Configuración y Buenas Prácticas en Email

Contenido

Control de cambios

Versión	***Fecha***	***Descripción de la Modificación***	***Responsable (s)***
1	Junio 2023	Creación del documento	Alejandro Martínez

1. Registros DNS

Los registros DNS son archivos de mapeo o sistemas que le indican a un servidor DNS a qué dirección IP está asociado un dominio particular. Estos registros también les indican a los servidores cómo manejar las solicitudes que se envían a cada nombre de dominio.
Para que puedas hacer envíos de correos electrónicos desde un dominio, es necesario que se configuren algunos registros de tipo TXT (texto) dentro de los DNS de dicho dominio. Un registro "TXT" significa "Texto". Esta sintaxis de DNS permite que los administradores inserten un texto en sus DNS y es utilizado para denotar hechos o información sobre dominios.

1.1. Autenticación manual de registros de texto (TXT)

La autenticación manual de registros TXT o CNAME dentro del dominio del cliente debe ser efectuada por el administrador del dominio desde el portal de proveedor de dominios del cliente.

La configuración de estos registros se debe dar para el registro SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail), estos deben ser agregados a los DNS del dominio.

La autenticación manual de registros TXT o CNAME requiere una configuración de la siguiente manera:

SPF: Sender Policy Framework es un registro que identifica las IPs y/o servidores que pueden enviar correo a un nombre de dominio.

El registro TXT que se debe agregar es:

Host: @

Value o destino:

- ✔ Se debe configurar un registro SPF en cada dominio, incluyendo a nuestros servidores (Tipo TXT):

v=spf1 include:_spf.aldeamo.com ~all

- ✔ Si ya existe un registro SPF, se debe incluir nuestro servidor dentro del registro existente (No se debe crear un segundo registro, esto causa errores en la entrega):

include:_spf.aldeamo.com

DKIM: El DKIM (DomainKeys Identified Mail) es un registro que se agrega a los DNS también como un registro tipo CNAME y tiene una llave pública o cadena de texto de autenticación que permite que cuando un E-mail salga

con llave privada, el servidor de E-mail de destino pueda comprobar que las llaves son válidas al contrastarlas.

El registro DKIM que se debe agregar es:

Host: default._domainkey

Value: _dkim.aldeamo.com

✔ Se debe configurar un registro DKIM en cada dominio, incluyendo nuestra firma (Tipo CNAME).

Para poder hacer envíos de correo electrónico desde la plataforma debes configurar estos registros. De otra manera, los correos no pueden ser entregados a sus destinatarios por falta de verificación de remitente y de permisos para envío de correo desde nuestros servidores.

1.2. ¿Cómo configurar un subdominio?

Para la configuración de registros dentro de un subdominio, ejemplo: registros.empresa.com, es necesario que el subdominio haya sido creado dentro del administrador que le otorga su proveedor de dominios.

La configuración de estos registros se debe dar de la misma manera para dominios y subdominios. Es necesario incluir el registro SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail), estos deben ser agregados a los DNS del dominio.

La autenticación manual de registros TXT o CNAME requiere una configuración de la siguiente manera:

> **SPF:** Sender Policy Framework es un registro que identifica las IPs y/o servidores que pueden enviar correo a un nombre de dominio.

El registro TXT que se debe agregar es:

Host: @

Value o destino:

✔ Se debe configurar un registro SPF en cada dominio, incluyendo a nuestros servidores (Tipo TXT):

v=spf1 include:_spf.aldeamo.com ~all

✔ Si ya existe un registro SPF, se debe incluir nuestro servidor dentro del registro existente (No se debe crear un segundo registro, esto causa errores en la entrega):

include:_spf.aldeamo.com

DKIM: El DKIM (DomainKeys Identified Mail) es un registro que se agrega a los DNS también como un registro CNAME y tiene una llave pública o cadena de texto de autenticación que permite que cuando un E-mail salga con llave privada, el servior de E-mail de destino pueda comprobar que las llaves son válidas al contrastarlas.

