ASEGURAMIENTO SERVICIOS OPERATIVOS TI

COLCERT AD 0429-015

TLP:CLEAR

Usurpación de cuentas de correo y mensajes phishing hell

El auge de mensajes de correo phishing en donde se pretende suplantar la imagen, marca, buen nombre y reputación de una entidad para que así el señuelo sea creíble, crece constantemente en la comunicación digital. Las entidades, usuarios y funcionarios se fían del supuesto remitente y firma ubicada en el pie de pagina del mensaje para abrirlo o no, visitar un enlace en la web y descargar un archivo adjunto.

Es ahí donde la perspicacia de los ciberdelincuentes actúa al emplear servicios como Fake Mailing o servicios de envío de correos falsos; en donde se intenta suplantar la identidad del remitente inclusive con un dominio legítimo en la caja “from”; esto se convierte en un tema de gran envergadura en materia de seguridad de la información, tomando en cuenta que casi el 80% de éxito de la afectación de ransomware en las entidades es a través del correo electrónico.

Debilidad identificada:

Los ciberdelincuentes conocen las medidas de concienciación del actual funcionario de la era digital, sabe que hay una confianza acerca de un sitio HTTPS y para este caso; la credibilidad en un remitente con dominio por ejemplo, gov.co; a continuación se detalla un estudio experimental en donde se pretende adentrarse a las herramientas Fake Mailing existentes y corroborar que ocurre al remitir este tipo de mensajes falsos a cuentas de correo corporativas como Microsoft y gratuitas como es el caso de Gmail. Se observará si el mensaje phishing llega al buzón de entrada o en la carpeta de no deseados, para así comprobar la configuración de los protocolos de autenticación SPF, DKIM y DMARC.

En primera medida es importante dar a conocer que el Fake Mailing es de fácil manejo, no requiere de ninguna experticia o conocimiento técnico, también es gratuito y online, no se necesita de una infraestructura adicional ya sea física o de software para usarla. Este alcance supone una gran oportunidad para la estructuración y remisión de un mensaje phishing.

En la figura 1, se observa cómo redactar el mensaje a través de una de estas herramientas, posee atributos como la capacidad de adjuntar archivos con características de RAT, enlaces que bien pueden ser manipulados por el ciberdelincuente y un presunto legítimo remitente. Estas opciones junto con un mensaje de urgencia y que llame la atención del usuario, es un cebo perfecto para que la víctima haga clic en el enlace o adjunto.

