CCN-CERT

BP/33

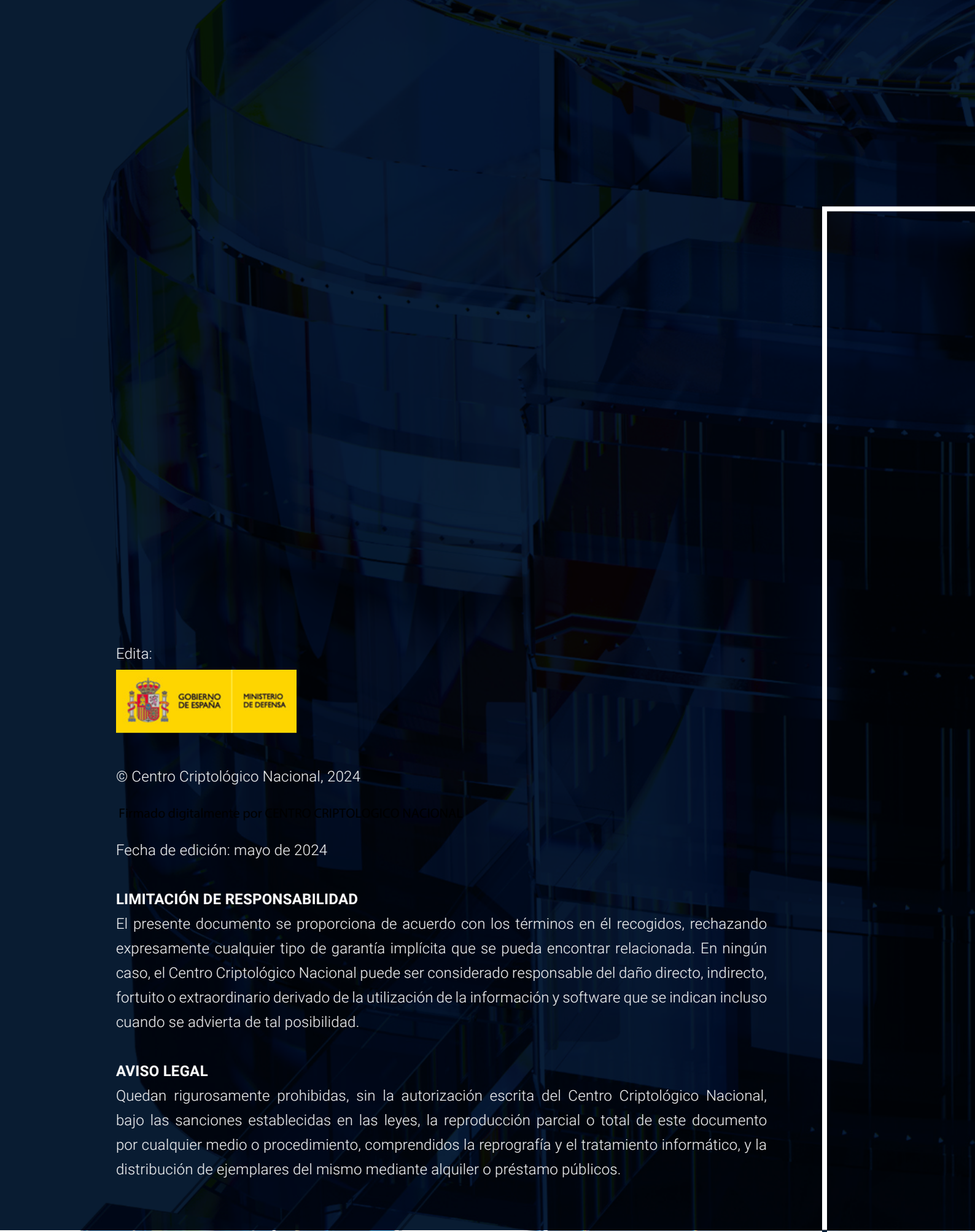
Recomendaciones de seguridad en el correo electrónico, DMARC

INFORME DE BUENAS PRÁCTICAS

MAYO 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional



Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de edición: mayo de 2024

Prólogo

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.
Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo de 2024

Esperanza Casteleiro Llamazares

Secretaria de Estado

Directora del Centro Criptológico Nacional

Índice

1. Objetivo de la guía

En el contenido de este documento, se explica el concepto de DMARC, el protocolo, las definiciones, sus aplicaciones prácticas y las implicaciones que surgen al implementarlo. Además, se analiza en detalle para qué sirve DMARC, destacando sus beneficios y cómo contribuye a fortalecer la seguridad y la autenticación de los correos electrónicos.

Asimismo, se examinan las repercusiones que se desencadenan al aplicar DMARC, detallando cómo esta medida puede influir en la identificación y prevención de intentos de suplantación de identidad (phishing) y otros ciberataques relacionados con el correo electrónico.

Se presentan ejemplos concretos de situaciones que pueden surgir al implementar DMARC y se proporciona información esencial para comprender cómo esta herramienta contribuye a garantizar la integridad y autenticidad de los mensajes electrónicos.

En resumen, **este documento constituye una guía completa sobre DMARC,** ofreciendo una visión detallada de su propósito, utilidad y las consecuencias prácticas que se derivan de su aplicación.

El documento describe el protocolo DMARC y cómo mejora la autenticación del correo electrónico, previene el phishing y refuerza la seguridad.

2. Introducción, DMARC y su importancia

2.1. Introducción a DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) es un protocolo de validación de correo electrónico diseñado para proteger los dominios de correo electrónico de la suplantación de identidad y otras formas de abuso en el correo electrónico, como el fraude y el phishing. Su historia se remonta a la colaboración entre varias organizaciones y expertos en seguridad de correo electrónico. Se encuentra especificado en el estándar **RFC7489**[1].

DMARC tiene dos funciones principales:

- Verificar la autenticidad del correo electrónico.
- Impedir que correos falsos alcancen su destino.

Contexto inicial

Antes de DMARC, ya existían SPF (*Sender Policy Framework*)[2] y DKIM (*DomainKeys Identified Mail*)[3], que son métodos para verificar si los correos electrónicos provienen de fuentes legítimas. Sin embargo, estos métodos tenían limitaciones, especialmente en cómo se trataban los mensajes que fallaban en estas verificaciones.

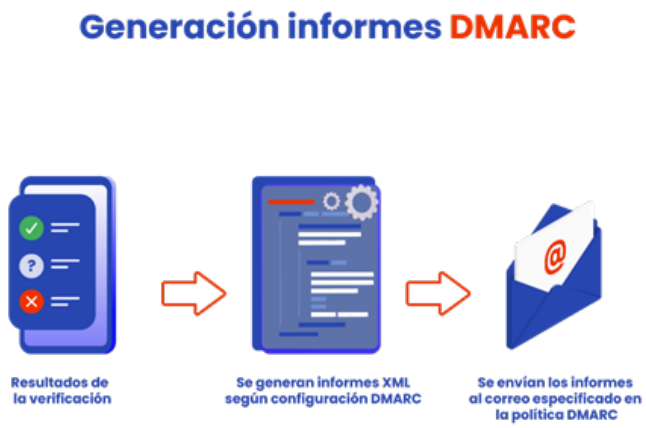
1: https://datatracker.ietf.org/doc/html/rfc7489
2: https://datatracker.ietf.org/doc/html/rfc7208
3:https://datatracker.ietf.org/doc/html/rfc6376

Necesidad de un nuevo estándar

El protocolo surgió como una solución para llenar los vacíos dejados por SPF y DKIM. Permitiría a los propietarios de dominios especificar cómo manejar los correos electrónicos que no pasarán las verificaciones individuales mediante **políticas**, además de construir un formato estándar de **informes** con mensajes informativos que los servidores de recepción de correo envían a los propietarios de los dominios sobre la autenticidad de los correos electrónicos recibidos.

Estos reportes ayudan a los administradores de dominios a entender cómo están siendo tratados sus correos electrónicos en el mundo exterior, incluyendo cuántos mensajes pasaron o fallaron las verificaciones de SPF y DKIM, y cómo fueron manejados de acuerdo con la política DMARC establecida.

Los informes se envían en un formato XML y proporcionan datos detallados que pueden ser utilizados para monitorizar y mejorar las medidas de seguridad del correo electrónico, **detectar problemas de configuración, combatir el abuso y el fraude y conocer el grado de alineamiento con DMARC.**



Colaboración y desarrollo

DMARC fue desarrollado en 2012 por un grupo de trabajo que incluía a grandes empresas tecnológicas y de comunicaciones como Google, Microsoft, Yahoo, AOL, y otras. La idea era crear un estándar que todos en la industria pudieran utilizar para hacer el correo electrónico más seguro y confiable.

2.2. Importancia de DMARC para las instituciones públicas

La implementación de DMARC es crucial para las instituciones públicas por varias razones:

- **Protección contra la suplantación de identidad en el correo electrónico,** impide que actores maliciosos envíen correos fraudulentos que parecen provenir de dominios legítimos de estas Instituciones Públicas.
- **Integridad de la información,** asegura que la información enviada por correo electrónico no ha sido alterada.
- **Confianza del ciudadano,** incrementa la confianza en las comunicaciones por correo electrónico de las Instituciones Públicas.
- **Soberanía,** en el contexto de la geopolítica actual, la protección contra campañas de desinformación y ciberataques es más importante que nunca para preservar la integridad y la soberanía.

El negocio de la ciberdelincuencia ha encontrado en la suplantación de dominios y correos electrónicos una actividad lucrativa. A través de técnicas de phishing e ingeniería social, estos grupos ciberdelincuentes pueden obtener acceso a información sensible, manipular eventos políticos, o incluso paralizar infraestructuras críticas.