El registro cname que se debe agregar es:

Host: default._domainkey
Value: _dkim.aldeamo.com
Se debe configurar un registro DKIM en cada dominio incluyendo nuestra firma (Tipo CNAME).

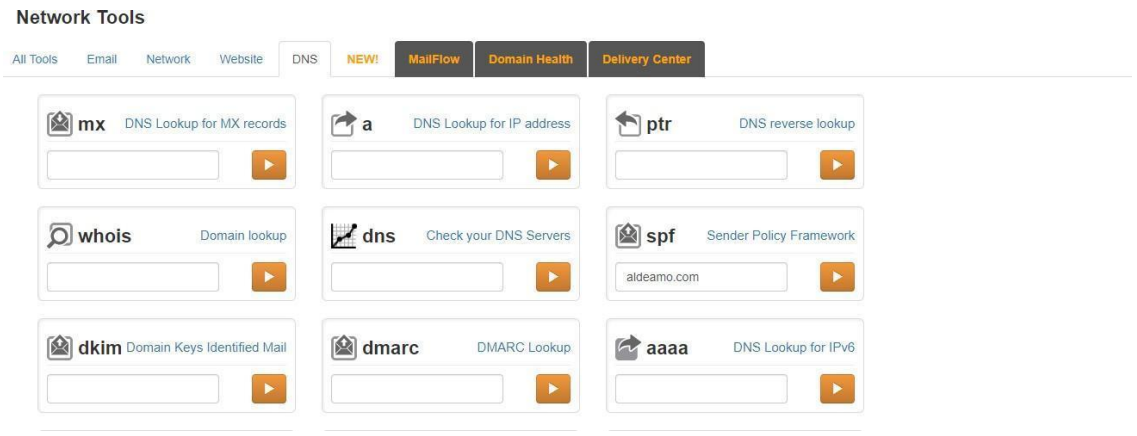
1.3. Probar que la configuración sea exitosa.

Para probar que los DNS estén bien configurados, puedes comunicarte con servicio:

Correo: servicio@aldeamo.com

Si deseas hacer la verificación directamente, recomiendamos herramientas gratuitas online como:

https://mxtoolbox.com/NetworkTools.aspx
En el link anterior se pueden encontrar diferentes parámetros para búsquedas desde registros DNS. Los registros que configuraste fueron SPF y DKIM, es por eso que para hacer la consulta solo deberás escribir el nombre del dominio en la casilla que refleje el registro



2. ¿Qué hacer para garantizar entregabilidad?

El correo electrónico como canal de comunicación ha estado en uso por más de 30 años. Esto ha generado que varias malas prácticas sean ejecutadas por las personas que lo han utilizado a lo largo de estos años. Es por esa razón que enviar un correo electrónico recientemente ha generado la inclusión de varios entes reguladores del proceso, que instalan barreras para poder detectar los correos no deseados por los usuarios en su bandeja.

Con el fin de regular y evitar las malas prácticas en el envío masivo de correo electrónico, la reputación del dominio es cada vez más utilizada por los proveedores de buzones de correo para poder identificar los correos que los usuarios no quieren recibir. Por esta razón, es importante garantizar que los dominios son presentados en el mundo digital de una manera adecuada y vital para reducir la probabilidad de problemas de entregabilidad.

Aunque la industria de correo electrónico no tiene pautas específicas para garantizar completa efectividad, es necesario adoptar un enfoque conservador y tener un calentamiento de dominio similar a un calentamiento que se le da a las direcciones IP. El presente documento muestra algunas de las prácticas que son necesarias seguir para evitar inconvenientes al momento de hacer envíos de correo electrónico.

2.1. ¿Qué esperar?