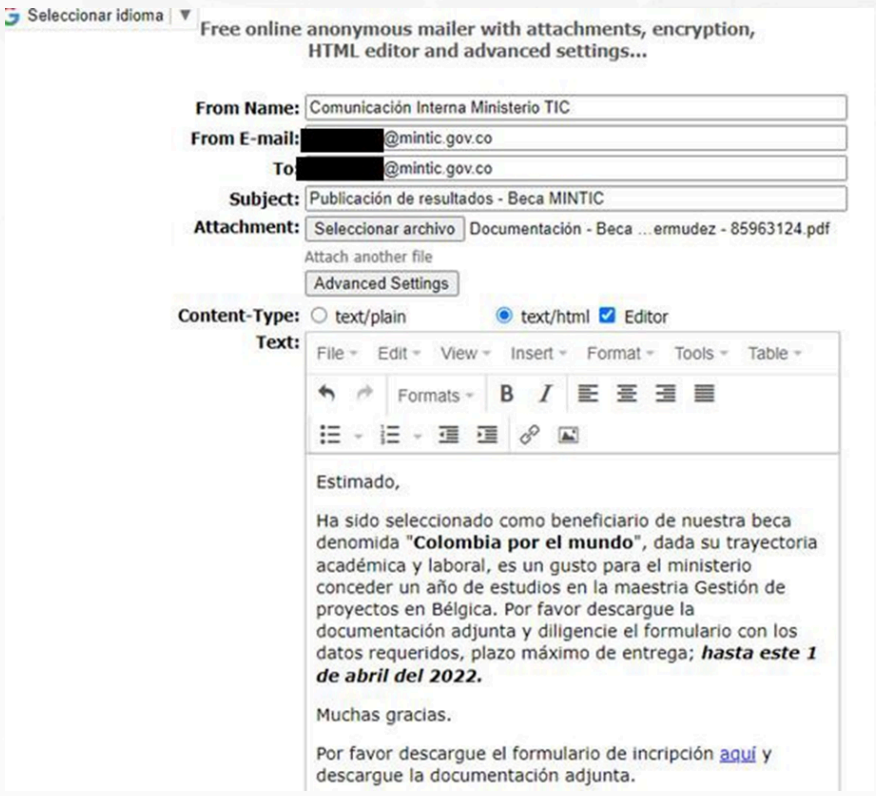


Figura 1. Estructura de un mensaje desde herramienta Fake Mailing.

La cuenta de correo a la que se intentó suplantar le fue enviado un mensaje en donde se informa acerca de este suceso, dicho mensaje llega a la carpeta de no deseados. Dentro del comunicado se observa el enlace verdadero a donde redirige el texto hipervinculado “aquí” el cual es de procedencia maliciosa.

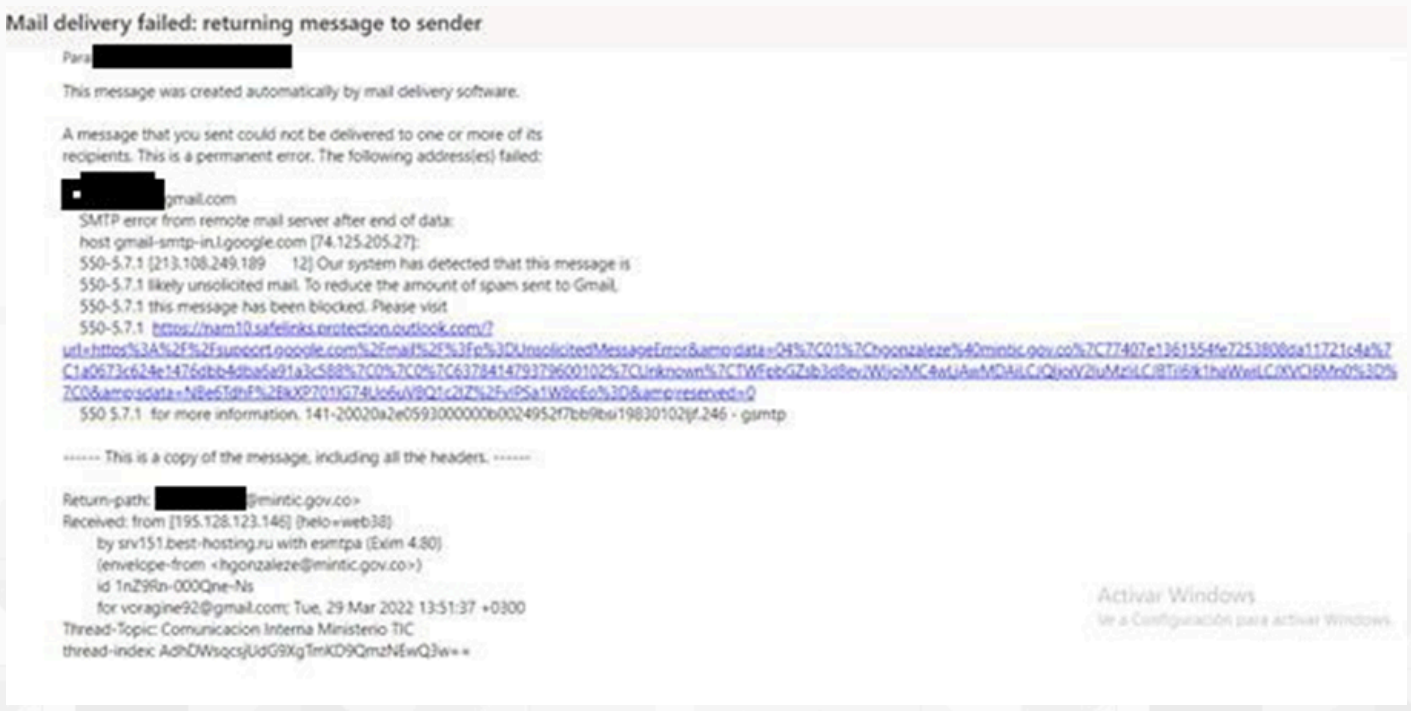


Figura 2. Mensaje al remitente suplantado.

