de marketing electrónico, use aplicaciones muy eficientes y confiables como Mailchimp o Sendinblue

8. # Tener una lista de contactos actualizada

Otro de los problemas de los envíos masivos, es no revisar los destinatarios de dichos correos. Si un gran número de nuestros envíos van a direcciones de mail que no existen, esto lo hace potencialmente susceptibles de considerarse correo basura, y más aún si se envían a correo que sí existen, pero que han manifestado anteriormente que no desean recibir tus correos. Existen dos cosas que puedes hacer principalmente. La primera es verificar si el correo al que envías existe con servicios como Verify Email. Y una vez te hayas cerciorado de que dicha cuenta existe, fomenta que puedan responderte al correo remitente, evitando buzones de correo como noreply@… Con esto, consigues que las posibilidades de que tus correos vayan a una lista blanca aumenten

9. # Sé estricto con la con RGPD

Es muy importante tener presente que, con la nueva normativa del reglamento general de protección de datos, el receptor de tus correos ha de primero consentir que le envíes correos comerciales, como ofrecerle después la posibilidad de darse de baja de estos. Esto se hace poniendo a disposición del usuario un consentimiento explícito en nuestros formularios de contacto, y añadiendo una cancelación de suscripción en nuestros correos comerciales. Muchos sistemas de email marketing como los anteriormente mencionados ya disponen de esta metodología

10. # Las claves de acceso

    La apropiación de contraseñas y cuentas de email es mucho más común de lo que parece. Una contraseña realmente robusta es una formada por 16 caracteres, establecidos al azar, y compuestos por letras, números y símbolos, y estas ser cambiadas con una regularidad, de al menos una vez cada tres meses. Con esto, dificultarás la apropiación por la fuerza de tu contraseña.

11. # Las herramientas de marketing digital

    La mejor manera de que tu IP no acabe fichada como SPAM, debido a envíos masivos, es usar herramientas especializadas a tal fin. Y no solo eso, dichas herramientas también ponen a tu disposición informes y estadísticas de estos, como quién lee tu correo, cuántas personas se dan de baja debido a un email, cuántas veces se ha accedido a un enlace del correo, etc. Esa información no se puede obtener mediante envío directo, el cual, únicamente permite saber si el correo se ha enviado o no. Todo eso, te ayudará a que tus comunicaciones lleguen a su destino: La bandeja de entrada. Evitando acaban en SPAM, devaluando tu dominio y marca comercial

¿No ha encontrado lo que busca? Contacte con nuestro equipo y le ayudaremos.