Es posible que encuentres algunos problemas de capacidad de entrega, especialmente durante las dos primeras semanas al haber iniciado las actividades de envío de E-mail Marketing. Esto sucede porque un nuevo dominio siempre necesita crear buena reputación. Aunque las IP de tu proveedor de E-mail estén previamente calentadas, es necesario que tu dominio adquiera una reputación, recuerda que, en el negocio del E-mail Marketing, en la mayoría de las veces, un dominio “Nace culpable hasta que demuestre lo contrario”.

Algunos servidores que reciben buzones tomarán la decisión de colocar tus correos electrónicos en la carpeta de “Correo No Deseado” para ver si los suscriptores los rescatan y los etiquetan como “No Spam”. En los primeros envíos, es necesario demostrar que los destinatarios quieren de verdad recibir correos electrónicos desde ese dominio remitente, es por eso por lo que se hace necesario que, en los primeros envíos, el correo electrónico tenga una buena tasa de apertura.

En este aspecto, la elección de un proveedor de Email Marketing es clave y uno de los criterios de mayor peso. Es necesario una plataforma sólida y con un historial de buena reputación ante los auditores de spam. De nada

sirve seguir los pasos para calentar un dominio si las IP remitentes no tienen una buena reputación de envío.

En promedio, la construcción de una reputación de envío en un dominio lleva aproximadamente 40 días. Puede tomar más tiempo dependiendo de:

1. Volumen de correo electrónico que está enviando.
2. Calidad de la lista de suscriptores.
3. ¿Con qué frecuencia envías correos?

2.2. Antes de calentar el dominio

1. Crea registros para solventar el marco de políticas de legitimación de remitente. Los registros especiales para mejorar la efectividad son registros de Texto en los DNS del dominio de tipo SPF y DKIM.

2. Revisa que el dominio no se encuentre en una lista negra por malos comportamientos previos. Para este paso puedes utilizar https://mxtoolbox.com/

3. Actualiza el registro WHOIS del dominio con información correcta y no uses un servicio de privacidad de dominio.

4. Configura un registro de intercambio de correo (MX) para el nuevo dominio para permitir el correo entrante.

5. Asegúrate de que tus suscriptores tengan un mecanismo para darse de baja y que tengan la posibilidad de retroalimentar sus quejas. Nuestra solución este aspecto lo tiene resuelto.

2.3. Recomendaciones

Las siguientes son Recomendaciones para empezar con el calentamiento de tu dominio:

1. Para empezar a calentar tu dominio, consigue una base de destinatarios de confianza (30 a 100 con direcciones personales, empleados, amigos, etc.) que incluya varios proveedores de correo (Gmail, Yahoo, Hotmail, etc.) y envía una campaña con el mismo contenido que se espera enviar a futuro. Después de esto, solicita a todos los destinatarios que abran el mensaje, que den clic en el correo y si llega a Spam, que lo marquen como “No Spam”.

2. Luego del paso 1, espera tres días para empezar con envíos de 2.000 a 4.000 suscriptores.

3. El envío debería ser a una lista variada. Un mismo dominio dentro de los destinatarios no debería superar el 40% de la base.

4. Si no puedes dirigirte a proveedores de buzones específicos, comienza con un volumen de 2.000 suscriptores totales.

5. Duplica el volumen de envío cada tres o cuatro días hasta que alcances tu volumen máximo diario.

6. No envíes campañas más de una vez a la misma lista en menos de una semana. Esto aumenta los reportes de Spam. Los envíos diarios deberían hacerse a listas diferentes.

7. La base de correos debe ser una base que asegure una efectividad alta en aperturas, mínimo del 50%. Por esto es mejor dirigirse a suscriptores activos al principio. La participación positiva de los suscriptores ayuda a generar confianza en el nuevo dominio de parte los proveedores de buzones.

8. Los envíos diarios calientan más rápido que los de periodicidad semanal, quincenal, etc.

9. Es probable que AOL, Outlook, Yahoo y Gmail requieran un periodo de calentamiento más prolongado.

10. Pausa el calentamiento si los resultados no cumplen con las expectativas. El calentamiento de un nuevo dominio no es una ciencia exacta, por lo que es importante monitorear el rendimiento, pausar el calentamiento, solucionar problemas si ocurren y empezar de nuevo.

