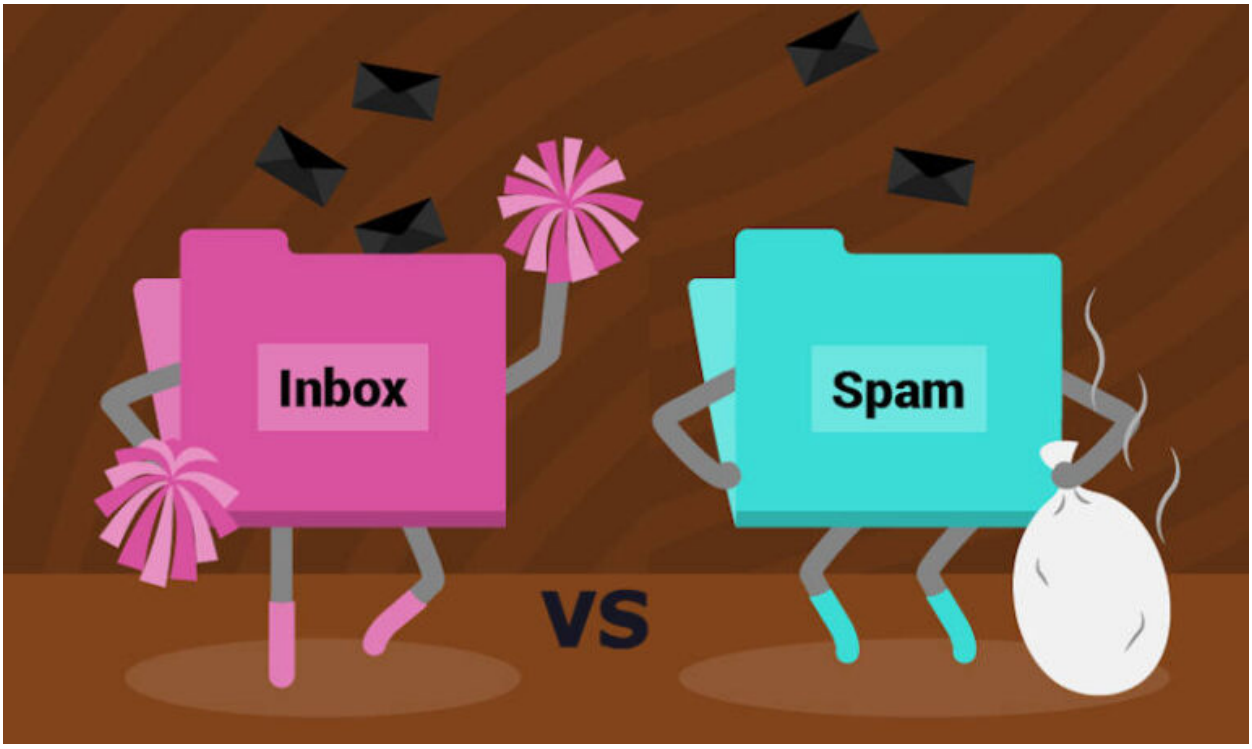
¿Por qué mis email llegan a SPAM o no llegan?

escrito por Andy Garcia | 24/03/2024



A pesar de los mecanismos anti-spam seguimos recibiendo SPAM y **algunas veces nuestros mensajes legítimos son los que llegan a la bandeja de correo no deseado** o incluso no llegan a su destino… ¿qué podemos hacer para solucionar este problema?

Si quieres estar seguro de que el 99,99% de los e-mails que envías de forma legítima, desde tu e-mail con tu propio dominio, llegan a su destino sigue leyendo.

> *Cuando digo «enviar de forma legítima» me refiero a un **e-mail único** (sin virus) enviado a un **destino único** o a pocos destinatarios en copia, usando un cliente de correo electrónico, porque para envíos masivos autorizados existen otras herramientas.*