Se adjuntan los encabezados del mensaje en donde se pueden detallar características como la IP pública del servidor de envío, con AS 47196 geolocalizado en Rusia.

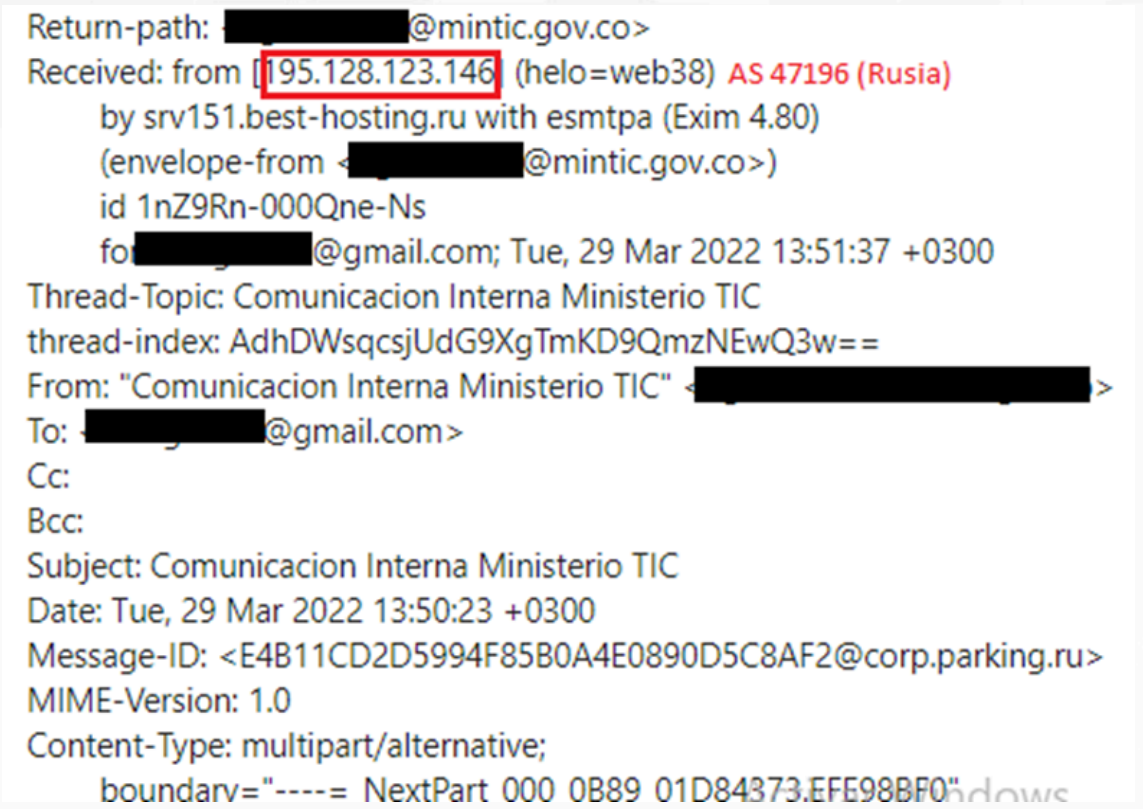


Figura 3. Encabezados del mensaje phishing.

Mitigaciones puntuales en servidor de correo electrónico:

Existen tres protocolos que ayudan a la comprobación de IP remitentes y dominios autorizados para enviar mensajes a nombre de la entidad; se habla concretamente de SPF, DKIM y DMARC.

