PUNTO NEUTRO - Cómo configurar DMARC, DKIM y SPF en mi dominio.

Mallorca, 221, At. 2 – 08008 Barcelona (Spain)
+34 930 130 262 | +34 639 401 730
info@puntoneutro.net | Twitter: @puntoneutro_es

Aviso de confidencialidad: La información del presente documento es confidencial y está exclusivamente dirigida a la persona o entidad destinataria. No está permitida su modificación, copia o distribución a terceros sin el consentimiento previo de Punto Neutro, S.L. Versión 16/02/2024

1. ¿Qué son DMARC, DKIM Y SPF, y para qué sirven?

La aparición del correo electrónico, anterior a la creación de Internet, fue una gran revolución en lo que se refiere a comunicación. No solo nos permite enviar mensajes de texto entre dos o más usuarios, sino que podemos incluso recibir cualquier tipo de documento o archivo multimedia.

Pero la creciente utilización del correo electrónico también ha conllevado la aparición de algunos problemas, como por ejemplo la falsificación de la dirección del remitente.

Con el fin de terminar con este problema se han desarrollado diferentes soluciones técnicas a nivel de DNS. Nos referimos a los registros DMARC, DKIM y SPF de los que, a continuación, conocerás su funcionamiento y aprenderás a configurarlos. ¡Sigue leyendo porque es muy recomendable que los tengas activados!

¿Qué son?

DMARC, DKIM y SPF son protocolos de autenticación de correo electrónico que trabajan juntos para ayudar a prevenir el correo electrónico no deseado, el fraude y el phishing al asegurar la autenticidad de los mensajes y garantizar que provengan de remitentes legítimos.

- **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**: DMARC es un estándar de autenticación de correo electrónico que ayuda a proteger los dominios de correo electrónico de los remitentes contra el phishing, el fraude y el correo no deseado. Permite a los propietarios de dominios especificar cómo se deben procesar los correos electrónicos que no pasan las comprobaciones de autenticación SPF y DKIM, proporcionando instrucciones claras a los servidores de correo sobre cómo manejar los mensajes que no cumplen con los estándares de autenticación.
- **DKIM (DomainKeys Identified Mail)**: DKIM es un método de autenticación de correo electrónico que permite a un remitente asociar un dominio con un correo electrónico, mediante la firma digital de cada mensaje saliente. Esta firma se agrega a las cabeceras del correo y es verificada por el servidor de correo del destinatario para asegurar que el mensaje no haya sido alterado durante el tránsito y que realmente provenga del dominio del remitente especificado.
- **SPF (Sender Policy Framework)**: SPF es un mecanismo de autenticación de correo electrónico que permite a los propietarios de dominios especificar qué servidores están autorizados para enviar correos electrónicos en nombre de su dominio. Esto ayuda a prevenir el spoofing de correo electrónico al verificar la dirección IP del servidor emisor con la lista de servidores autorizados para enviar correos electrónicos en nombre de ese dominio.

¿Qué protocolos debo implementar?

Cuantos más protocolos que implementes, tendrás más probabilidad de que tus correos legítimos se entreguen y menos que te puedan suplantar tu identidad.

El siguiente cuadro comparativo explica el resultado en la entrega de mis correos legítimos y de posibles correos fraudulentos si implemento ninguna, alguna o todas estas tecnologías:

	Correos electrónicos legítimos entregados	Correos electrónicos de spam entregados	Correos electrónicos falsificados entregados
Ninguna tecnología implementada	Variable, algunos pueden ser entregados, pero otros pueden ser marcados como spam o bloqueados.	Mayor probabilidad de entrega de spam debido a la falta de autenticación.	Mayor probabilidad de entrega de correos electrónicos falsificados, ya que no hay autenticación para verificar la legitimidad del remitente.
SPF implementado	Mayor probabilidad de entrega, pero aún puede haber casos de falsos positivos y negativos.	Algunos correos electrónicos de spam pueden ser bloqueados, pero algunos pueden pasar.	Mayor probabilidad de entrega de correos electrónicos falsificados, ya que solo SPF se puede verificar.
DKIM implementado	Mayor probabilidad de entrega, menos probabilidades de ser marcados como spam.	Menor probabilidad de entrega de spam, ya que los servidores de correo pueden verificar el SPF y DKIM.	Menor probabilidad de entrega de correos electrónicos falsificados, ya que SPF y DKIM se pueden verificar.
DMARC implementado	Mayor probabilidad de entrega, menos falsos positivos y menos posibilidades de ser marcados como spam.	Menor probabilidad de entrega de spam, ya que los servidores de correo pueden verificar el SPF y DKIM, y aplicar políticas basadas en DMARC.	Menor probabilidad de entrega de correos electrónicos falsificados, ya que SPF y DKIM se pueden verificar, y se pueden aplicar políticas basadas en DMARC para rechazar correos electrónicos que no cumplan con las políticas especificadas.

DMARC se basa en SPF y DKIM, por lo que primero debes empezar por estos dos últimos.