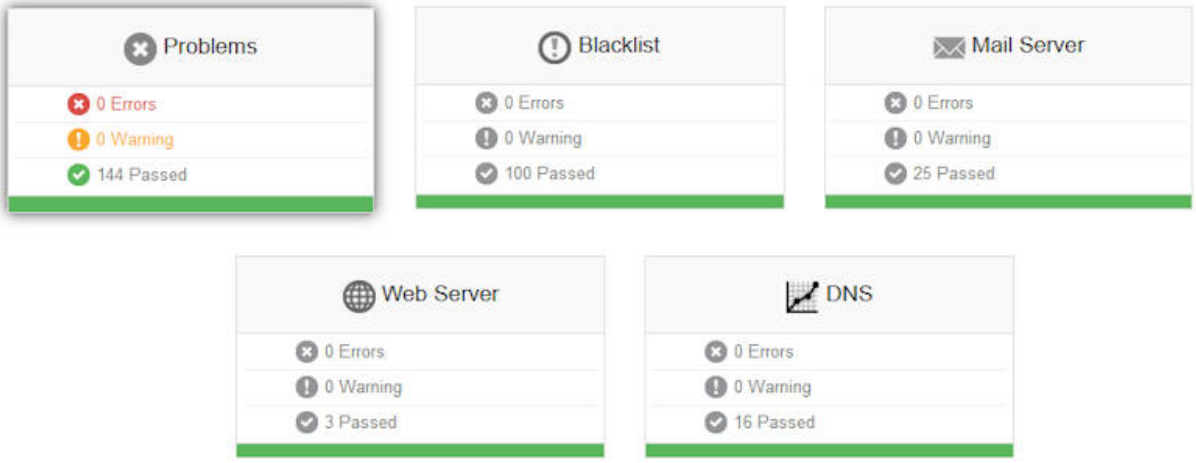
¿Cómo podemos hacer una prueba de envío para saber las posibilidades de que nuestro e-mail sea detectado como spam?

1. Entrar en: https://www.mail-tester.com/.
2. Copiar la dirección de e-mail que nos muestra *mail-tester.com* en pantalla.
3. Enviar un e-mail de prueba desde nuestra aplicación de correo a la dirección anterior.
4. Volver a *mail-tester.com* y pulsar el botón «*A continuación comprueba tu puntuación*».

Si no obtienes un 10/10 (como en el ejemplo de la imagen superior) tienes un problema que tendrás que arreglar para conseguir que tus comunicaciones lleguen a la bandeja de entrada de tus destinatarios de correo electrónico.

¿Cómo podemos verificar la salud del servidor de e-mail y obtener pistas de posibles problemas?

- Indica tu dominio (o el de tu competencia, cliente, familiar, vecino, amigo, etc…) en el siguiente servicio online: https://mxtoolbox.com/emailhealth pulsando a continuación el botón correspondiente.



Obviamente, antes de comprobar los mecanismos para detectar SPAM (los veremos más abajo, en este mismo post), necesitas una correcta configuración de correo electrónico (usando protocolos de seguridad SSL), unas buenas intenciones (me refiero a no enviar correos masivos) y no enviar virus (tener un anti-virus puede ayudar).

¿Cuál son los servidores de e-mail y puertos correspondientes usando SSL?

- Como servidor de correo entrante y saliente puedes usar la IP de tu servidor, tu nombre de dominio o **mail.tudominio.com** (para ambos servidores) o, pop3.tudominio.com (para el correo entrante) y smtp.tudominio.com (para el correo saliente), dependiendo de como tengas configuradas las zonas DNS.

> *Yo prefiero crear en las DNS un registro A o CNAME con mail, por si alguna vez necesito tener el e-mail en una máquina diferente a la web, poder cambiar la IP de cada servicio desde los registros correspondientes.*