Podemos comparar estos tres protocolos como el firewall del correo, en donde se valida si un dominio y remitente es seguro, de ser seguro, el mensaje es enviado directamente al buzón de correo, de lo contrario, es enviado a carpeta spam o no deseado. Es importante que las entidades realicen las configuraciones pertinentes en sus servidores de correo para estos tres protocolos.

SPF o Sender Policy Framework es una protección contra las falsificaciones de cuentas de correo electrónico, identificado el remitente legítimo y de esta forma evita que alguien más intente enviar mensajes en su nombre.

El SPF se define en un archivo .txt distribuido de la siguiente forma:

- DNS del dominio de la entidad
- Identificador que es la IP del dominio
- El CNAME que es el alias del dominio
- MX que aloja los servidores que contienen los buzones de email
- Los registros txt que hacen referencia a los dominios personalizados de la entidad.

Desde el momento que se ingresa un dominio, ya se obtiene por defecto un registro TXT que es el del SPF, el cual es el antispoofing del dominio. Este TXT se copia y se pega en el registro DNS o el hosting.

El registro TXT de SPF debe tener esta apariencia según especificaciones de si existe la autorización de IP salientes, sistemas de correo electrónico de terceros, entre otros: **v=spf1 include:spf.protection.outlook.de -all**

ELEMENTO	SI USA...	¿ES COMÚN PARA LOS CLIENTES?	AGREGUE ESTO...
1	Cualquier sistema de correo electrónico (obligatorio)	Común. Todos los registros TXT de SPF comienzan con este valor	v=spf1
2	Exchange Online	Común	include:spf.protection.outlook.com
3	Solo Exchange Online dedicado	No es común	ip4:23.103.224.0/19 ip4:206.191.224.0/19 ip4:40.103.0.0/16 include:spf.protection.outlook.com
4	Solo para Office 365 Alemania y Microsoft Cloud Alemania	No es común	include:spf.protection.outlook.de
5	Sistema de correo electrónico de terceros	No es común	include:<domain_name> <domain_name> es el dominio del sistema de correo electrónico de terceros
6	Sistema de correo local. Por ejemplo, Exchange Online Protection y otro sistema de correo electrónico	No es común	Use uno de estos para cada sistema de correo adicional: ip4:<IP_address> ip6:<IP_address> include:<domain_name> <IP_address> y <domain_name> son la dirección IP y el dominio del otro sistema de correo que envía correos en nombre de su dominio
7	Cualquier sistema de correo electrónico	Común. Todos los registros TXT de SPF acaban con este valor	<enforcement rule> Puede ser uno de varios valores. Le recomendamos que use -all

Tabla 1. Parámetros en SPF. Fuente: Microsoft.