Una entidad pública actual debería trabajar para obtener una política de cuarentena al 100% en un tiempo razonable, en función de lo declarado y los pasos a seguir que se indican más adelante.

3. Consideraciones técnicas previas a la implementación de DMARC

3.1. Qué es y cómo se configura SPF

SPF permite a los propietarios de dominios especificar **qué servidores de correo están autorizados para enviar correos electrónicos en nombre de su dominio.** Esto se logra mediante la publicación de un registro SPF en los DNS del dominio. Los servidores de recepción de correo pueden consultar este registro para verificar si el correo que están recibiendo proviene de un servidor autorizado por el propietario del dominio del remitente.

Ejemplo de SPF

Supongamos que una entidad con dominio "entidad.com" desea implementar SPF para protegerse. La entidad establece una política SPF que solo permite enviar correos desde sus servidores de correo internos y, opcionalmente, desde un proveedor de servicios de correo que utilizan. El registro SPF en el DNS de "entidad.com" podría verse algo así.

```
v=spf1 ip4:192.168.0.1 include:mailservice.com -all
```

Este registro SPF indica lo siguiente:

- **v=spf1,** La versión de SPF que se está utilizando.
- **ip4:**192.168.0.1, los correos electrónicos enviados desde la dirección IP 192.168.0.1 están autorizados.

include:serviciocorreo.com, incluye la política SPF del dominio "serviciocorreo.com", que es un ejemplo de proveedor de servicios de correo electrónico externo autorizado.

-all: Un mecanismo de fallo que indica que cualquier servidor que no cumpla con los criterios anteriores no está autorizado para enviar correos desde "entidad.com".

Cuando un servidor de recepción recibe un correo electrónico que afirma ser de "entidad.com", verificará contra el registro SPF. Si el correo proviene de un servidor no listado o autorizado en el registro SPF, será rechazado o marcado como sospechoso, dependiendo de la configuración del servidor receptor.

En el ejemplo solo hemos tratado los parámetros esenciales: versión, ipv4, include y all. Esto es lo mínimo necesario para que SPF funcione correctamente, asumiendo que el resto de los valores por defecto sean adecuados para la mayoría de las implementaciones. No es común ver el resto de parámetros, pero estos son:

Etiqueta	Descripción y valores permitidos
v	Este es siempre el primer parámetro en un registro SPF y declara la versión de SPF que se está utilizando. No hay alternativas para este valor; siempre debe ser **spf1**.
ip4 e ip6	Estos mecanismos especifican **las direcciones IP** (en formato IPv4 o IPv6, respectivamente) **que están autorizadas** para enviar correo en nombre del dominio. No hay un valor por defecto para estos campos; deben ser configurados explícitamente con las direcciones IP correctas. ipv4 es una etiqueta diferente a ipv6, comúnmente solo se utiliza ipv4 en la actualidad.
include	Este mecanismo **permite incluir la política SPF de otro dominio dentro de tu registro SPF.** Es útil cuando se utilizan servicios de terceros para enviar correos electrónicos en nombre de tu dominio. Al igual que con ip4 e ip6, no hay un valor predeterminado.
a y mx	Estos mecanismos **permiten que los correos electrónicos sean enviados desde las direcciones IP asociadas a los registros A o MX del dominio,** respectivamente. Si se usan sin parámetros adicionales, se refieren al propio dominio. No hay valores predeterminados; estos se aplican solo si se incluyen explícitamente.
ptr	**No se recomienda usarlo debido a problemas de rendimiento** y porque no es efectivo como mecanismo de verificación. El mecanismo ptr verifica que la dirección IP inversa del remitente coincida con el dominio especificado.
exists	Este mecanismo permite que el dominio **especifique una consulta de DNS** que, si resuelve, permite que la IP pase. Se usa raramente debido a su complejidad y carga en los servidores de DNS.
redirect	Permite **redirigir la evaluación de SPF** a otro dominio. Si se usa, reemplaza completamente la política del dominio original por la del dominio al que se redirige.

El mecanismo all

all es un mecanismo que **especifica cómo deben ser tratados los correos electrónicos que no coinciden con ninguno de los anteriores mecanismos en el registro SPF.** Es el "catch-all" al final del registro y es vital porque define el comportamiento por defecto para las direcciones IP que no están específicamente autorizadas. Este siempre debe aparecer al final del registro DNS para el SPF:

all	Descripción
+all	Permite a cualquier servidor enviar correo en nombre de tu dominio (esto efectivamente **desactiva SPF como medida de seguridad y no es recomendado).**
-all	Indica que los correos enviados desde servidores no especificados en el registro SPF deben ser rechazados. (Recomendado)
~all	Resulta en una **política de "softfail"**, que sugiere pero no requiere que los mensajes sean tratados como spam o rechazo; es útil para la fase de pruebas.
?all	Indica una política neutral donde no se da ninguna instrucción sobre cómo tratar los correos que no coinciden con otros mecanismos del registro.

3.2. Qué es y cómo se configura DKIM

DKIM permite al dominio del remitente asociar su dominio con un mensaje de correo electrónico, añadiendo una firma digital a la cabecera del mensaje. Esta firma digital es creada utilizando una clave privada que solo posee el remitente, y cualquier receptor puede verificar esta firma utilizando la correspondiente clave pública, la cual está publicada en el DNS del dominio del remitente.

Ejemplo de DKIM

Imaginemos que la entidad "entidad.com" quiere implementar DKIM para sus correos electrónicos. El administrador de sistemas de "entidad.com" genera un par de claves criptográficas (una privada y una pública). La clave privada se utiliza para firmar digitalmente los correos salientes del dominio, mientras que la clave pública se publica en un registro DKIM en el DNS del dominio.

Un posible registro DKIM en el DNS de "entidad.com" podría verse así:

```
dkim._domainkey.ejemplo.com. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC..."
```

Este registro DKIM indica lo siguiente:

- **dkim._domainkey,** el prefijo estándar que indica dónde se encuentra la clave pública DKIM para el dominio "entidad.com".
- **v=DKIM1**, la versión de DKIM.
- **k=rsa**, el tipo de clave criptográfica utilizada, en este caso RSA.
- **p=MIGfMA…**, la clave pública que se utiliza para verificar las firmas digitales.

Cuando un servidor de recepción recibe un correo electrónico que afirma ser de "entidad.com", verificará la firma en la cabecera del correo utilizando la clave pública. Si la verificación es exitosa, esto confirma que el mensaje realmente proviene de "entidad.com" y que no ha sido modificado en tránsito. Si la verificación falla, el correo puede ser tratado como sospechoso.

En el ejemplo solo hemos tratado los parámetros esenciales: versión, tipo de clave, y la clave pública. Esto es lo mínimo necesario para que DKIM funcione correctamente, asumiendo que el resto de los valores por defecto sean adecuados para la mayoría de las implementaciones. No es común ver el resto de parámetros, pero estos son:

Etiqueta	Descripción y valores permitidos
v	Versión del **DKIM**, por defecto: DKIM1. Este parámetro siempre debe estar presente y configurado para indicar que se trata de un registro DKIM.
h	Algoritmos de hash permitidos. Generalmente, no se especifica y los sistemas asumen los más comunes como **sha256**.
k	Tipo de clave, DKIM utiliza **rsa** por defecto, y es el tipo de clave más comúnmente utilizado para firmar los correos electrónicos.
p	Clave pública, este campo debe contener la clave pública que corresponde a la clave privada utilizada para firmar los correos electrónicos.
s	Ámbito de los correos que la firma pretende cubrir, generalmente, no se especifica y se asume ***, lo que significa que la firma es válida para **todos los correos del dominio.**
t	Marca de tiempo de la firma, no se usa comúnmente en los registros DKIM, **la gestión de la validez temporal se realiza en el software que verifica la firma.**

Etiqueta	Descripción y valores permitidos
g	Granularidad de la firma. Define a qué usuarios específicos se aplica la firma. Por defecto, suele estar configurado para coincidir con cualquier usuario (*).
n	Notas, campo de texto libre para incluir comentarios del administrador.
o	Política de firma, indica si todos los correos deben estar firmados (-) o si algunos correos pueden no estarlo (~).
i	Identidad del usuario que firma el mensaje. Esta permite especificar una dirección de correo electrónico particular en el campo "From:" que la clave se supone que firma.

3.3. Qué es y cómo se implementa DMARC

DMARC utiliza las tecnologías de SPF y DKIM antes mencionadas para verificar que los mensajes de correo electrónico procedentes de un dominio sean auténticos y no hayan sido alterados en tránsito.

Además, permite a los propietarios de dominios establecer políticas que dictan cómo deben manejar los servidores receptores los correos que no pasan estas verificaciones. También proporciona un sistema de informes que permite a los administradores de dominios recibir retroalimentación sobre el rendimiento de los correos enviados desde su dominio y cómo están siendo procesados bajo las políticas de DMARC.

Ejemplo de DMARC

Seguimos con el ejemplo de la entidad "entidad.com" y esta desea implementar DMARC para mejorar la seguridad de su correo electrónico. El administrador de sistemas de "entidad.com" añade un registro DMARC al DNS del dominio, que podría ser así:

```
v=DMARC1; p=none; rua=mailto:reportes@proveedordmarc.com;
ruf=mailto:fallos@proveedordmarc.com; fo=1; adkim=r; aspf=r
```

Este registro DMARC indica lo siguiente:

- **v=DMARC1**: Versión de DMARC.
- **p=none:** Política de DMARC que pide no realizar ninguna acción en los correos que no pasen las pruebas de SPF y/o DKIM, pero sí generar los reportes.
- **rua=mailto**:reportes@proveedordmarc.com, dirección de correo electrónico para recibir reportes agregados de autenticación.
- **ruf=mailto**:fallos@proveedordmarc.com, dirección de correo electrónico para recibir reportes forenses detallados de fallos de autenticación.
- **fo=1:** Generar reportes de fallo si falla cualquier verificación (SPF o DKIM).
- **adkim=r; aspf=r,** alineación relajada para DKIM y SPF respectivamente, indicando que la parte del dominio debe coincidir con el dominio en el mensaje, pero permite ciertas discrepancias.