11. Si tu lista de contactos proviene de suscripciones de tu sitio web o empresa, asegúrate de usar un proceso de suscripción Double Opt In o envía un mensaje desde nuestra plataforma inmediatamente después de la suscripción. Esto aumenta significativamente las probabilidades de que el próximo mensaje llegue a bandeja de entrada.

12. El filtro de Spam es distinto para cada destinatario, aun si está dentro del mismo proveedor. Es por eso por lo que lo mejor al iniciar el proceso de E-mail Marketing es hacer varios envíos pequeños y segmentados (Recomendaciones 1 y 2), luego de unas semanas podrás realizar envíos que superen los 50 mil envíos.

13. Si tu lista de contactos es comprada, adquirida de algún evento, no

validada, minada de internet o creada de forma artificial, lo más seguro es que todos los mensajes lleguen a Spam, aun si tiene los procesos de autenticación correctos. Es por eso que desestimamos de cualquier manera la compra o adquisición no correcta de base de destinatarios.

14. Por ley de protección de datos, enviar mensajes a destinatarios que no autorizaron previamente es ilegal, (al hacer envíos con la compañía aceptas que tu base tiene autorización previa para ser contactada y que es necesario el cumplimiento obligatorio de CAN SPAM ACT 2003). Entendemos que las prácticas de E-mail Marketing en muchos casos no contienen destinatarios autorizados, es por eso que, si quieres que tus correos lleguen a bandeja de entrada, debes seguir todas las recomendaciones descritas en el presente documento.

15. El envío de mensajes de E-mail Marketing es un proceso delicado que sirve para aumentar ventas y presencia de marca, sin embargo, solo es efectivo si se hace con paciencia y siguiendo nuestras recomendaciones.

16. Los proveedores de correo guardan un registro de las direcciones IP y servidores desde donde se envían mensajes de cada dominio, por lo cual un cambio abrupto de proveedor de E-mail Marketing o el uso de múltiples puede afectar la reputación de un dominio.

2.4. Monitoreo

Después de tener buenas prácticas establecidas y actividades con resultados específicos, es necesario medir las acciones previamente realizadas para el calentamiento del dominio. Para eso, recomiendamos seguir las siguientes pautas:

1. Incluye tu correo electrónico en la base de envío para ver la efectividad.

2. Solicita un monitoreo periódico y notificación de tu dominio, esto lo puedes hacer en https://mxtoolbox.com/

3. Revisa las estadísticas en la reportería expuesta por la plataforma. Si tu gestión se está llevando de manera correcta, las estadísticas deben mejorar.

4. Monitorea constantemente el estado de tu base de datos y de los nuevos ingresos. Para esto, utiliza el Validador de Correos que ponemos a su disposición.

El proceso de calentamiento para construir la reputación de envío de tu nuevo dominio, en promedio, puede tardar 40 días. Construir una reputación de envío con un proveedor de buzones puede ir más rápido o dependiendo de las prácticas de envío y la reputación de envío.

El proceso de calentamiento será más fácil si utilizas direcciones IP con buena reputación de envío (esto lo garantiza nuestra solución) y que estén registradas con listas blancas, ya que la confianza de la dirección IP ayuda a establecer la confianza con el nuevo dominio. Si ya tienes una mala reputación de envío y no sigues las mejores prácticas de marketing por correo electrónico, es probable que los problemas de capacidad de entrega continúen, independientemente del cambio de dominio

3. Buenas prácticas de Email

3.1. Buenas prácticas técnicas

3.1.1. Listas negras

Las Listas Negras son bases de contactos en donde figuran todas aquellas direcciones de correo electrónico, IP o dominios cuyas comunicaciones se rechazan por no considerarlas legítimas o de confianza. Los usuarios también pueden colaborar en esta clasificación, ya que cada vez que un usuario final se "desuscribe", clasifica un email como spam o plantea una queja que contribuye a nutrir esta Base. Esto podría derivar como posible "efecto secundario" que una dirección de correo legítima sea considerada como SPAM.

