PUNTO NEUTRO, Políticas de Seguridad y Buenas Prácticas para el Correo Electrónico.

Travessera de Dalt, 36, Ent. 4 – 08024 Barcelona (Spain) | +34 930 130 262 | +34 639 401 730
info@puntoneutro.net | Twitter: @puntoneutro_es

1. ¿QUÉ EXPLICA ESTE DOCUMENTO?

PUNTO NEUTRO es una plataforma de comunicaciones electrónicas certificadas. **PUNTO NEUTRO** incluye una **suite de servicios electrónicos basada en el uso del correo electrónico como plataforma de envío**.

Debido a ello, **desde PUNTO NEUTRO queremos informarle sobre las Políticas de Seguridad que tenemos implementadas en nuestra plataforma, en relación con sus comunicaciones por correo electrónico, y aprovechar para ofrecerle un listado de buenas prácticas** que recomendamos tener en cuenta en el uso del correo electrónico.

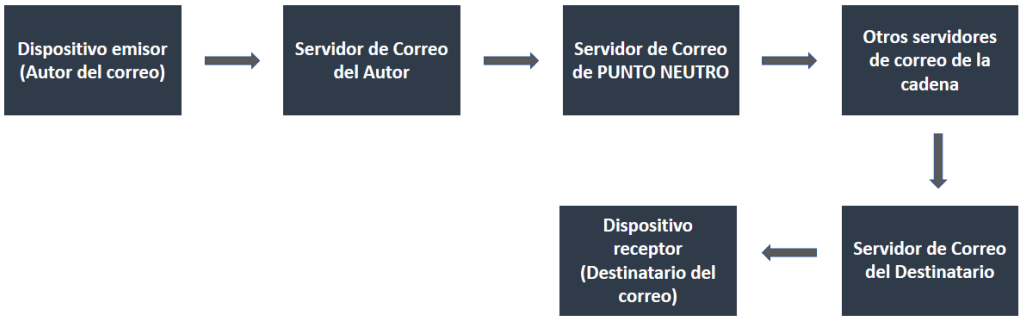
2. POLÍTICAS DE SEGURIDAD

PUNTO NEUTRO tiene aplicadas las siguientes **Políticas de Seguridad** para el buen funcionamiento del correo electrónico.

1º) DomainKeys Identified Mail (DKIM): Es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por el destinatario.

Dicha organización puede ser una fuente directa del mensaje, como el autor y su servidor de correo, o puede ser un servidor intermedio situado en la cadena de servidores que transportará ese correo, en este caso el servidor de correo de **PUNTO NEUTRO**, quien validará el tipo de certificación que el autor está pidiendo para su envío, la aplicará, y enviará el correo a los destinatarios.

Veámoslo de forma más clara con un esquema de flujo.



¿Qué tiene que ver esto con el DKIM?

Si nos fijamos en el esquema, en principio quien envía el correo al destinatario es el Autor desde su dispositivo, pasando por su servidor de correo. Sin embargo, esto no es realmente así, pues como el Autor del envío lo que quiere es certificar ese correo, el servidor de correo de **PUNTO NEUTRO** lo recibe y lo procesa, realiza las transformaciones que el Autor ha pedido para poder certificar, y posteriormente es el servidor de correo de **PUNTO NEUTRO** quien realmente envía el correo al destinatario.

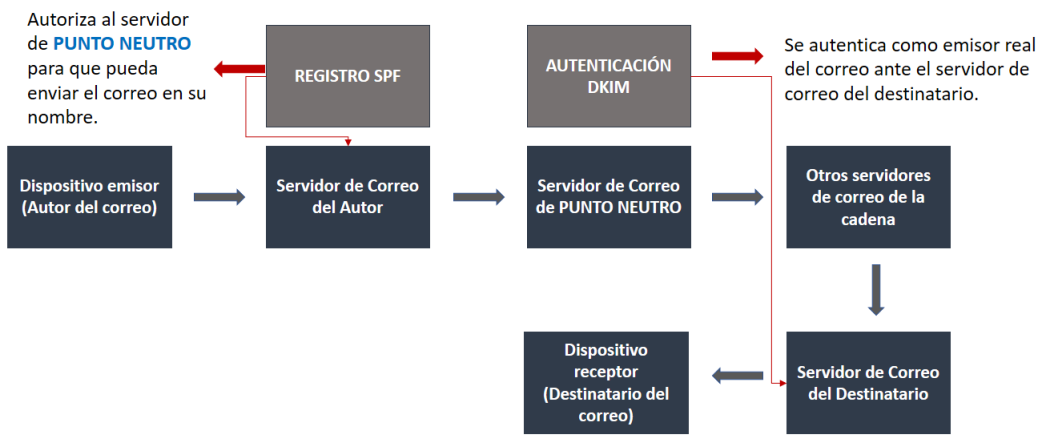
Esto implica que el servidor de correo del destinatario recibirá un correo desde el servidor de **PUNTO NEUTRO** pero enviado en nombre del dominio de correo del Autor.