2. SPF

SPF o Sender Policy Framework, como indican sus siglas en inglés, **describe uno de los protocolos más usados que sirven como protección contra la falsificación de direcciones en el envío de correo electrónico**.

El registro SPF define qué servidores están autorizados para enviar correo electrónico con nuestro dominio (el dominio es el sufijo que aparece detrás del @ de nuestro correo, como por ejemplo @tudominio.com). **De esta manera, se lucha contra la suplantación de identidad y el correo basura (SPAM). Además, evitamos que los correos electrónicos que enviamos acaben en la carpeta de correo no deseado.**

El servidor que recibe el correo electrónico busca, en el dominio del remitente, la lista de los equipos autorizados para realizar el envío de mensajes de correo electrónico en su nombre. Según si el servidor de correo consta o no en el registro, el servidor decide si dejar que el correo se envíe y se entregue al destinatario o, por el contrario, si hay que bloquearlo.

¿Cómo configurar un registro SPF?

Si aún desconoces si tienes un registro SPF activado, solo tienes que acceder a la zona DNS de tu dominio y comprobar si existe una entrada de tipo TXT similar a la siguiente:

```
tudominio.com. IN TXT “v=spf1 a mx -all”
```

En el ejemplo superior se indica un registro de texto (IN TXT) para el dominio tudominio.com con la siguiente descripción SPF:

“v=” define la versión usada de SPF.

“a” autoriza a las máquinas con la IP del registro A de tu dominio.

“mx” autoriza a las máquinas con la IP de los registros MX.

“-all” desautoriza a las máquinas que no encajen en lo autorizado explícitamente.

Puedes cambiar -all por ~all. En este caso, si el correo es recibido por una máquina no autorizada, el correo no se rechaza, pero se marca como spam.

¿Cómo configurar mi registro spf para autorizar a Punto Neutro?

Supongamos que este es tu registro original:

```
v=spf1 a mx ~all
```

Una vez modificado, debería quedar así:

```
v=spf1 a mx include:spf.puntoneutro.net ~all
```

****NOTA: Esto es un ejemplo. La información que puedes encontrar en el registro SPF puede variar parcialmente. Lo importante es incluir spf.puntoneutro.net.**

Esta modificación la puedes solicitar a tu proveedor de dominio o a tu informático de referencia.

Puedes modificar el registro SPF por ti mismo o misma si dispones de las credenciales de acceso facilitadas por tu proveedor de dominio. Para ello debes acceder al apartado DNS. Algunos paneles de control ya tienen su propio sistema de registro SPF, por lo que te recomendamos que lo busques antes.

¿Y si no sé cómo configurar mi registro SPF?

Si no quieres hacer esta modificación tú mismo, te recomendamos que reenvíes este manual a tu proveedor de dominio o a tu informático.

Puedes escribirle el siguiente correo:

Buenos días,

Solicito que modifiquen mi registro spf añadiendo el modificador **include:spf.puntoneutro.net**

Quedo a la espera de su confirmación para realizar las comprobaciones oportunas.

Atentamente,

Si no dispones de ninguna de estas dos opciones, **puedes contactar con nosotros en** oficina@puntoneutro.net y **solicitar asesoramiento para la modificación de tu registro SPF**.

Recuerda, el registro SPF sirve para autorizar el envío de correo electrónico desde otros servidores y para evitar el uso fraudulento de tu correo.

El uso del registro SPF es recomendable si estás usando los servicios de certificación de correo electrónico de PUNTO NEUTRO, pero solo podrás hacerlo si tienes contratado un dominio de correo propio.

3. DKIM

DKIM, o DomainKeys Identified Mail, es como un "sello digital" que se coloca en tus correos electrónicos salientes. Este sello es único para tu dominio de correo electrónico y garantiza que el correo proviene realmente de ti y no ha sido alterado durante el envío.

Cuando envías un correo electrónico, DKIM agrega un sello digital único al mensaje, utilizando una clave criptográfica asociada con tu dominio de correo electrónico. Cuando el servidor de correo del destinatario recibe el mensaje, puede verificar este sello digital para asegurarse de que el correo realmente proviene de ti y no ha sido modificado en el camino.

Implementar DKIM es importante para la correcta verificación de tus correos electrónicos. Adicionalmente, para el envío de correo electrónico a través de Punto Neutro es necesaria una configuración específica, que te indicamos más adelante.

¿Como configurar DKIM?

La implementación de DKIM implica varios pasos. Aquí tienes una descripción general de cómo se realiza:

1. **Generación de Claves**: En primer lugar, se genera un par de claves criptográficas: una clave privada y una clave pública. La clave privada se mantiene segura y se utiliza para firmar digitalmente los correos electrónicos salientes, mientras que la clave pública se publica en el DNS del dominio de correo electrónico.

2. **Configuración DNS**: Se añade un registro de tipo TXT al DNS del dominio de correo electrónico. Este registro contiene información sobre la clave pública DKIM, así como una serie de políticas y configuraciones opcionales.