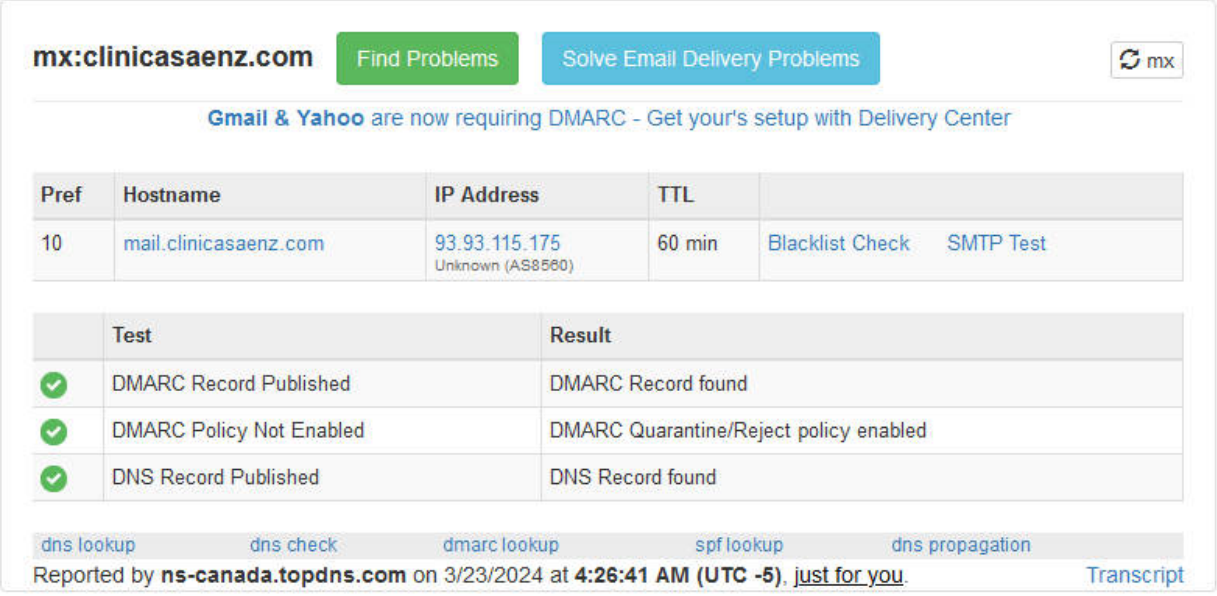
- Para el correo entrante (**IMAP** sobre SSL): Puerto estándar: 993 – Puerto alternativo: 585
- Para el correo entrante (**POP3** sobre SSL): Puerto

estándar: **995** – Puerto alternativo: 9950
- Para el correo saliente (**SMTP** sobre SSL): Puerto estándar: **465** – Puerto alternativo: 587

Normalmente se usa el servidor POP3 para el correo entrante y SMTP para el saliente, así que puedes omitir el IMAP, salvo que explícitamente lo uses, si tienes dudas no lo usas. Los puertos alternativos no están disponibles por defecto, salvo que tu servidor lo tenga explícitamente activado siempre tienes que usar el puerto estándar.

¿Cómo comprobar si mi servidor de correo electrónico está correctamente configurado?

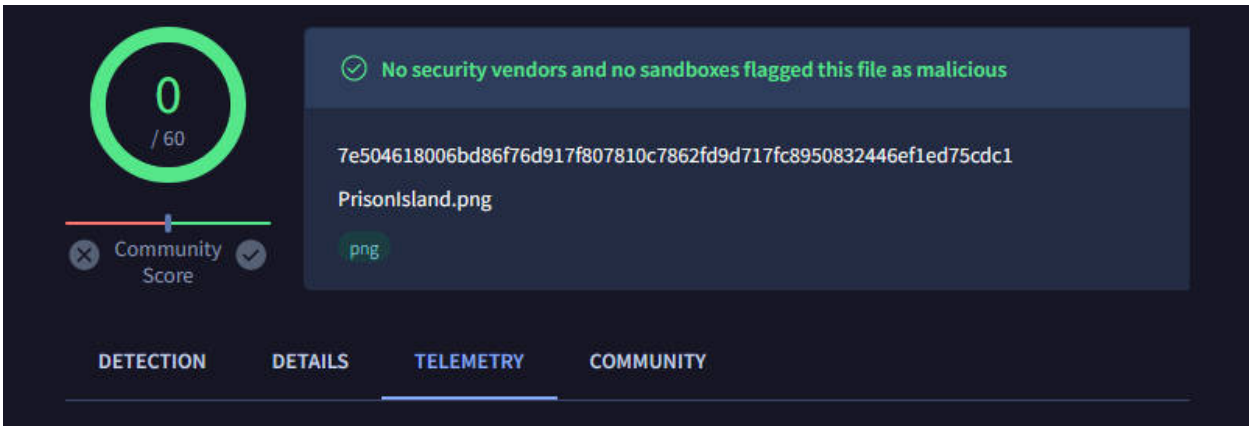
- Indicando tu nombre de dominio aquí: https://mxtoolbox.com/ y a continuación pulsa el botón «*MX Lookup*».



¿Cómo comprobar si un archivo que voy a adjuntar tiene virus?