Al utilizar este registro DMARC, "entidad.com" no protege su marca de usos indebidos en el correo electrónico por la política seleccionada, pero permite recibir información valiosa sobre el rendimiento y la seguridad de sus comunicaciones por correo electrónico, lo que le permite realizar ajustes y mejoras continuas en sus protocolos de seguridad para planificar un cambio de política.

En el ejemplo solo hemos tratado los parámetros básicos: versión, política, rua, ruf y fo. Esto es lo mínimo necesario para que DKIM funcione correctamente, asumiendo que el resto de los valores por defecto sean adecuados para la mayoría de las implementaciones. No es común ver el resto de parámetros, pero estos son:

Etiqueta	Descripción y valores permitidos
v	Versión del protocolo DMARC, actualmente **DMARC1**.
p	Política para aplicar al correo electrónico que no superan la verificación de DMARC. Puede ser: ◆ **none:** Esta política permite que todos los correos electrónicos alcancen su destino, incluso si fallan la verificación de DMARC. Se utiliza como una política de monitorización para analizar los reportes de fallo y determinar el nivel de alineamiento con DMARC. ◆ **quarantine:** Esta política determina que los correos que fallan la verificación sean marcados como correo no deseado o spam. ◆ **reject:** Esta es la política más estricta, mediante la cual los correos que fallan la verificación son rechazados impidiendo que lleguen a su destino.

Etiqueta	Descripción y valores permitidos
sp	Política para aplicar al correo electrónico, correspondiente a **subdominios**, que no superan la verificación de DMARC. Si se omite esta etiqueta, se aplicará la política definida en la etiqueta "p" a los subdominios.
aspf	El modo de alineación aspf se refiere a la precisión con la que se comparan los registros del remitente con las firmas SPF, con dos posibles valores: ◆ "r" (**relajado**) permite coincidencias parciales, como subdominios de un dominio dado. ◆ "s" (**estricto**) requiere una coincidencia exacta.
adkim	El modo de alineación adkim se refiere a la precisión con la que se comparan los registros del remitente con las firmas DKIM, con dos posibles valores: ◆ "r" (**relajado**) permite coincidencias parciales, como subdominios de un dominio dado. ◆ "s" (**estricto**) requiere una coincidencia exacta.
pct	La etiqueta de porcentaje indica que solo apliquen la política de DMARC a un **porcentaje** de los correos electrónicos fallidos. "pct=50" indicará a los receptores que apliquen sólo la política al 50% de los correos electrónicos que no superen la verificación DMARC. Si se omite esta etiqueta, se aplicará al 100% de los correos electrónicos fallidos. La etiqueta pct se diseñó como una forma de aplicar gradualmente las políticas DMARC para acortar el período de implementación para las empresas en línea.
rua	Lista de URI para enviar **reportes** XML de comentarios **agregados**. Los reportes RUA son resúmenes agregados que los servidores receptores envían al propietario de un dominio para informar sobre el volumen y los resultados de la autenticación de correos electrónicos enviados en su nombre. DMARC requiere una URI o lista de URIs y no solo un correo, quedando: **"mailto:analizador-dmarc@receptor-del-reporte.com".**
ruf	Lista de URI para enviar **reportes forenses**. Los reportes RUF son mensajes que los servidores receptores de correo electrónico envían al propietario de un dominio para proporcionar información detallada sobre incidentes individuales de falla en la autenticación de mensajes. Actualmente en desuso por la mayoría de proveedores de correo ya que hay problemas de privacidad en las comunicaciones. DMARC requiere una URI o lista de URIs y no solo un correo, quedando: **"mailto:analizador-dmarc-forense@receptor-del-reporte.com".**
rf	**Formato** para el reporte de fallo. Esto puede ser "afrf" (Authentication Failure Reporting Formats) o "iodef" (Incident Object Description Exchange Format). Por defecto, su valor es "afrf".
fo	Etiqueta usada dentro del registro DMARC para especificar las **condiciones** bajo las cuales los receptores deben **generar y enviar** reportes de fallos. Los valores permitidos son: ◆ "0" para generar informes si tanto DKIM como SPF fallan ◆ "1" para generar informes si DKIM o SPF falla ◆ "d" para generar un informe si DKIM falla ◆ "s" para generar un informe si SPF falla Este campo puede tener múltiples opciones combinadas.
ri	Intervalo entre informes expresado en segundos. Es la frecuencia con la que desea recibir informes XML agregados. Se trata de una preferencia, los proveedores deben tener la capacidad de ofrecer un informe diario, pero si el intervalo es menor, se aplica la base del mejor esfuerzo. Por defecto, su valor es "86400".

3.4. Alineamiento del DMARC

Los mecanismos de seguridad de SPF y DKIM son suficientes para validar que un correo se envía desde un servidor autorizado, pero no garantizan, en ningún caso, que no estén realizando suplantaciones de identidad. Para evitar esta casuística, DMARC, incorpora un nuevo concepto de seguridad llamado “Alineamiento del DMARC”.

Para entender este concepto, es fundamental comprender las diferencias entre las cabeceras "Mail From" y "Header From" y su importancia en el proceso de alineación DMARC. El “Mail From” se utiliza durante el proceso de autenticación (se le aplica el DKIM y SPF) y el “Header From” se utiliza durante la visualización del correo. Es decir, un servidor puede autenticarse correctamente, pero puede utilizar como remitente una identidad suplantada que será la que aparecerá ante el usuario durante la visualización. Por ello, es la alineación de DMARC la que evitará que un servidor, autenticado legítimamente, pueda enviar correos utilizando como remitente dominios no autorizados.

Importancia del Mail From, Header From, SPF y DMARC en la alineación DMARC

En el proceso de alineación DMARC, se examinan tanto el “Mail From” como el “Header From” y se tienen en cuenta los resultados de las verificaciones de SPF y DKIM. Se realizan dos verificaciones de la alineación distintas:

- **SPF alineado:** Para que se dé una alineación del SPF es necesario que el correo cumpla con la verificación SPF y que el “Mail From” y “Header From” pertenezcan al mismo dominio.

- **DKIM alineado:** Para que se dé una alineación del DKIM es necesario que el correo cumpla con la verificación DKIM y que el dominio utilizado durante la firma de integridad de DKIM pertenezca al mismo dominio que el usuario de “Header From”.

Si se cumple uno de ellos consideraremos que un correo electrónico está parcialmente alineado y si cumple los dos consideraremos que está completamente alineado. Únicamente es necesario que se cumpla uno de ellos para que cumpla el DMARC correctamente.

Alineamiento relajado y estricto

En DMARC, la alineación SPF y DKIM puede ser relajada o estricta. En el modo relajado, se permite una coincidencia aceptando subdominios entre el encabezado "Header From" y los dominios analizados por SPF y DKIM mientras que, en el modo estricto, se requiere una coincidencia exacta.

En la siguiente tabla se puede observar cuando se cumple cada tipo de alineamiento dependiendo de los dominios del “Header From” y “Mail From”

Header From	Mail From	Alineamiento relajado	Alineamiento estricto
ejemplo.com	**ejemplo.com**	Cumple	Cumple
app.ejemplo.com	**app.ejemplo.com**	Cumple	Cumple
ejemplo.com	**app.ejemplo.com**	Cumple	No cumple
app.ejemplo.com	**ejemplo.com**	Cumple	No cumple
app.ejemplo.com	**email.ejemplo.com**	Cumple	No cumple
ejemplo.com	**badmail.com**	No cumple	No cumple

3.5. Cómo crear un registro TXT de SPF, DKIM y DMARC

Para crear un registro DNS, incluido un registro DMARC, puede seguir estos pasos generales que se aplican a la mayoría de los proveedores de servicios de DNS. Aquí se detallan los pasos sin incluir ejemplos específicos:

Acceso al administrador de DNS

Inicie sesión en el panel de control de tu proveedor de hosting o registrador de dominios donde se aloja tu DNS.

Localice la sección de administración de DNS o Dominios en su panel de control.

Navegar a la gestión de registros DNS

Entra en la sección específica donde puedes ver y modificar los registros DNS. Esto podría estar etiquetado como "Zona DNS", "Gestor DNS", "Configuración de DNS", o algo similar.

Agregar un nuevo registro

Selecciona la opción para añadir un nuevo registro. Esto puede ser un botón o enlace que diga "Agregar Registro", "Nuevo Registro", o "Crear Registro".

Especificar el tipo de registro y detalles

Escoja el tipo de registro adecuado, seleccionará "TXT" como tipo de registro.

Especifique el nombre del host o nombre de registro.

- **Para un registro SPF** generalmente, el nombre del host para un registro SPF es simplemente "@" si quiere que se aplique al dominio principal. El valor del registro SPF debe empezar con v=spf1 seguido de las directivas que especifican qué servidores están autorizados para enviar correo en nombre de su dominio

- **Para un registro DKIM** el nombre del host es usualmente algo como selector._domainkey. Aquí, "selector" es un prefijo que se puede definir (es una etiqueta que ayuda a identificar la clave específica usada para firmar correos). Por ejemplo, si elige mail como selector, el nombre completo del registro sería mail._domainkey.tudominio.com.

  El valor para un registro DKIM incluye la versión de DKIM (v=DKIM1), el tipo de clave, y la clave pública en sí.