La solución de email se encarga diariamente de cuidar la reputación de tus IP. Este proceso se establece con un continuo monitoreo y rotación con inteligencia artificial automática de una gran cantidad de IPs "calentadas" y verificadas frente a los servidores destinatarios de correos electrónicos (Gmail, Hotmail, Yahoo, Live, Outlook etc.)

3.1.2. Reputación de IP

En este aspecto, la elección de un proveedor de Email Marketing es clave y uno de los criterios de mayor peso. Es necesario una plataforma sólida y con un historial de buena reputación ante los auditores de spam.

Además de nuestras buenas prácticas, filtrar tu base de contactos utilizando nuestro Validador de E-mail te ayudará mucho para conseguir buenos resultados.

3.1.3. Historial de actividad de la IP

Los guardianes (creadores y dueños de listas negras) llevan un registro de historial de envíos de los remitentes, recopilando la frecuencia de envío, la velocidad, sanciones anteriores, etc. Teniendo en cuenta este historial, se clasifican los emails en válidos o no.

*Es importante evitar y desestimar rotundamente la compra de Base de contactos, ya que además de ser considerada como una mala práctica, derivará en malas métricas y quejas o denuncias por parte de los destinatarios. Esto definitivamente causa inclusión de IPs y Dominios en listas negras.

3.1.4. Volumen y velocidad de envío

Las campañas enviadas a una base de contactos muy grande y a velocidades rápidas podrían impactar negativamente en los filtros anti-spam. Por otro lado, el número de mails enviados de forma repetitiva a un mismo dominio o a un destinatario en particular puede ser considerado como un ataque hacia la compañía o empresa.

Puedes estar tranquilo, nosotros tenemos un sistema de entrega inteligente que dosifica el envío de correos electrónicos para evitar en este aspecto filtros anti-spam y malas prácticas.

3.1.5. Legitimación de remitentes

Es muy importante garantizar la autenticidad de los envíos; es una forma de demostrar que el email ha sido enviado por la persona que afirma ser el remitente. Se utiliza dos estándares aceptados por la mayoría de los ISP (estos utilizan una o las dos para chequear la legitimidad):

DKIM (DomainKeys Identified Mail).

SPF (Sender Policy Framework).

Los filtros verifican si el remitente se encuentra en el listado de direcciones del destinatario. Si no lo encuentra, probablemente dirigirá el correo a la carpeta de spam o no lo entregará.

Importante: Al hacer un envío debes tener en cuenta que nuestros servidores hayan sido "autorizados" para enviar correos en nombre de tu dominio. Este es un aspecto técnico asociado a la configuración de los DNS de las partes involucradas. Sin esta configuración, no debes hacer envíos.

3.1.6. Archivo adjunto

Adjuntar un archivo no es considerado una buena práctica y perjudica el pasaje del email frente a los filtros.

Recomendaciones: Subir el documento al servidor e insertar el link de descarga en la pieza HTML; así sólo los destinatarios interesados descargarán dicho adjunto.

3.1.7. Links rotos y sin seguridad

Los enlaces rotos son links de un sitio web que ya no sirven, bien porque ya no existan o porque la dirección es incorrecta.

Estos enlaces llevan directamente al usuario a una dirección HTTP 404, junto con un mensaje informativo de "dirección no encontrada" o bien "la página web que está solicitando no está disponible en el momento".

Estos enlaces defectuosos junto con enlaces sin certificado de seguridad "http:" afectan significativamente la efectividad de los correos. Es por eso por lo que debes evitar tener enlaces rotos o sin certificado de seguridad en tus correos electrónicos.