- Comprueba la integridad de tus archivos usando tu propio anti-virus o el siguiente anti-virus online:

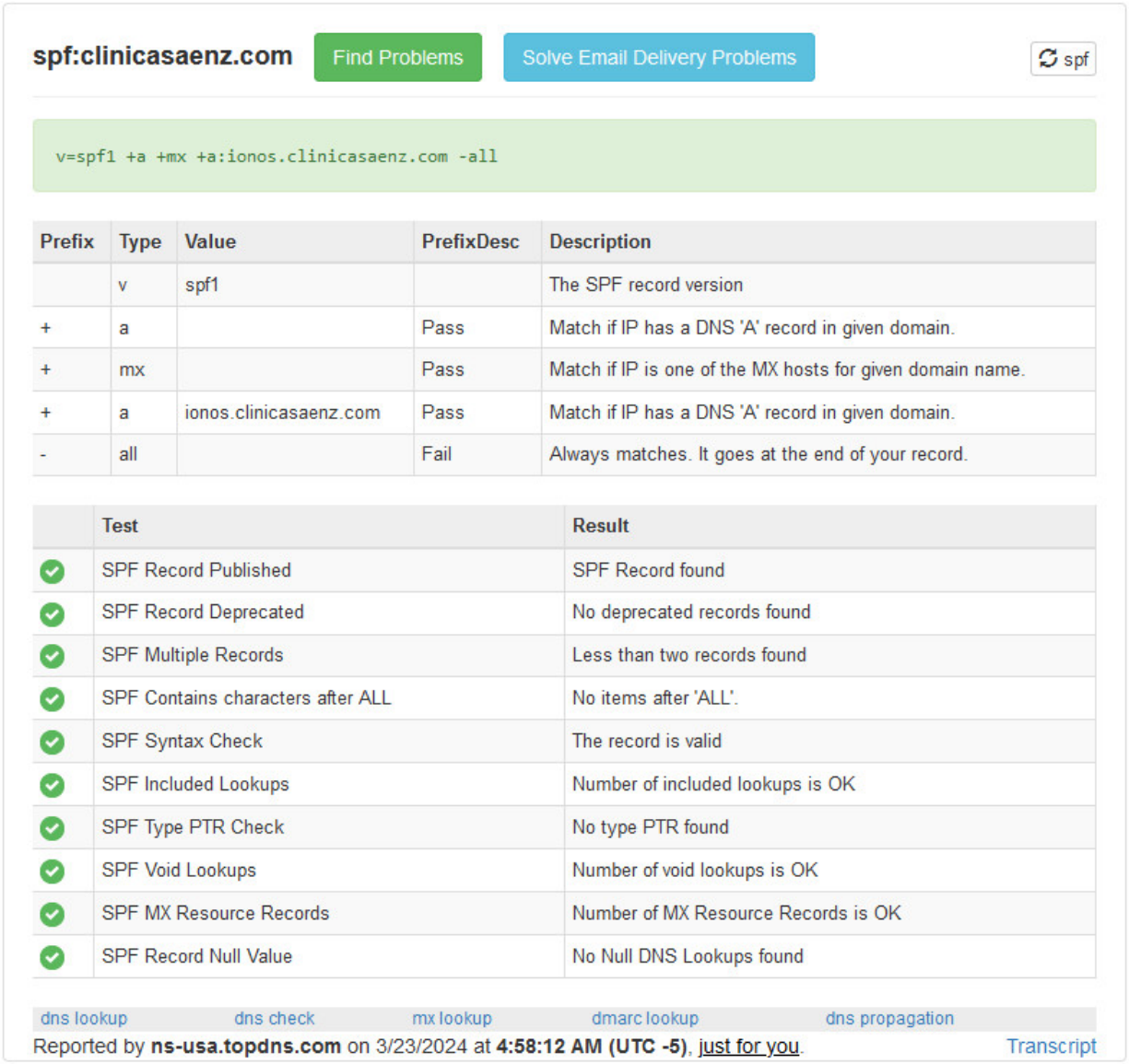
https://www.virustotal.com/.



¿Cómo hacer que mis e-mails lleguen a la bandeja de entrada y no a SPAM?

A partir de ahora, vamos a hablar de los mecanismos para detectar SPAM, o mejor dicho de lo que tú dominio tiene que tener para que tus correos legítimos no sean nunca o casi nunca detectados como SPAM, al menos no por una mala configuración.