- **Para un registro DMARC,** usualmente escriba "_dmarc". Esto hará que el nombre completo del registro sea "_dmarc.entidad.com".

  Introduzca el valor del registro. Aquí es donde colocará los detalles del registro DMARC, como la política, las direcciones de correo para reportes, etc.

Guardar el registro
Revise la información que ha ingresado para asegurarse que es correcta.

Guarde o aplique los cambios. Puede haber un botón que diga "Guardar", "Aplicar", o "Actualizar".

Verificación
Verifique que el registro se haya creado correctamente usando herramientas locales como el comando “dig” o mediante herramientas online de terceros como MXToolbox o similares para asegurarse de que el registro se está propagando y es accesible públicamente.

Esperar la propagación
Tenga en cuenta que los cambios en los registros DNS pueden tardar en propagarse. Este tiempo puede variar desde unos pocos minutos hasta 48 horas, dependiendo del TTL (tiempo de vida) configurado para los registros y del proveedor de DNS.

3.6. Uso adecuado de selectores DKIM

Un selector en DKIM es una cadena de caracteres que identifica de manera única un conjunto específico de claves públicas utilizadas para firmar los mensajes de correo electrónico mediante DKIM. Cada dominio que implementa DKIM puede tener múltiples selectores, cada uno asociado con un par de claves pública/privada único. El selector se incluye en la cabecera DKIM del correo electrónico firmado, lo que permite al servidor receptor identificar qué conjunto de claves debe utilizar para verificar la firma DKIM.

Una buena práctica en el uso de selectores DKIM es utilizar múltiples selectores para diferentes conjuntos de claves, lo que facilita la gestión y la revocación en caso necesario. Esto implica asignar un selector específico para los servidores de correo internos y crear selectores independientes para cada tercero o servicio externo que envíe correo en nombre de la organización. Al hacerlo de esta manera, se puede revocar selectivamente un conjunto de claves comprometido sin afectar la autenticación de otros servicios. Además, proporciona una mayor granularidad en la gestión de claves y mejora la seguridad global del sistema DKIM.

3.7. Medidas adicionales durante la aplicación de políticas de DMARC

Durante la implementación de políticas de DMARC, es fundamental considerar medidas adicionales para fortalecer la seguridad del correo electrónico y mitigar los riesgos de suplantación de identidad y phishing. Además de las políticas de “reject” o “quarantine”, para los correos electrónicos que no cumplen con SPF, DKIM o DMARC, existen otras acciones que las organizaciones pueden tomar para proteger a sus usuarios:

- Sustitución del "Header From" por el "Envelope From" cuando no se cumple DMARC, permitiendo visualizar el remitente real en lugar del "Header From" que podría ser suplantado.
- Agregar un banner informativo que alerte al usuario sobre la posibilidad de suplantación de identidad y recomiende precaución al abrir el correo.

Estos controles se aplican durante la recepción de los correos de los usuarios del dominio protegido. Son medidas poco intrusivas pero que resultan eficaces para alertar a los usuarios de correos sospechosos. Es importante destacar que estos controles en ningún caso previenen la suplantación de usuarios del dominio hacia un tercero (esto se realiza gracias a SPF, DKIM y DMARC) ya que operan en la infraestructura del dominio que estamos protegiendo.

4. Planificación y preparación

4.1. Análisis de la infraestructura de correo electrónico

Antes de implementar DMARC, resulta esencial realizar una auditoría completa de la infraestructura de correo electrónico actual. Esto incluye:

- **Identificar todos los dominios de correo electrónico que necesitan protección DMARC.** Esto incluye dominios primarios, subdominios y cualquier otro dominio utilizado para enviar correos electrónicos legítimos.
- **Realizar un inventario completo** de todos los sistemas que envían correos electrónicos en nombre de tu dominio, incluyendo sistemas internos y proveedores externos.
- **Revisar los registros** SPF y DKIM existentes para cada dominio. Asegurarse de que estos registros estén correctamente configurados y alineados con los servicios de correo electrónico utilizados.
- En caso de utilizar servidores de correo electrónicos pertenecientes a la Institución, **evaluar el hardware y software utilizados** para verificar que se encuentran actualizados y se aplican las mejores prácticas de seguridad.
- Valorar la aplicación de DMARC a los **dominios que no se utilicen para correo** electrónico para evitar la suplantación de los mismos por parte de los actores maliciosos.

4.2. Configuración de SPF y DKIM

Antes de configurar DMARC, se debe garantizar la correcta implementación de los estándares SPF y DKIM.

- **Revisar o configurar los registros** SPF y DKIM para garantizar que estén correctamente alineados con los servicios de correo electrónico utilizados para enviar correos en nombre del dominio.
- Asegurarse de que todos los servidores de correo autorizados para enviar correos se encuentran **listados en el registro SPF**. Si es necesario se debe solicitar un listado completo a los proveedores de servicio de correo electrónico que se estén utilizando.
- Asegurarse de que la infraestructura de correo electrónico sea capaz de generar **firmas DKIM válidas** y que se permita la inclusión en el registro DNS.

4.3. Determinar la configuración inicial de DMARC

La implementación inicial de DMARC debe contemplar al menos los siguientes puntos:

- Defina **qué espera lograr con DMARC** no basándose en el estado actual de alineamiento, sino en el objetivo final o idóneo. Con esto tenemos una política objetivo.
- Asegúrese de que **los equipos de IT y seguridad entiendan cómo funcionan** DMARC y sus dependencias con SPF y DKIM.
- **Decida la política DMARC inicial** para cada dominio. La política puede ser "ninguna acción" (*none*), "cuarentena" (*quarantine*) o "rechazo" (*reject*) para los correos electrónicos que no superan la autenticación SPF y DKIM.
- En caso de no tener nada configurado o dudas del alineamiento, **publique un registro DMARC con una política de none** (p=none) para monitorear y no afectar el flujo de correo existente.
- **Incluya en el registro las direcciones para los reportes** agregados (rua) para recibir los análisis de los correos que pasan y fallan las verificaciones.

4.4. Establecimiento de un protocolo para monitorización continua y ajuste de la política DMARC

La implementación de DMARC no es un evento único, sino un proceso continuo y escalonado que requiere de una monitorización continua, análisis de resultados y ajustes en la configuración de DMARC.

- **Establecer al menos una dirección de correo electrónico específica** para la recepción de los informes de DMARC para su posterior análisis. Se recomienda trabajar con empresas que analicen y gestionen el dato para la fácil lectura del mismo en gráficos y métricas.
- **Conformar un equipo de seguridad** que se encargue del análisis de los informes agregados y la interpretación de dichas gráficas de los proveedores y pueda actuar en consecuencia.
- **Utilizar herramientas de análisis de DMARC de terceros** para evaluar la efectividad de la política y hacer ajustes.
- **Establecer un proceso para revisar regularmente** el estado de DMARC, su alineamiento y entender las tendencias o problemas emergentes.
- **Revisar periódicamente las políticas de seguridad** para asegurar que siguen siendo efectivas y relevantes.
- **Identificar los flujos legítimos de correo electrónico que no están alineados** con la configuración actual de SPF y DKIM.
- **Ajustar las configuraciones de SPF, DKIM y DMARC** de forma periódica, según sea necesario para mantener una postura de seguridad sólida. En base a los puntos anteriormente mencionados.

4.5. Establecimiento de un protocolo o proceso de gestión de cambios

La implementación de cambios en la infraestructura de correo electrónico debe hacerse de manera controlada y documentada. Esto implica:

- Desarrollar un **plan de implementación que incluya hitos y plazos.**
- **Procesos de aprobación claros** para cualquier cambio en la configuración del correo electrónico.
- **Registros detallados de los cambios realizados** para facilitar la auditoría y el seguimiento de problemas.

4.6. Planificación de procedimientos de escalada y respuesta a incidentes

Disponer de un plan claro para responder a los problemas identificados por DMARC es crucial.

- **Establecer canales de comunicación claros** para reportar y responder a incidentes de seguridad relacionados con el correo electrónico.
- **Definir un procedimiento claro de escalada** para los casos de intento de suplantación o abuso significativo del dominio de correo electrónico que se detecten.
- **Desarrollar procedimientos para la investigación** rápida de fallos en la autenticación DMARC.
- **Establecer un plan de respuesta a incidentes** que incluya la notificación a los usuarios afectados, la corrección de registros de DNS mal configurados y la comunicación con las autoridades si es necesario.

- **Analizar regularmente los informes DMARC** para detectar y responder a las tendencias emergentes o nuevos vectores de ataque. Es recomendable contar con una empresa que colabore en este proceso mediante la representación de los datos con gráficas y métricas.
- **Integrar los informes DMARC con herramientas de análisis de seguridad** para obtener una comprensión más profunda de los patrones de ataque y las vulnerabilidades potenciales.

4.7. Planificación de pruebas y validación periódica

- **Realizar pruebas periódicas** para validar la eficacia de los planes de contingencia y comprobar el estado de actualización y efectividad de los procedimientos de respuesta.
- **Incluir simulacros** de falsos positivos como parte del entrenamiento regular de respuesta a incidentes para evaluar la preparación del equipo y la eficacia de los protocolos.

4.8. Documentación y registro

- **Crear guías** de operaciones estándar para la gestión y el mantenimiento de DMARC. La documentación es vital para la sostenibilidad y gestión.
- **Mantener documentación detallada** y registros de auditoría de todas las acciones y decisiones relacionadas con DMARC, SPF y DKIM para facilitar el cumplimiento de las regulaciones pertinentes y las investigaciones de incidentes.
- **Mantener un registro detallado** de todos los cambios realizados y los falsos positivos identificados y las acciones tomadas para su resolución.
- **Registrar y documentar todos los incidentes de seguridad** y las acciones tomadas en respuesta.
- **Utilizar la información recopilada para determinar mejoras** en las políticas y procesos de seguridad de correo electrónico.