3. **Firma del Correo Electrónico**: Antes de enviar un correo electrónico, el servidor de correo utiliza la clave privada para generar una firma digital única para ese mensaje. Esta firma se añade como una cabecera al correo electrónico saliente.

4. **Verificación en el Destinatario**: Cuando el servidor de correo del destinatario recibe el mensaje, extrae la firma DKIM del encabezado del correo electrónico y utiliza la clave pública del DNS del dominio del remitente para verificar la autenticidad de la firma.

5. **Validación y Acciones**: Después de verificar la firma DKIM, el servidor de correo del destinatario puede tomar varias acciones dependiendo de la configuración del dominio del remitente. Estas acciones pueden incluir aceptar, rechazar, marcar como spam o realizar otras acciones basadas en políticas definidas por el propietario del dominio.

6. **Monitoreo y Mantenimiento**: Es importante monitorear regularmente los informes DKIM para asegurarse de que las firmas se estén aplicando correctamente y de que no haya problemas de autenticación. Además, se deben tomar medidas para mantener segura la clave privada utilizada para firmar los correos electrónicos.

¿Como configurar DKIM para enviar correo electrónico certificado con Punto Neutro?

Debes acceder a la zona DNS de tu dominio y configurar dos entradas de tipo CNAME como las siguientes:

```
puntoneutro1._domainkey IN CNAME puntoneutro1._domainkey.puntoneutro.net.

puntoneutro2._domainkey IN CNAME puntoneutro2._domainkey.puntoneutro.net.
```

4. DMARC

DMARC (Domain-based Message Authentication, Reporting, and Conformance) es un estándar de autenticación de correo electrónico que permite a los propietarios de dominios especificar políticas sobre cómo los servidores de correo deben procesar los correos electrónicos que pretenden ser enviados desde su dominio. Funciona en conjunto con SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail) para proporcionar una capa adicional de seguridad.

Cuando un correo electrónico se envía con DMARC habilitado:

1. El receptor del correo electrónico verifica si el dominio del remitente tiene una política DMARC establecida.
2. Si hay una política DMARC establecida, el receptor comprueba si el correo electrónico cumple con las políticas especificadas (como SPF y DKIM).
3. Si el correo electrónico pasa las verificaciones de autenticación (SPF y DKIM) y cumple con las políticas DMARC, se entrega normalmente.
4. Si el correo electrónico no pasa las verificaciones de autenticación o no cumple con las políticas DMARC, el receptor puede aplicar acciones basadas en las políticas establecidas por el propietario del dominio, como rechazar el correo electrónico, marcarlo como spam o enviarlo a una carpeta de correo no deseado.

DMARC también proporciona informes detallados sobre la autenticación de correo electrónico y los intentos de suplantación de identidad, lo que permite a los propietarios de dominios monitorear y mejorar la seguridad de sus dominios de correo electrónico.

¿Cómo configurar DMARC?

La implementación de DMARC implica varios pasos. Aquí tienes una descripción general de cómo se realiza:

1. **Publicación de registros DNS**: El primer paso es publicar un registro DNS TXT en el dominio de correo electrónico. Este registro DMARC contiene información sobre la política DMARC, incluyendo qué acciones deben tomar los servidores de correo cuando reciben mensajes que no pasan las pruebas de autenticación SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail). El registro mínimo sería: `v=DMARC1; p=none;`
2. **Monitoreo y ajuste de la política DMARC**: Inicialmente, se puede configurar la política DMARC en modo de observación (p=none), lo que indica a los servidores de correo que no tomen acciones en base a la política DMARC, pero que envíen informes sobre los correos electrónicos que no pasen las pruebas de autenticación. Esto permite al propietario del dominio monitorear la autenticación de correo electrónico y ajustar la política DMARC según sea necesario.
3. **Análisis de informes DMARC**: Se deben revisar y analizar los informes DMARC que se reciben periódicamente. Estos informes proporcionan información detallada sobre los correos electrónicos que no pasaron las pruebas de autenticación SPF y DKIM, incluyendo detalles sobre el remitente, el destinatario, los resultados de autenticación y más.

4. **Ajuste de políticas y acciones DMARC**: Basándose en los informes DMARC y en las necesidades de seguridad de la organización, se pueden ajustar las políticas DMARC para especificar acciones como rechazar, marcar como spam o aceptar los correos electrónicos que no pasen las pruebas de autenticación SPF y DKIM.
5. **Implementación gradual**: La implementación de DMARC puede ser gradual, comenzando con políticas menos restrictivas (p=none) y luego cambiando gradualmente a políticas más estrictas (p=reject) a medida que se revisan y se ajustan las políticas basadas en los informes DMARC.
6. **Monitoreo continuo y mantenimiento**: Es importante realizar un monitoreo continuo de los informes DMARC y mantener actualizadas las políticas DMARC para garantizar una protección efectiva contra el phishing, el fraude y el correo no deseado.