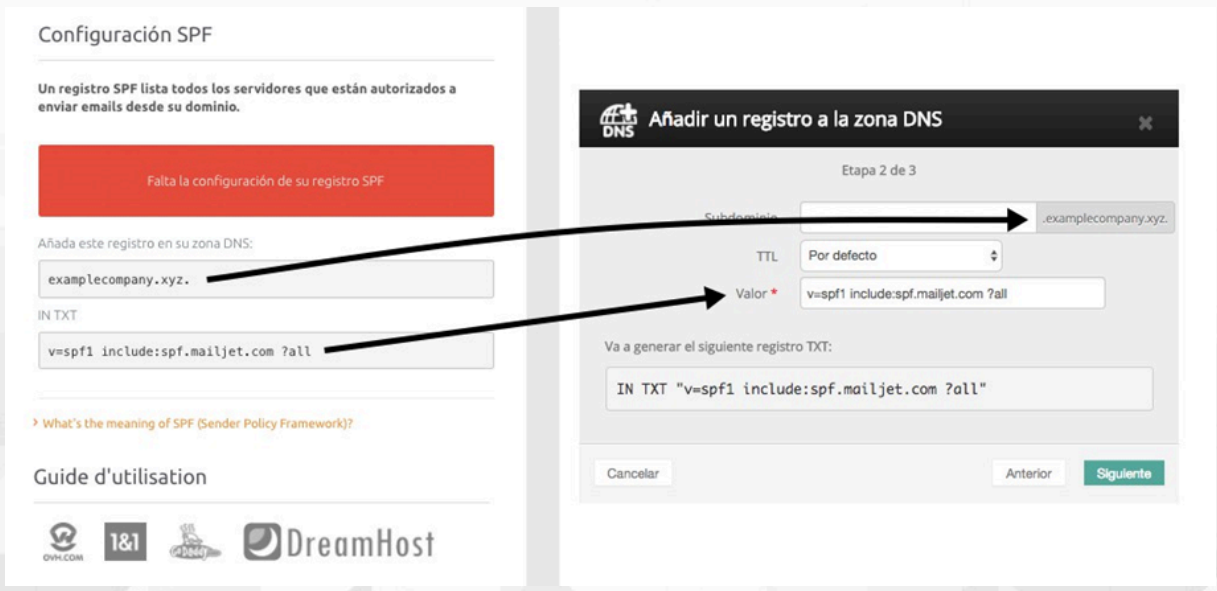


Figura 4. Inserción de txt de SPF en zona DNS del servidor de correo.
Fuente: Mailjet.

DKIM o Domain Keys Identified Mail, evita correos fraudulentos, hay una firma cifrada que se envía en el mensaje de correo; cuando el servidor destinatario lo recibe, pregunta al servidor DNS si ese servidor está autorizado para enviar esos correos, por ejemplo, si Gmail recibe un mensaje de un banco, Gmail pregunta al banco si está autorizado para recibir correos de ese servidor.

En primera medida se deben crear las llaves de registro CNAME. Si usa Microsoft, este proporciona un dominio por defecto, lógicamente se pueden agregar dominios personalizados. Para aplicar el DKIM, se usan dos llaves CNAME por cada dominio, cada una con un selector o apuntador.

Ejemplo CNAME RECORD

Host name	selector1._domainkey
Points to address or value	selector1-example-net-co._domainkey.example.onmicrosoft.com
TTL:	3600
Host name	selector2._domainkey
Points to address or value	Selector2-example-net-co._domainkey.example.onmicrosoft.com
TTL:	3600

Tabla 2. Registro DKIM

Se publican estas dos llaves del dominio example.net.co y se habilita, los cambios pueden demorar hasta 72 horas, cuando se encuentre operativo, se procede con los siguientes pasos si usa Microsoft: Diríjase a Seguridad y cumplimiento de office 365 - Administración de amenazas – directiva – DKIM Seleccione el dominio personalizado al que desea activar el DKIM (example.net.co) y habilite.

Figura 5. DKIM en zona DNS del servidor de correo.

Fuente: Mailjet

DMARC o Domain-based Message Authentication, Reporting & Conformance, permite autenticar el correo electrónico, garantizando que el mensaje proviene del dominio del cual indica venir. Si el remitente de un correo no tiene implementado el DMARC, el destinatario no tiene la certeza de que la identidad de este no esté siendo suplantada. Tiene diferentes formas de actuar al validar DMARC:

- Modo bloqueo: modo deseado, el correo no se recibe.
- Modo Cuarentena: el mensaje va a bandeja spam
- Modo none: solo a modo de reporte

Si el mensaje está validado por SPF Y DKIM, se dirige directamente al buzón del destinatario, pero si alguno de estos atributos falla; DMARC decide que hacer con el correo por medio de policy “p”.

_dmarc.example.net.co 3600 IN TXT "v=DMARC1; p=quarentine"

Ejemplo DMARC RECORD

Host name	_dmarc.example.net.co
Value	v=DMARC1; p=quarentine; pct=100
TTL:	3600

Tabla 3. Registro DMARC

pct= 100 (regla usada para el 100% de los correos, al 100% se les aplica la regla del DMARC).
p= especifica que directiva siga el servidor de recepción cuando se produce error en el DMARC.