4.9. Formación y concienciación

Es fundamental que el **personal técnico involucrado en la implementación y gestión** de correo electrónico entienda la importancia de la autenticación del correo electrónico y cómo DMARC puede ayudar a proteger contra el phishing y el spoofing. Esto puede incluir:

- **Talleres y seminarios web** sobre los fundamentos de DMARC, SPF y DKIM.
- **Creación de materiales de referencia rápida** y guías para el personal técnico.
- Programas de **formación continua** para mantener al personal actualizado con los cambios en las normativas y tecnologías.
- **Establecer canales de comunicación** para que los usuarios puedan informar sobre cualquier problema relacionado con la entrega de correos electrónicos.

4.10. Coordinación con proveedores de correo electrónico

- **Trabajar junto a los proveedores de servicios** de correo electrónico para resolver problemas relacionados con las configuraciones de SPF y DKIM.
- **Establecer acuerdos de nivel de servicio (SLAs)** con los proveedores para garantizar respuestas rápidas y efectivas cuando surjan problemas con los correos electrónicos legítimos.

5. Implementación inicial desde cero

En este punto, vamos a **ejemplificar** con una casuística en la que la entidad **no tiene registros creados**, no ha implementado nunca DMARC o quiere eliminar los actuales para crear la base sólida documentada desde la que construir su proceso.

Vamos a detallar todo lo planificado, comenzamos con las configuraciones ejemplificadas descritas y explicadas en el **apartado 3.1.** de este documento, **creando el registro SPF con los datos de todos los proveedores y/o terceros autorizados por la entidad** para mandar correos electrónicos en su nombre. Asimismo, la configuración de DKIM, también descrita en el **apartado 3.2**., este punto requiere la comunicación o consulta de soporte con el proveedor de correo electrónico si este no es gestionado por la entidad. Recordar de nuevo que el **DKIM debe ser implementado por todos los proveedores de correo electrónico,** estos pueden compartirnos diferentes registros TXT para aceptar la firma de todos ellos en el caso de ser múltiples proveedores, los datos del registro y contenido del registro deben ser proporcionados por cada uno de los proveedores.

Tendríamos algo parecido a estos registros DNS como ejemplo:

```
@ IN TXT "v=spf1 ip4:192.168.0.1
include:proveedorcorreo.com -all"

dkim._domainkey.entidad.com. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC..."
```

Importante remarcar que las dudas surgidas en este punto deben estar resueltas en el apartado 3.1. y 3.2.

5.1 Política inicial de DMARC

- Se recomienda establecer siempre una implementación inicial de DMARC, si no se dispone de una previamente, en modo de monitorización (política none) inicialmente, para evaluar tanto el nivel de alineamiento como el posible impacto en la entrega de correo electrónico legítimo e intentos de suplantación.

- Configurar los registros DMARC para generar informes agregados y de fallos etiquetas rua) que deben ser enviados a un analista designado o a un tercero que ofrezca servicios de análisis de DMARC.

Como hemos visto en el **apartado 3.3.** de este mismo documento la configuración inicial para las entidades que no contaban con un registro DMARC o entidad que desconozca el estado del mismo.