- Tienes que tener un registro TXT en tus DNS con **información sobre SPF**, para comprobarlo indica tu dominio aquí: https://mxtoolbox.com/SuperTool.aspx pulsando el **botón SPF Record Lookup** (fíjate que antes de pulsar el botón tienes que desplegar la opción correcta usando la flecha hacia abajo).



spf:clinicasaenz.com Find Problems | Solve Email Delivery Problems | spf

```
v=spf1 +a +mx +a:ionos.clinicasaenz.com -all
```

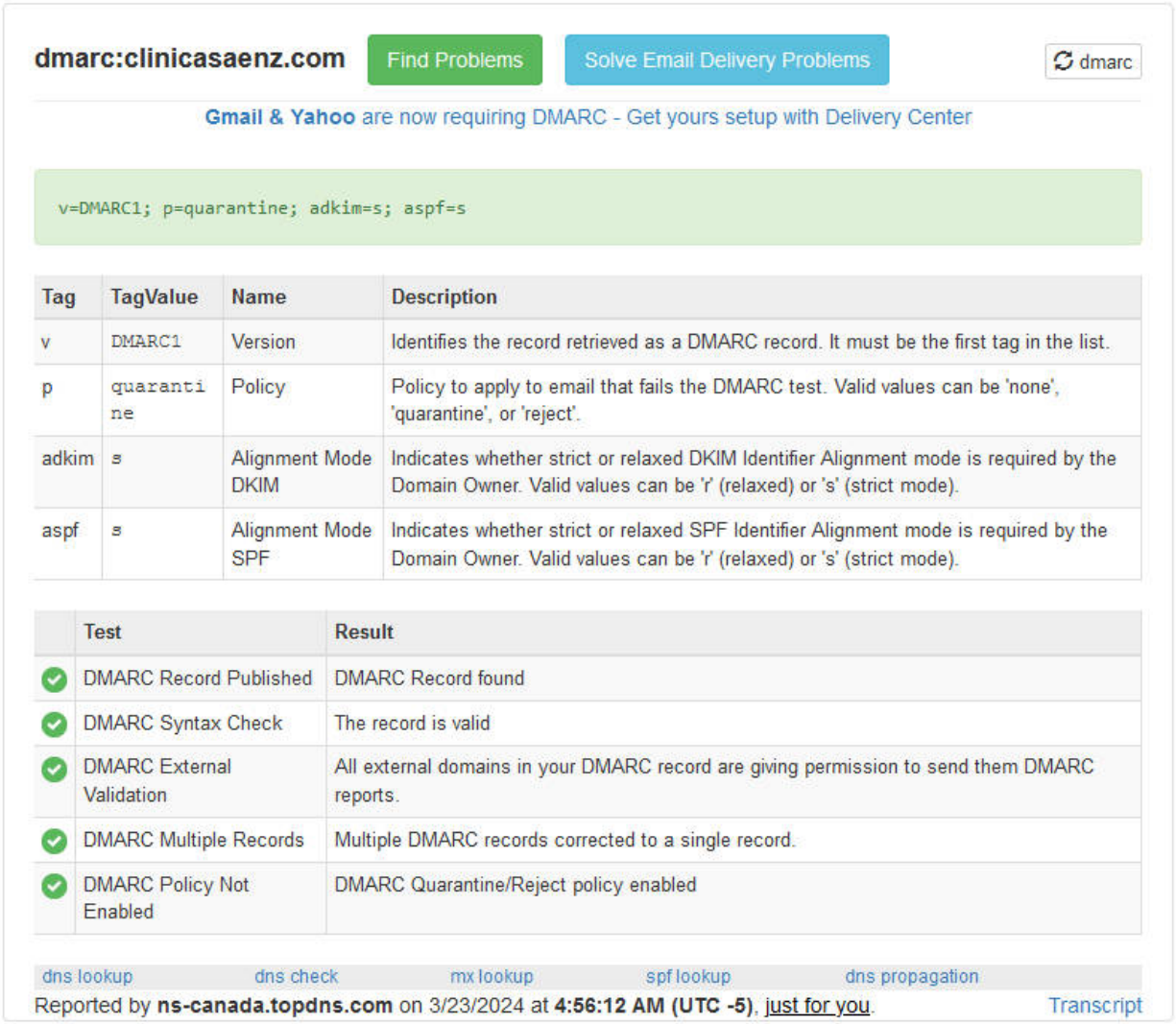
Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	a	ionos.clinicasaenz.com	Pass	Match if IP has a DNS 'A' record in given domain.
-	all		Fail	Always matches. It goes at the end of your record.