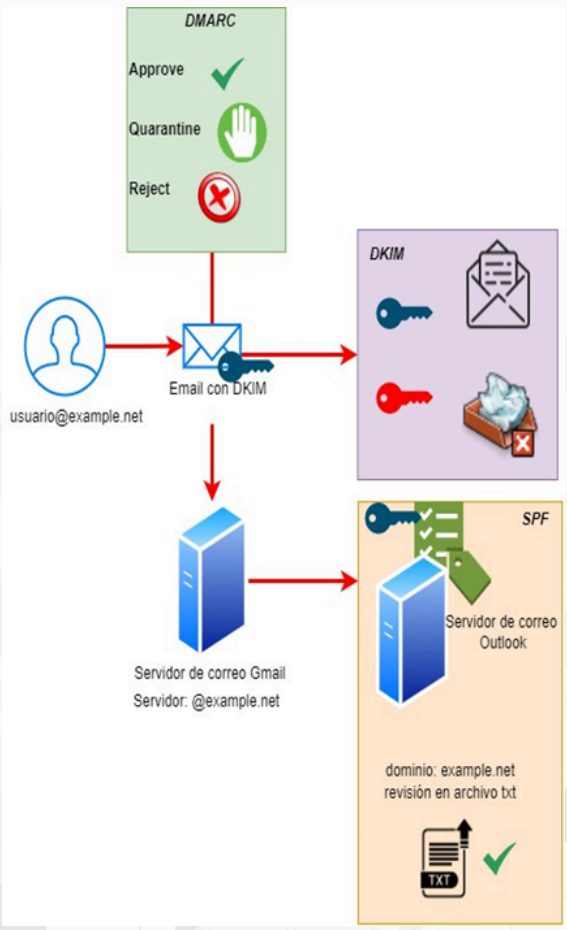


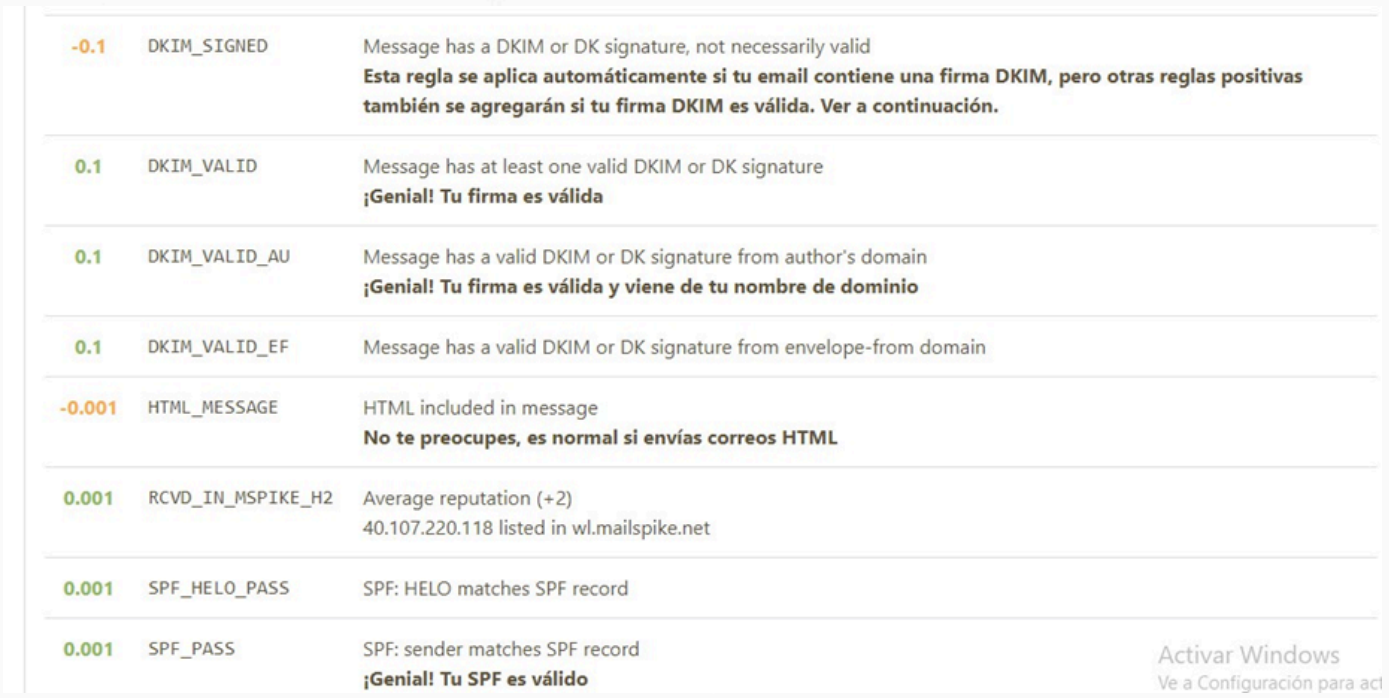
Figura 7. SPF,DKIM yDMARC

En la figura 7 se observa el accionar de los tres protocolos en el envío y recepción de mensajes de correo electrónico.

ASEGURAMIENTO SERVICIOS OPERATIVOS TI

Recursos para auditar mi cuenta de correo electrónico.

Existen recursos online (https://www.mail-tester.com/) para conocer si los protocolos SPF, DKIM y DMARC se encuentran configurados correctamente. Primero, envíe un mensaje al destinatario que indica la página, seguidamente haga clic en probar en la página para ver el resultado del test, que para este caso fue de un 10/10,en la figura 8 se observa que para la cuenta de correo corporativa, los 3 protocolos están configurados.



-0.1	DKIM_SIGNED	Message has a DKIM or DK signature, not necessarily valid **Esta regla se aplica automáticamente si tu email contiene una firma DKIM, pero otras reglas positivas también se agregarán si tu firma DKIM es válida. Ver a continuación.**
0.1	DKIM_VALID	Message has at least one valid DKIM or DK signature **¡Genial! Tu firma es válida**
0.1	DKIM_VALID_AU	Message has a valid DKIM or DK signature from author's domain **¡Genial! Tu firma es válida y viene de tu nombre de dominio**
0.1	DKIM_VALID_EF	Message has a valid DKIM or DK signature from envelope-from domain
-0.001	HTML_MESSAGE	HTML included in message **No te preocupes, es normal si envías correos HTML**