Tipo de Registro TXT
Nombre del Host _dmarc.entidad.com
Valor del Registro

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=none;
rua=mailto:reportes@proveedordmarc.com;"
```

Descripción de los componentes del registro

- **v=DMARC1,** esto especifica la versión del protocolo DMARC que se está utilizando.

- **p=none,** esta política indica que, aunque se verificarán los mensajes de correo electrónico para ver si pasan las pruebas de DMARC, no se tomarán acciones específicas si fallan. Esencialmente, esto permite a los propietarios de dominios monitorizar la efectividad de SPF y DKIM sin afectar la entrega de sus correos.

- **rua=mailto:reportes@proveedordmarc.com,** esta parte del registro indica dónde deben enviarse los reportes agregados. Los reportes agregados contienen datos sobre todos los intentos de envío desde el dominio, lo que ayuda a los administradores a comprender cómo se está manejando su correo en la red.

5. Implementación inicial desde cero

Usando este registro, los servidores que reciben correos de tu dominio no tomarán acciones punitivas contra los correos que fallen las pruebas DMARC, pero enviarán reportes agregados a la dirección especificada, permitiéndote analizar y ajustar tus configuraciones de SPF y DKIM para mejorar la autenticación de tus correos. Esto es ideal para una fase inicial de implementación de DMARC, donde aún estás evaluando y refinando tus políticas de autenticación de correo.

5.2. Monitorización y ajuste gradual

- **Monitorizar los informes** de DMARC para identificar los servidores de correo electrónico que envían correos electrónicos en nombre del dominio.
- **Desarrollar un cronograma** para revisar los niveles de alineamiento con una periodicidad[4] **(Te)*** establecida según el tipo de Institución.
- **Establecer umbrales claros** para cada incremento basados en el análisis de los informes de DMARC y la retroalimentación de los usuarios: si supera el 95%, valorar un cambio de política. Este debe comenzar con un porcentaje bajo **(P0)*** y aumentarlo gradualmente **(Pin)*** a medida que se gana confianza en la configuración y se reduce la incidencia de falsos positivos.
- **Comunicar los cambios en la política DMARC** a todos los usuarios para que estén preparados para posibles preguntas o informes de correos legítimos marcados incorrectamente. Aunque el establecimiento de porcentajes para la aplicación paulatina de la política se utiliza para evitar falsos positivos, es posible que estos ocurran, siendo necesario que los usuarios corroboren que ningún correo legítimo ha sido marcado como no deseado.

5.3. Corrección de problemas

- **Identificar y corregir los problemas de autenticación** SPF y DKIM utilizando los informes de DMARC. Esto puede incluir agregar nuevos servicios de correo electrónico a los registros SPF, configurar correctamente las firmas DKIM o abordar problemas de alineación.
- **Actualizar los registros SPF y DKIM según sea necesario** para reflejar cambios en la infraestructura de correo electrónico.

4: * Ver apartado 7

5.4. Revisión de informes

- **Analizar los informes de DMARC** para determinar qué porcentaje de correos electrónicos se autentican correctamente y cuáles fallan la autenticación.
- **Identificar cualquier patrón de comportamiento sospechoso** o actividad no autorizada que pueda requerir acciones adicionales.
- **Utilización de herramientas de terceros para obtener gráficas, resúmenes, inteligencia, métricas y** soporte en base a los datos concretos de la entidad en ese momento.

6. Implementación progresiva y refinamiento

6.1. Estrategias para incremento progresivo de la política

- **Desarrollar un cronograma** para revisar y aumentar la proporción de correos enviados a cuarentena. Por ejemplo, puede comenzar con un porcentaje bajo **(P0)*** y aumentarlo gradualmente **(Pin)*** si los niveles de alineamiento de DMARC se mantienen o mejoran y se reduce la incidencia de falsos positivos.
- **Supervisar el impacto** de la política actual en los flujos de correo legítimo y realizar pruebas de validación para corroborar que los correos legítimos no sean marcados como sospechosos o bloqueados.
- **Ajustar la configuración**[5] de los registros SPF y DKIM basándose en los hallazgos de las revisiones para mejorar el nivel de alineamiento de DMARC.

6.2. Preparación para políticas más estrictas

Una vez alcanzado el nivel máximo (porcentaje de aplicación al 100%) de la política establecida y si los niveles de alineamiento se mantienen por encima del 95% (si la política es *none*) o del 98% (si la política es *quarantine*), se puede considerar la posibilidad de implementar una política más estricta. Se debe aplicar la misma estrategia especificada anteriormente: iniciar con un porcentaje bajo y aumentarlo gradualmente.

5: * Ver apartado 7

6.3. Monitorización continua

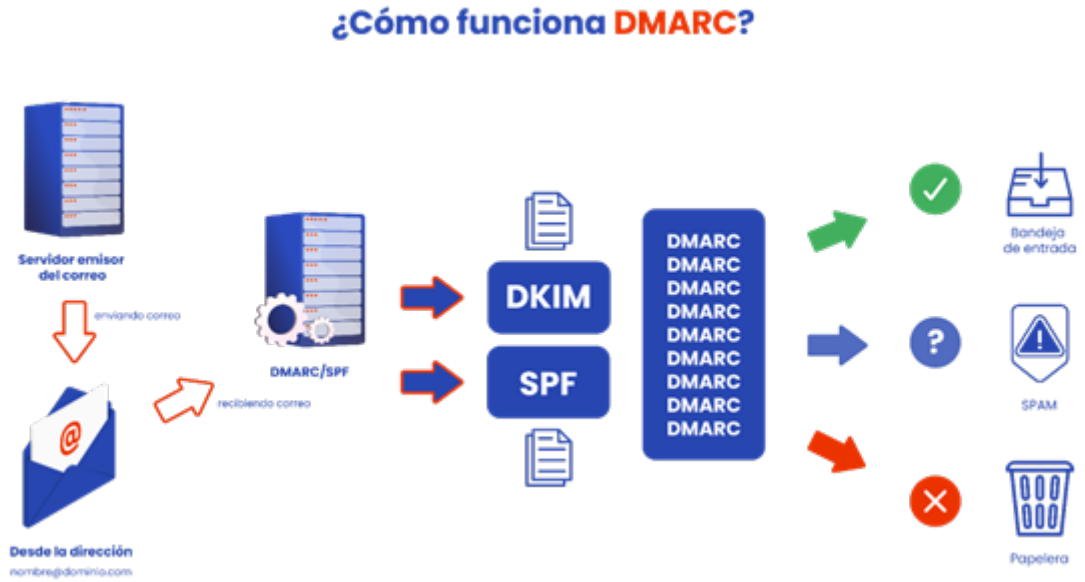
- **Continuar monitorizando** los informes de DMARC para identificar cualquier cambio en el comportamiento del correo electrónico.
- **Tomar medidas correctivas** según sea necesario para abordar cualquier problema nuevo que surja con la autenticación de correo electrónico.

6.4. Actualización y mantenimiento

- **Mantener actualizados los registros SPF y DKIM** según sea necesario para reflejar cambios en la infraestructura de correo electrónico.
- **Realizar auditorías periódicas de la configuración** de DMARC y la autenticación de correo electrónico para garantizar su efectividad continua.

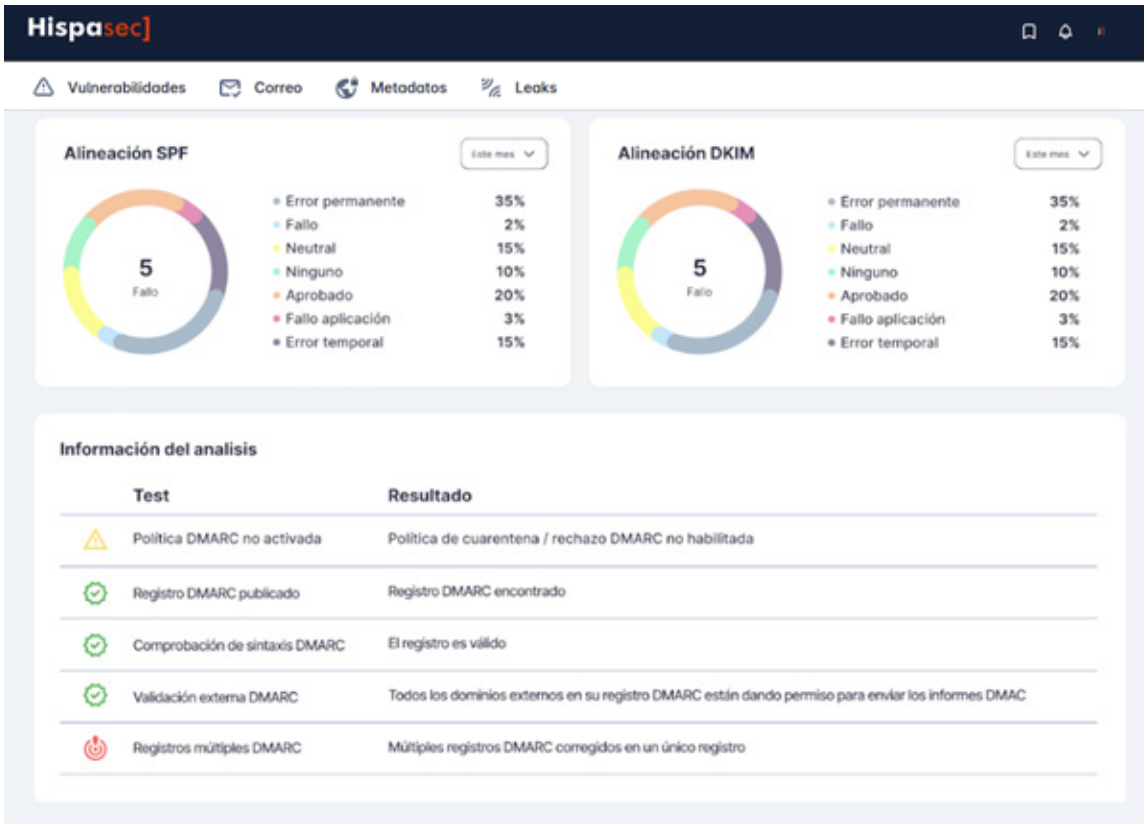
7. Implantación, consideración por volumen de proveedores y tamaño de la entidad

En este punto queremos ver cómo se implanta con pasos, números y ejemplos de implantación. Un breve recordatorio en este punto es que debemos tener en cuenta que el punto de partida es la política “none”. Una vez hemos alineado todos los proveedores, configurado el SPF y el DKIM correctamente, introducimos la política “quarantine” (cuarentena). Esta envía a spam el correo no alineado, tras una implantación exitosa con esta política, podemos plantearnos el siguiente paso, siempre teniendo en cuenta los riesgos asociados y pasar a una política “reject” o rechazo. Esto causará que el correo no alineado desaparezca en el buzón destino, no siendo visible ni en la carpeta de spam.



7.1. Identificación de datos y métricas importantes para evaluar y cuáles podrían considerarse buenos indicadores para avanzar

En este punto vamos a tratar los ajustes eficaces de una implementación de DMARC y a tomar decisiones informadas sobre cómo avanzar con las políticas de SPF y DKIM. En este proceso es esencial analizar detalladamente los datos de alineación y el rendimiento.



7.1.1. Tasa de alineamiento de SPF y DKIM

Se debe observar el porcentaje de correos que pasan las verificaciones de SPF y DKIM.

Idealmente, lo ideal sería que este porcentaje sea del 100%, pero en la práctica, **un porcentaje superior al 95%** es generalmente aceptable para considerar que las políticas están funcionando bien.

El caso más común en entidades que se enfrentan por primera vez a este proceso, por facilidad de implementación, es tener SPF bien alineado (apartado 3.1.) y tener ciertos problemas con la implementación de DKIM (apartado 3.2.). **Si observamos que el porcentaje de alineación de DKIM es bajo, es crucial reforzar la configuración de SPF para asegurar un alto porcentaje de cumplimiento en esta área.**

Un SPF robusto puede compensar parcialmente las debilidades de DKIM, especialmente en el contexto de DMARC, donde ambos mecanismos contribuyen a la tasa general de cumplimiento.

Para mejorar la eficacia de SPF en este escenario, una medida importante a considerar es ajustar la directiva adkim en el registro DMARC. Esta directiva controla la alineación de DKIM, establecer **adkim=s (alineación estricta) podría ser contraproducente si la alineación de DKIM es baja,** por lo que ajustarla a adkim=r (alineación relajada) puede ser más beneficioso. Esto significa que sólo se requiere que la parte del dominio en la firma DKIM coincida con la del dominio en el campo "From:" del encabezado del correo, en lugar de una coincidencia exacta.

Este cambio puede ayudar a mejorar la tasa de correos que pasan DMARC, permitiendo una mayor flexibilidad en la validación de DKIM mientras se confía más en la robustez de SPF.

Esta casuística puede aplicarse en el otro sentido, si DKIM tiene una facilidad de implantación, pero el SPF no por problemas con el proveedor, en este caso el parámetro a evitar sería aspf=s.

7.1.2. Tasa de alineamiento de DMARC

Es crucial medir el porcentaje de correos electrónicos que cumplen completamente con DMARC, lo que significa que tanto SPF como DKIM están alineados correctamente y pasan las verificaciones.

Al igual que con SPF y DKIM, **una tasa de cumplimiento de DMARC superior al 95% es un buen indicador** de que las cosas están yendo bien. Este escenario no siempre es fácil de lograr.

Hay una alineación muy importante y la más común en las entidades primerizas en este proceso que es la **alienación parcial,** este es el término que se utiliza para para describir una situación donde solo uno de los métodos, SPF o DKIM, está bien alineado con el dominio "From", mientras que el otro no. Esto es lo que podría estar sucediendo:

- **SPF tiene un alto nivel de alineación, pero DKIM no.** Esto significa que los correos electrónicos pasan la verificación SPF correctamente, y el dominio utilizado en SPF coincide o está relacionado con el dominio. Sin embargo, la firma DKIM puede estar fallando o no estar alineada correctamente.