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found

dns lookup | dns check | mx lookup | dmarc lookup | dns propagation

Reported by **ns-usa.topdns.com** on 3/23/2024 at **4:58:12 AM (UTC -5)**, just for you. Transcript

- Tienes que tener un registro TXT en tus DNS con **información sobre DMARC**, para comprobarlo usa la misma herramienta anterior, pero pulsando el **botón DMARC Lookup**.



dmarc:clinicasaenz.com Find Problems Solve Email Delivery Problems dmarc

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

```
v=DMARC1; p=quarantine; adkim=s; aspf=s
```

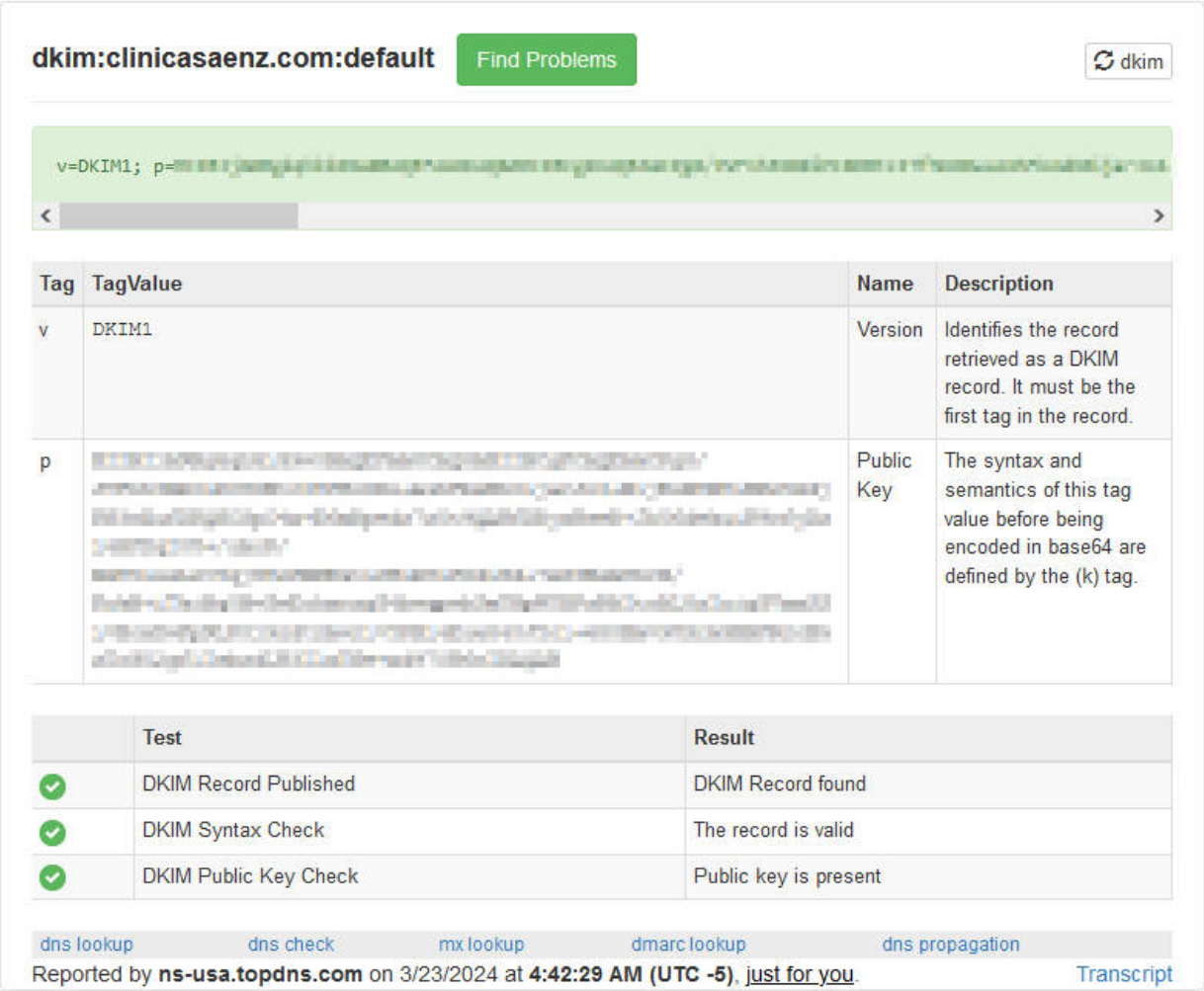
Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	quarantine	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
adkim	s	Alignment Mode DKIM	Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
aspf	s	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

dns lookup dns check mx lookup spf lookup dns propagation

Reported by **ns-canada.topdns.com** on 3/23/2024 at **4:56:12 AM (UTC -5)**, just for you. Transcript