Esto generalmente se considera sospechoso y el servidor del correo del destinatario puede filtrar ese correo como no seguro y no entregarlo al dispositivo del destinatario, pues ambos campos contenidos en la cabecera del correo (SMTP From y Mail From) no coinciden.

Para solucionar esto **PUNTO NEUTRO** tiene aplicado por defecto el mecanismo DKIM. Con este mecanismo el servidor de **PUNTO NEUTRO** le está demostrando al servidor de correo del destinatario que es realmente él quien está enviando el correo.

2º) Sender Policy Framework (Registro SPF): Es una protección contra la falsificación de direcciones de envío de correo electrónico. Permite identificar a través de los registros de nombres de dominio (DNS) a los servidores de correo SMTP autorizados para el transporte de los mensajes, es decir, para enviar en el nombre de ese dominio.

Si seguimos el esquema anterior, el Autor del envío puede acceder a su Servidor de Correo, y configurar en el Registro SPF la dirección IP del servidor de correo de **PUNTO NEUTRO**. Cuando **PUNTO NEUTRO** envíe al destinatario el correo certificado, el servidor de correo del destinatario verá que el dominio de correo del Autor ha autorizado al servidor de **PUNTO NEUTRO** a enviar en su nombre, con lo que se reducirá el riesgo de que ese correo se clasifique como no seguro o no deseado.



3º) Contenido y estructura correcta de los correos: A pesar de los cambios que tiene que introducir en los correos para poder llevar a cabo la certificación, **PUNTO NEUTRO** cumple perfectamente con las recomendaciones internacionales de configuración y formateo de correo electrónico, siendo estas:

- Incluir texto plano aun usando código HTML.
- Incluir pocas imágenes en el cuerpo de mensaje del correo.
- Evitar palabras con riesgo de considerarse SPAM, como, por ejemplo: Aviso Importante, Anuncio, Publicidad, Oferta, etc. Si necesita realizar campañas publicitarias hay herramientas especializadas para ello.
- Registrarse en listas blancas de dominio y revisar no aparecer en listas negras. **PUNTO NEUTRO** revisa periódicamente esas listas.
- Mantener una política de reenvío ante grey-listing (listas de rebote). **PUNTO NEUTRO** tiene automatizado un reenvío en caso de detectar un rebote de correo.

3. RECOMENDACIÓN DE BUENAS PRÁCTICAS

A pesar de las **Políticas de Seguridad** aplicadas por **PUNTO NEUTRO** para evitar problemas en el envío y recepción de sus correos electrónicos certificados, existe un gran número de variables que pueden afectar a la entrega / no entrega de su correo electrónico al destinatario final. A continuación, le enumeramos las principales y le ofrecemos recomendaciones al respecto.

1. En caso de incluir código HTML en el cuerpo del correo este debe estar bien formateado y seguir los estándares establecidos.
2. Autorizar la IP de **PUNTO NEUTRO** en el registro SPF. La línea para autorizar la IP de **PUNTO NEUTRO** es *v=spf1 mx a:mail.puntoneutro.net ~all*
3. No incluir imágenes adicionales en el cuerpo del correo si se está realizando un envío certificado por **PUNTO NEUTRO**.
4. Comprobar diariamente que sus correos llegan correctamente al destinatario, e incluso comprobar que el destinatario le ha acusado la lectura certificada o a descargado la documentación adjunta (según la modalidad de envío certificado que usted haya escogido).
5. En caso de comprobar que el destinatario no le acusa lectura o no le descarga la documentación adjunta, ponerse en contacto con él por una vía alternativa para comprobar a qué se debe y recomendarle que realice esas acciones.

6. No se recomienda el uso de servicios de correo gratuitos (@telefonica.net, @yahoo.com, @gmail.com, @hotmail.com, etc.). El motivo es que estos servicios no permiten configurar el correo, por lo que no podrán acceder al registro SPF y además suelen tener más problemas de entrega que un correo con dominio propio.
7. No realizar de forma habitual envíos masivos de correo por su dominio habitual. En caso de necesidad utilizar plataformas especializadas.
8. Mantener actualizada su libreta de direcciones y revisar que se introducen de forma correcta las direcciones en el momento de enviar un correo.