3.2. Buenas prácticas en marketing

3.2.1. Segmenta a tus suscriptores

Las empresas deben adoptar en su modelo de negocio la estrategia de "**Customer Centricity**", invirtiendo tiempo en segmentar sus bases de datos, teniendo en cuenta parámetros útiles para hacer llegar el contenido adecuado al usuario. Lo anterior evita que el usuario pierda el interés en la marca, no se inscriba, o cause baja como suscriptor.

Segmentos sugeridos: Temática, periodicidad de envío, edad, ubicación, género, última compra, historial de consumo, etc.

3.2.2. Personaliza al máximo

Aunque E-mail Marketing es una técnica de comunicación masiva, a todo el mundo le gusta sentirse especial y recibir un correo electrónico personalizado, con datos personalizados. Es por esto que tu correo electrónico debe estar orientado al usuario lo más que puedas.

Personalizaciones recomendadas: Nombre (en el asunto y en el saludo), personaliza por género (puedes enviar dos campañas), personaliza por edad, cuidad, preferencias.

3.2.3. Diseño responsive

Asegúrate de que tus emails se ven perfectos en todos los dispositivos.

¡No te preocupes por este ítem! Como proveedor de envío de correos electrónicos proporciona un diseño responsive en sus plantillas. Con este diseño tus usuarios pueden ver tus correos electrónicos en smartphones, tablets, computadores, etc.

3.2.4. Menos es más, Emails sencillos

En la mayoría de los casos, los correos (Newsletters) más sencillos funcionan mucho mejor que los que están llenos de imágenes, colores diferentes, diseños complicados…

Menos es más: Tu email tiene que ser sencillo. Cuanto menos se parezca a las típicas newsletters (esas que están maquetadas a diferentes columnas, repletas de imágenes enormes o con encabezados), mucho mejor.

Nuestra recomendación es la siguiente:

3.2.5. Evita palabras SPAM

Palabras Spam: Gratis, regalo, mejor precio, promoción especial, descuento, rebajas, oferta, clic aquí, gana dinero, compra, mejor precio, menor precio, por solo, llama gratis, inversión, 50% menos, ¿por qué pagar más?, elimina tu deuda, ya, hazlo ya, comienza hoy, por tiempo limitado, visto en TV, pierde peso.

Debido al historial de malas prácticas que ha tenido el correo electrónico en el mundo, estas palabras son catalogadas como Spam y generan menor efectividad en tus campañas.

Elige un remitente antispam. En la mayoría de los casos debes evitar errores como info@, noreply@, noresponder@, comunicacion@.

3.2.6. Añade un CTA

Todos los correos electrónicos que envíes deben tener un objetivo. Para esto debes invitar al usuario a que realice una acción.

CTAs recomendados: Leer un post (artículo), descargar un documento en PDF, redireccionar a un vídeo, comprar un producto, apuntarse a una conferencia, pedir más información, suscribirse, etc.

3.2.7. Busca las mejores horas (Haz pruebas)

La hora en que envías tus emails afecta mucho a la tasa de apertura. Tienes que descubrir qué horario es el más adecuado para enviar tus newsletters. Cada caso, segmento, industria, objetivo en correo electrónico tiene horas diferentes con mayor efectividad. Debes saber identificarlas para encontrar el momento óptimo para entregar tus mails.

Haz pruebas, mide, analiza y comprueba qué hora del día (y qué día de la semana) es el que tus suscriptores abren más emails, hacen más clics y completan más conversiones.

3.2.8. Enlace para darse de baja

Todos tus emails deben incluir un enlace para que los suscriptores se puedan dar de baja siempre que quieran.

*La solución de email te soluciona automáticamente este paso.

3.2.9. Prueba, envía, mide y analiza

Si quieres que tus campañas de Email Marketing funcionen a la perfección, debes analizar todos y cada uno de los correos electrónicos que envíes.

La secuencia debe ser esta: haz pruebas de tus correos > realiza el envío > mide todos los factores > analiza los resultados.

*Solo así podrás descubrir qué funciona y qué no funciona