- Tienes que tener un registro TXT en tus DNS con **información sobre DKIM**, para comprobarlo usa la misma herramienta anterior, pero pulsando el **botón DKIM Lookup** y en lugar de poner simplemente el dominio tendrás que poner el dominio seguido de 2 puntos y el nombre del registro TXT, en caso de duda prueba con default que es la opción más común, es decir «*dominio.com:default*«.

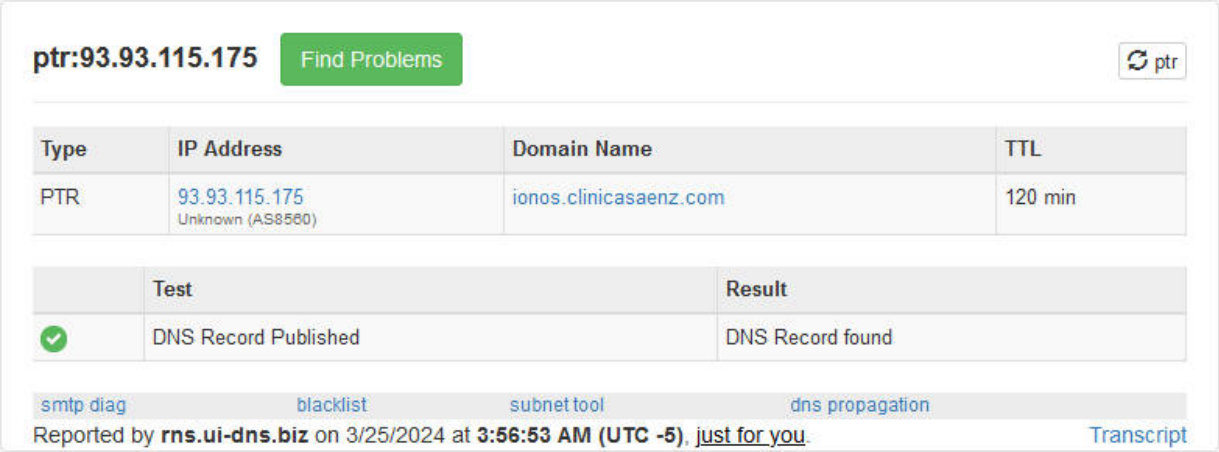


OJO: la clave DKIM contiene una clave privada que usada con malas intenciones podría permitir que alguien la usara para enviar correos en tu nombre desde tu dominio, por ese motivo conviene no revelarla públicamente y por eso está difuminada en la imagen anterior.

Y por último… ¿cómo configurar y comprobar la IP inversa o PTR?

- Para configurar la IP inversa y asociar la IP de tu servidor a su nombre de dominio: cada proveedor de hosting te permite hacerlo de una forma diferente, algunos te piden que les mandes el nombre de tu servidor e IP y ellos se encargan de configurarlo.
- Para comprobar la IP inversa: puedes entrar en

https://mxtoolbox.com/SuperTool.aspx, introducir tu IP y pulsar el botón, seleccionando antes la opción «*Reverse Lookup*«.



Hasta aquí los aspectos más importantes que tienes que tener en cuenta para **que todos tus e-mails lleguen correctamente a la bandeja de entrada de su destinatario**.

Si has llegado hasta aquí, has hecho las comprobaciones y está todo perfecto puedes estar tranquilo, pero si has obtenido mensajes de error o puntuaciones insuficientes significa que algunos de tus correos electrónicos no van a llegar a la bandeja de entrada de su destino, llegarán a la bandeja de SPAM (correo no deseado) o incluso no llegarán.

En tal caso, ya tienes lo más difícil de conseguir, el diagnostico, ahora sólo necesitas arreglar el problema, si necesitas más ayuda o tienes algo que aportar puedes usar la zona de comentarios, que para eso está.