- **DKIM tiene un alto nivel de alineación, pero SPF no.** En este caso, la firma DKIM es válida y el dominio que firma el mensaje está correctamente alineado con el dominio, pero la verificación de SPF está fallando, ya sea porque los correos no vienen de los servidores listados en el registro SPF o porque el dominio SPF no coincide con el "From".

Este porcentaje de alineamiento relajado no da el dato de cuántos de los correos pasan al menos una de las validaciones, pudiendo entre los dos parámetros a medir tener un porcentaje de alineamiento parcial muy alto, superior a un 90% o 95%. Esta casuística no es idónea, pero es una medición importante cuando una de las implantaciones no está avanzando al nivel deseado o necesario. Este porcentaje no tiene el peso del alineamiento antes explicado, pero sí tiene un peso en la medición de la salud y el avance de la implementación.

Este proceso midiendo el alineamiento relajado permite una mayor flexibilidad. Los correos enviados desde subdominios o con firmas de subdominios pueden pasar la comprobación de DMARC más fácilmente. Esto es particularmente útil para organizaciones grandes con múltiples unidades de trabajo o servicios externos que envían correos en su nombre.

No podemos dejar de lado el proceso de revisar los reportes de fallos y los reportes agregados para identificar patrones de fallos, tipos de errores más comunes, y fuentes de envío problemáticas. Estas mediciones deben tener en cuenta datos como frecuencia de fallos, fuentes de envío recurrentes con problemas, y tipos específicos de errores de configuración o alineación.

7.1.3 Consideraciones para avanzar con las políticas de DMARC

- **Análisis de los Reportes**, antes de hacer cualquier cambio en la política de DMARC, asegúrate de analizar a fondo los reportes DMARC. Identifica las causas de los fallos y abordarlas antes de avanzar a políticas más restrictivas.
- **Implementación Gradual,** si los datos indican un alto cumplimiento y alineación, considere mover la política de DMARC de none a quarantine. Comience con un pequeño porcentaje, como un pct=10, y aumenta gradualmente si los resultados son positivos.
- **Comunicación con proveedores de correo,** si trabaja con terceros para enviar correos en su nombre, asegúrese de que estén informados sobre tus políticas DMARC y que sus sistemas están configurados para cumplir con sus requisitos de SPF y DKIM.
- **Educación continua y pruebas,** continúe educando a su equipo sobre las mejores prácticas de DMARC, SPF y DKIM. Realice pruebas periódicas para asegurarse de que las configuraciones siguen siendo efectivas a medida que cambian las infraestructuras de red y los patrones de envío de correo electrónico.

Al seguir estos pasos y mantener una monitorización constante de los datos de alineación de DMARC, SPF y DKIM, puede avanzar de manera segura hacia una política de DMARC más restrictiva, lo que mejorará la seguridad del correo electrónico y la protección contra el fraude y la suplantación de identidad.

Para este proceso es muy recomendable contar con un proveedor de métricas, gráficas y toda la información de los reportes agregados que vienen originalmente en formato XML representado en gráficos. La capacidad de convertir datos brutos en gráficas y visualizaciones es fundamental para el análisis rápido y efectivo. Para conocer estos porcentajes de alineamiento DMARC, alineamiento parcial, alineamiento SPF, alineamiento DKIM y su evolución a lo largo del tiempo. Además, estas plataformas también le permiten descubrir de un vistazo el listado de los proveedores con más fallos en cada una de las categorías, incluso hacer un análisis en profundidad con facilidad.

7. Implantación, consideración por volumen de proveedores y tamaño de la entidad

Las **visualizaciones** pueden destacar tendencias, picos en intentos de suplantación, y otros eventos críticos que podrían requerir atención inmediata. Esto es particularmente útil durante las revisiones de seguridad y las presentaciones a la gerencia, donde las representaciones visuales pueden ser mucho más impactantes que los números crudos.

Un buen proveedor ofrecerá herramientas para la **monitorización continua,** lo que permite a las organizaciones reaccionar rápidamente a nuevos riesgos y amenazas a medida que surgen. Esto es esencial en un paisaje de amenazas en constante evolución, donde la capacidad de adaptarse rápidamente puede significar la diferencia entre un incidente menor y una violación de seguridad significativa.

Además de organizar y visualizar datos, los proveedores pueden **ofrecer informes accionables** que destacan problemas específicos y sugieren medidas correctivas. Esto puede incluir recomendaciones para la reconfiguración de registros SPF o DKIM, ajustes en la política DMARC, o incluso alertas sobre comportamientos de envío anormales que podrían indicar una cuenta comprometida.

Las empresas a menudo necesitan **demostrar cumplimiento** con diversas regulaciones de seguridad y privacidad. Un proveedor que pueda generar informes detallados y precisos es invaluable para simplificar los procesos de auditoría y garantizar que las políticas de seguridad cumplan con las normativas aplicables.

Elegir un proveedor que pueda ofrecer servicios avanzados de organización, análisis y visualización de datos relacionados con DMARC, SPF y DKIM es esencial para las organizaciones que buscan optimizar su seguridad de correo electrónico y garantizar la integridad y confiabilidad de sus comunicaciones.

7.2. Entidades pequeñas o con 5 o menos proveedores diferentes de correo electrónico

Para entidades con 5 o menos proveedores diferentes de correo y otras entidades públicas de tamaño similar, la implementación de DMARC puede parecer una tarea más sencilla dado el número de proveedores. Es esencial para proteger tanto su comunicación como la de sus ciudadanos. Aquí se detallan los niveles recomendados:

- **Revisar los niveles de alineamiento con una periodicidad (Te) de 60-90 días.**
- **Porcentaje inicial (P0) para políticas *quarantine* o *reject*: 10%.**
- **Tasa de incremento (Pin) de porcentaje para políticas *quarantine* o *reject*: +10%.**

Debemos trabajar siempre con el **apartado 3.3.** como referencia, quedando una configuración de ejemplo:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=30; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Que, tras una revisión favorable, se decide avanzar a:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=40; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Tras una nueva revisión favorable, se decide avanzar a:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=50; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Y así consecutivamente avanzando siempre que los resultados sean favorables y no detectemos pérdida de correo.

7.3. Entidades con más de 5 proveedores, de importancia media[6]

Las entidades de importancia media o más de 5 proveedores de correo electrónico tienen una responsabilidad sustancial en la protección de la información debido a la cantidad de datos sensibles que manejan y su potencial impacto en una mayor población. Aquí se detallan los niveles recomendados:

- **Revisar los niveles de alineamiento con una periodicidad (Te) de 45-60 días.**
- **Porcentaje inicial (P0) para políticas *quarantine* o *reject*: 5%.**
- **Tasa de incremento (Pin) de porcentaje para políticas *quarantine* o *reject*: +5%.**

Debemos trabajar siempre con el apartado 3.3. como referencia, quedando una configuración de ejemplo:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=30; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

6: Ayuntamientos de entre 100.000 y 1.000.000 de habitantes, Diputaciones Provinciales, Hospitales y Centros Sanitarios, Universidades, Cabildos y Entidades Públicas de tamaño medio.

Que, tras una revisión favorable, se decide avanzar a

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=35; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Tras una nueva revisión favorable, se decide avanzar a

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=40; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Y así consecutivamente avanzando siempre que los resultados sean favorables y no detectemos pérdida de correo.

7.4. Entidades críticas[7]

Las entidades críticas gestionan datos altamente confidenciales y proporcionan servicios esenciales que, si se ven comprometidos, podrían tener consecuencias graves para la seguridad nacional y el bienestar público. Por esta razón, la adopción de DMARC debe ser particularmente rigurosa y metódica, aspirando a una alineación con las políticas más estrictas. Aquí se detallan los niveles recomendados:

- **Revisar los niveles de alineamiento con una periodicidad (Te) de 30-45 días.**
- **Porcentaje inicial (P0) para políticas *quarantine* o *reject*: 2%.**
- **Tasa de incremento (Pin) de porcentaje para políticas *quarantine* o *reject*: +2%.**

Debemos trabajar siempre con el apartado 3.3. como referencia, quedando una configuración de ejemplo:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=30; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

7: Ministerios, Comunidades Autónomas, Ejército y Fuerzas de Seguridad del Estado, Infraestructuras Críticas.

7. Implantación, consideración por volumen de proveedores y tamaño de la entidad

Que, tras una revisión favorable, se decide avanzar a:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=32; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Tras una nueva revisión favorable, se decide avanzar a:

```
_dmarc.entidad.com. IN TXT "v=DMARC1; p=quarantine; pct=34; fo=1;
rua=mailto:dmarc@hispasec.com; ruf=mailto:dmarc@hispasec.com;"
```

Y así consecutivamente avanzando siempre que los resultados sean favorables y no detectemos pérdida de correo.

8. Implicaciones de la implementación

8.1. Qué no hace DMARC

No cifra los correos electrónicos, DMARC no proporciona ningún mecanismo de cifrado para los correos electrónicos. Su función es autenticar la fuente del correo electrónico y asegurar que no haya sido alterado en tránsito, no mantener el contenido del mensaje seguro de interceptaciones.

No previene el spam, aunque DMARC puede ayudar a reducir ciertos tipos de correo no deseado (como aquellos que intentan suplantar la identidad de un dominio), no está diseñado como una herramienta anti-spam en general. No bloqueará correos spam que no intenten falsificar la dirección del remitente.

No funciona sin SPF y DKIM, DMARC depende de SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail) para funcionar. Sin estos dos mecanismos de autenticación configurados, DMARC por sí solo no puede operar.

No garantiza la entrega de correos electrónicos: Aunque DMARC puede mejorar la reputación de un dominio al reducir la posibilidad de que los correos sean marcados como falsos, no garantiza que todos los correos legítimos serán entregados. La entrega de correos también depende de otros factores como la reputación del dominio y la configuración del servidor receptor.

No protege contra todos los tipos de ataques de phishing, DMARC es efectivo contra ataques de phishing que implican la suplantación de un dominio en la dirección del remitente, pero no detiene los ataques que utilizan dominios visualmente similares o que no intentan suplantar directamente el dominio de una entidad conocida.

- **No corrige automáticamente configuraciones erróneas de SPF y DKIM,** Mientras que DMARC puede informar al administrador del dominio sobre los problemas con las configuraciones de SPF y DKIM a través de sus reportes, no ofrece soluciones automáticas para corregir estos problemas. Es responsabilidad del administrador del dominio hacer los ajustes necesarios.

- **No controla la política de manejo de correos de los receptores,** aunque DMARC permite a los propietarios de dominios sugerir cómo deben ser tratados los correos que fallan en las verificaciones SPF y DKIM, los servidores de correo receptores tienen la última palabra sobre cómo procesar estos correos. Esto significa que diferentes servidores pueden manejar los fallos de DMARC de maneras distintas.

- **No bloquea la interceptación de correos electrónicos,** DMARC no puede prevenir que un atacante intercepte o lea correos electrónicos en tránsito; su función principal es validar la autenticidad del remitente y la integridad del mensaje.

Al comprender lo que DMARC no puede hacer, las organizaciones pueden tomar medidas adicionales para asegurar sus comunicaciones y sistemas de correo electrónico de manera más efectiva.

8.2. Riesgos del desconocimiento o el no uso de DMARC

- **Aumento de la suplantación de identidad (spoofing),** sin DMARC, los atacantes pueden enviar correos electrónicos que aparentan ser del dominio de la organización más fácilmente. Esto puede conducir a ataques de phishing efectivos contra clientes, empleados o socios comerciales, quienes pueden ser engañados para que divulguen información confidencial o realicen acciones maliciosas, como transferencias de dinero fraudulentas.

- **Daño a la reputación del dominio y de la marca,** si los atacantes utilizan con éxito un dominio para enviar spam o malware, esto puede dañar la reputación de la marca asociada. Los clientes pueden perder confianza en la organización, y los dominios pueden ser incluidos en listas negras por servicios de correo electrónico y filtros de spam, afectando la entrega de correos legítimos.

- **Pérdida de control sobre la política de envío de correo,** al no especificar y hacer cumplir una política de envío de correos electrónicos a través de DMARC, las organizaciones pierden la oportunidad de definir y controlar quién puede enviar correos en nombre de sus dominios, lo que incrementa el riesgo de abuso.

- **Dificultad para identificar abusos y ataques** sin los informes de DMARC, las organizaciones pueden no ser conscientes de que su dominio está siendo utilizado para suplantación o de otros problemas de seguridad relacionados con el correo electrónico. Esto retrasa la capacidad de respuesta ante incidentes y reduce la efectividad de las medidas de mitigación.

- **Impacto en la confiabilidad de la comunicación,** los correos electrónicos enviados desde dominios sin una política DMARC clara pueden ser tratados con mayor sospecha por los servidores de correo receptores. Esto puede llevar a una mayor tasa de correos marcados como spam o incluso bloqueados, afectando la comunicación efectiva con clientes y socios.

- **Vulnerabilidad a ataques dirigidos,** las organizaciones sin DMARC son más vulnerables a ataques de spear phishing y otros tipos de ataques dirigidos, ya que los atacantes pueden explotar la falta de autenticación de correo electrónico para realizar ataques más convincentes y difíciles de detectar.

La falta de implementación de DMARC puede exponer a las organizaciones a riesgos de seguridad más elevados y a consecuencias negativas tanto operativas como estratégicas. Por tanto, adoptar DMARC es una parte importante de la estrategia de seguridad en correo electrónico para proteger los recursos y la integridad de una organización.

8.3. Riesgos de pérdida de correo electrónico o que este sea recibido como spam

Cuando se implementa DMARC, es crucial **comprender los riesgos asociados con la pérdida potencial de correos electrónicos legítimos.**

8. Implicaciones de la implementación

La implementación de **DMARC** está diseñada para **mejorar la seguridad** del **correo electrónico** al verificar que los **mensajes** procedentes de su **dominio** sean **auténticos** y no hayan sido **alterados** en tránsito. A pesar de sus **beneficios** en la protección contra la **suplantación de identidad** y el **phishing**, la configuración de **DMARC** no está exenta de ciertos **riesgos**, especialmente relacionados con la posible **pérdida** de correos electrónicos **legítimos**.

La incorrecta configuración de los registros **SPF** y **DKIM**, que son esenciales para DMARC, puede llevar a una mayor cantidad de **rechazos o cuarentenas** de correos legítimos. Esto se debe a que los correos que no pasan las **verificaciones** pueden ser automáticamente **rechazados o filtrados** dependiendo de la política de DMARC establecida (p.ej., 'reject' o 'quarantine').

Las **modificaciones en la infraestructura** de correo electrónico, como la adición de nuevos **servidores** de envío o servicios de **terceros** que no están incluidos en los registros **SPF** o no tienen configurado **DKIM**, pueden resultar en fallos de autenticación que afecten la entrega de correos electrónicos legítimos.

Los **servidores** de correo receptores tienen la **autonomía** para decidir cómo procesar los correos que fallan en las verificaciones de DMARC. Incluso con una política de 'none', los correos que fallan podrían ser tratados de manera más **restrictiva por algunos proveedores de correo,** lo que podría impactar la entrega de mensajes legítimos, existe una cierta dependencia del manejo de correos por parte de terceros.

Los cambios en los **registros DNS**, incluyendo los de **DMARC, SPF y DKIM,** pueden tardar en propagarse. Durante este período, los correos electrónicos pueden no autenticarse correctamente, lo que podría afectar temporalmente la entrega de correos legítimos.

Mientras **DMARC** puede significativamente mejorar la seguridad de su correo electrónico, es vital abordar estos **riesgos** mediante una **cuidadosa planificación, configuración precisa y monitorización constante.** De ahí la recomendación de iniciar una implementación de DMARC en modo de **monitorización** (p=none) y ajustar gradualmente la política como se trabaja en el documento, a medida que se verifique la correcta configuración y funcionamiento de los registros **SPF** y **DKIM** asociados. Asimismo, se hace especial énfasis en la recomendación de formar al **personal técnico** involucrado sobre la importancia de una configuración adecuada y la necesidad de adaptarse a cambios en la infraestructura de **correo electrónico** para minimizar la interrupción de la comunicación legítima.

En la actualidad algunos de los grandes proveedores de correo electrónico trabajan con grandes volúmenes de correos electrónicos, generando la necesidad de autoescalado de sus infraestructuras en cualquier momento de manera puntual, por eso es muy importante definir correctamente **DKIM y SPF** ya que con estos grandes proveedores, por la volatilidad y picos de carga de sus necesidades, se corre un riesgo de no alinear en la totalidad de los casos ambos parámetros, teniendo que trabajar solo con la validación de uno de ellos, esto es común cuando se usan proveedores de correo. Por las necesidades de estos proveedores pueden desplegar bloques de servidores fuera de los rangos o no desplegarse a tiempo las claves de **DKIM** y enviar correos no alineados correctamente. Este porcentaje es residual, pero debe tenerse en cuenta.

8.4. Importancia de la configuración de DMARC en dominios que no envían correo electrónico

La configuración de DMARC en **dominios que no envían correo electrónico es una práctica de seguridad esencial** que a menudo se pasa por alto, pero que puede tener implicaciones significativas en la protección de la reputación y la identidad de una marca. Aunque un dominio no esté activamente enviando correos, aún puede ser objeto de suplantación y otros tipos de abusos. Implementar DMARC en estos dominios ayuda a prevenir tales problemas y **no tiene los riesgos anteriormente negociados.**

Uno de los principales beneficios de configurar DMARC en dominios que no envían correo es **prevenir la suplantación de identidad.** Los atacantes a menudo buscan dominios que parecen legítimos pero que no estén adecuadamente protegidos con políticas de autenticación de correo electrónico. Al configurar DMARC, recomendando en este caso con una política de p=reject, se puede asegurar que ningún correo electrónico supuestamente enviado desde ese dominio sea aceptado por un servidor receptor, cerrando así una vía comúnmente explotada para ataques de phishing.

La **reputación de una marca** puede ser gravemente dañada si su dominio se utiliza en ataques de phishing. Esto puede llevar a una pérdida de confianza del cliente y posibles implicaciones legales, especialmente en industrias altamente reguladas. Configurar DMARC protege el nombre de la empresa asegurando que los correos fraudulentos no sean fácilmente aceptados por los receptores.

Al adoptar DMARC en todos los dominios bajo el control de una organización, **se contribuye a elevar los estándares generales de seguridad del correo electrónico en la red.** Esto no solo protege los dominios individuales, sino que también promueve mejores prácticas que pueden fomentar un entorno en línea más seguro.

En algunas jurisdicciones, existen **regulaciones que requieren protecciones específicas** para la información personal y la seguridad de los datos. Configurar DMARC en todos los dominios puede ser parte de cumplir con estas regulaciones, demostrando un compromiso con la seguridad de la información y la protección de los datos de los clientes.

Aunque un dominio no envíe correo, si es suplantado, podría utilizarse para enviar grandes cantidades de **spam**, que no solo afecta a las víctimas potenciales sino también puede resultar en que el dominio sea incluido en listas negras de correo electrónico.

El punto más reseñable de esta práctica es la **monitorización y conocimiento,** en el supuesto caso de que un atacante o un tercero intentase hacer uso de ese dominio desde el que no se tiene planificado que se envíe correo gracias a los reportes y las herramientas para el análisis de datos que tengamos configuradas (registro rua y ruf) **obtendremos métricas y notificaciones sobre el potencial uso fraudulento que se detecte y conoceremos al momento la existencia de una campaña de phishing** que trate de hacer uso de un dominio configurado.

8.5. Otras recomendaciones

Asegurar una **colaboración efectiva con los principales receptores de correo electrónico,** incluyendo la propia entidad, para facilitar la implementación de DMARC y mejorar la gestión de la seguridad del correo electrónico.

Elabore un plan con bajo nivel de detalle, donde se requiera comunicar lo más básico y no entrar en detalles.

Identifica a los principales receptores de correo electrónico dentro y fuera de la organización, que incluyan departamentos internos clave y socios externos.

Para la **comunicación interna**, organiza una reunión inicial con los equipos de TI y administradores de sistemas para comunicar el plan de implementación de DMARC. Explica la importancia del proceso y cómo puede impactar en la recepción del correo electrónico, enfocándose en la necesidad de monitorizar y ajustar los filtros de spam y las **políticas de recepción para monitorizar lo que se recibe de la propia entidad y cómo se trata.**

Establece un canal de comunicación regular (por ejemplo, reuniones quincenales o grupo de chat en línea) para discutir actualizaciones y resolver problemas relacionados con la implementación de DMARC.

Para la comunicación externa, **envía un comunicado formal a los principales receptores de correo electrónico externos, con los que tengas un trato cordial,** informando sobre el proceso de la implementación de DMARC. El comunicado debe incluir el propósito de la implementación, cómo podría afectar la recepción de correos desde tu dominio, y **solicitar su cooperación** en ajustar sus sistemas de recepción si es necesario.

Establece un proceso para revisar y ajustar la configuración de DMARC basado en la retroalimentación interna y externa.

Centro Criptológico Nacional

20 ANIVERSARIO

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es