0.001	RCVD_IN_MSPIKE_H2	Average reputation (+2) 40.107.220.118 listed in wl.mailspike.net
0.001	SPF_HELO_PASS	SPF: HELO matches SPF record
0.001	SPF_PASS	SPF: sender matches SPF record **¡Genial! Tu SPF es válido**

Figura 8. Herramienta Mail tester

Recomendaciones generales:

- Si su entidad tiene un dominio propio por favor configure un certificado SPF para garantizar que los correos lleguen al buzón y no en la bandeja de spam.
- Mantenga su registro SPF correctamente configurado y actualizado, ya sea cuando cambie de hosting o servidor.
- Establezca si o si DMARC para no ser víctima de spoofing y suplantación de identidad.
- Implemente la segmentación de red, de manera que no se pueda acceder a los equipos de red desde todos los equipos.
- Realice jornadas de capacitación y concienciación de los usuarios, funcionarios y colaboradores, en donde se puedan observar las últimas campañas de los ciberdelincuentes junto con vectores de infección más populares.
- Parchee sistemas operativos, antivirus y programas con las últimas actualizaciones, NO use bajo ningún motivo aplicaciones obsoletas que ya no cuenten con soporte técnico.
- No inicie sesión con su cuenta de correo o red social corporativa en servicios de uso cotidiano.
- Por favor implemente los tres protocolos descritos en su servidor de correo o hosting, establezca contacto con el encargado, si tiene tercerizado el servicio para que inmediatamente realice las configuraciones.