**Análisis de Correos Electrónicos**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_oe0sczh5n4lv) **1**

[**2. Actividades**](#_wc8wq5qtqi6h) **2**

[**2.1 Analizar la cabecera para determinar los saltos que ha hecho el correo entre los distintos servidores y el tiempo en estos, para tratar de buscar algún comportamiento anómalo**](#_5d38uxjyswtl) **2**

[**2.1.1 Correo 1**](#_21lyjg3wej4e) **2**

[**2.1.2 Correo 2**](#_pflo67y808vs) **2**

[**2.2 Determinar el lugar de origen (localización física) del envío del correo.**](#_evl9gpy9j4qp) **3**

[**2.2.1 Correo 1**](#_m3ev0d191sxi) **3**

[**2.2.2 Correo 2**](#_rd6wi6vt3z49) **3**

[**2.3 Indicar la IP desde donde se originó el mensaje.**](#_ifcu2em2me1g) **4**

[**2.3.1 Correo 1**](#_t36soclxcdyb) **4**

[**2.3.2 Correo 2**](#_py5zzuhmihrw) **4**

[**2.4 Analizar si se ha suplantado el nombre o el dominio del emisor del correo que ve el usuario receptor del mail (sin conocimientos técnicos), así como determinar si el dominio usado existe realmente (usando comando dig).**](#_pmgxspxhcyr3) **5**

[**2.4.1 Correo 1**](#_w4314uaidnwq) **5**

[**2.4.2 Correo 2**](#_4pg2q8fqxe2q) **5**

[**2.5 Comprobar si se cumplen los protocolos de autenticación.**](#_br21w9gjf24v) **6**

[**2.5.1 Correo 1**](#_5pnmecy0m1s2) **6**

[**2.5.2 Correo 2**](#_4pjpggeenrmo) **6**

[**2.6 Verificar cuál es la dirección de respuesta del correo, comentando si es diferente a la del remitente. Analizar esta dirección.**](#_yae97xrxn0l) **6**

[**2.6.1 Correo 1**](#_h8vwx3wtu2zq) **6**

[**2.6.2 Correo 2**](#_ps5zsk1trh8r) **7**

[**2.7 Verificar el valor del análisis SPF, explicando la razón del valor mostrado, profundizando en el análisis todo lo posible. ¿A qué bandeja habrá entrado cada correo?**](#_a0bmfscbqqx5) **7**

[**2.7.1 Correo 1**](#_e8nounoakdvs) **7**

[**2.7.1 Correo 2**](#_6exbcqsgg0r4) **7**

[**2.8 Mostrar el cuerpo del correo tal y como lo vería el usuario, analizando el propósito del mismo y si existe algo sospechoso.**](#_pfrwfmkcom34) **8**

[**2.8.1 Correo 1**](#_4q88m46l0g9g) **8**

[**2.8.2 Correo 2**](#_4ebk9b2qbqgh) **9**

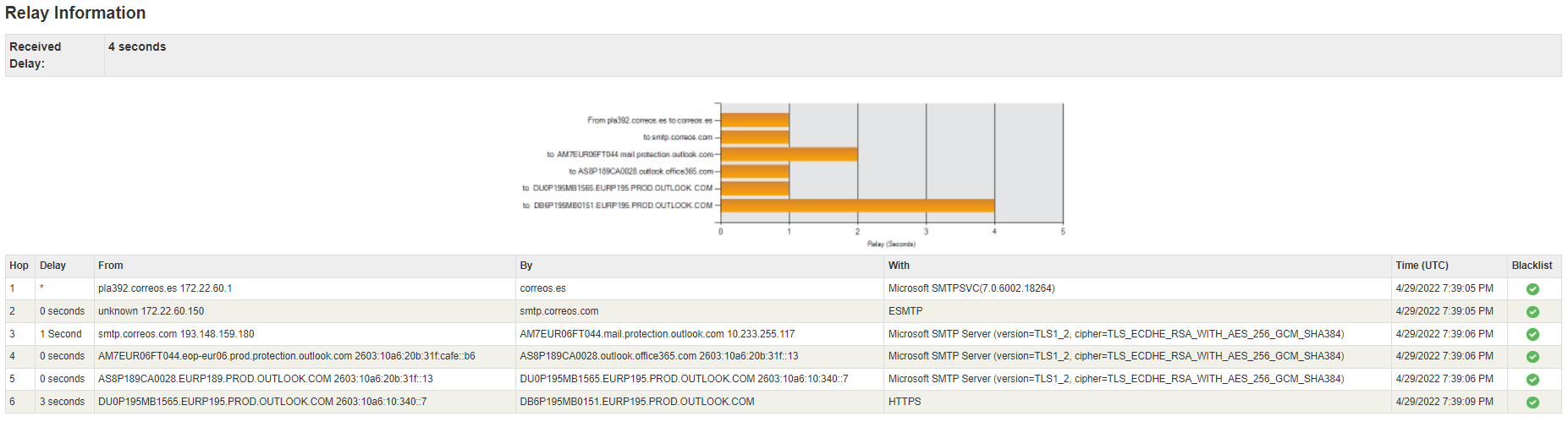
[**2.9 Analizar los enlaces del cuerpo si los tuviera.**](#_a44n10w8ws1t) **9**

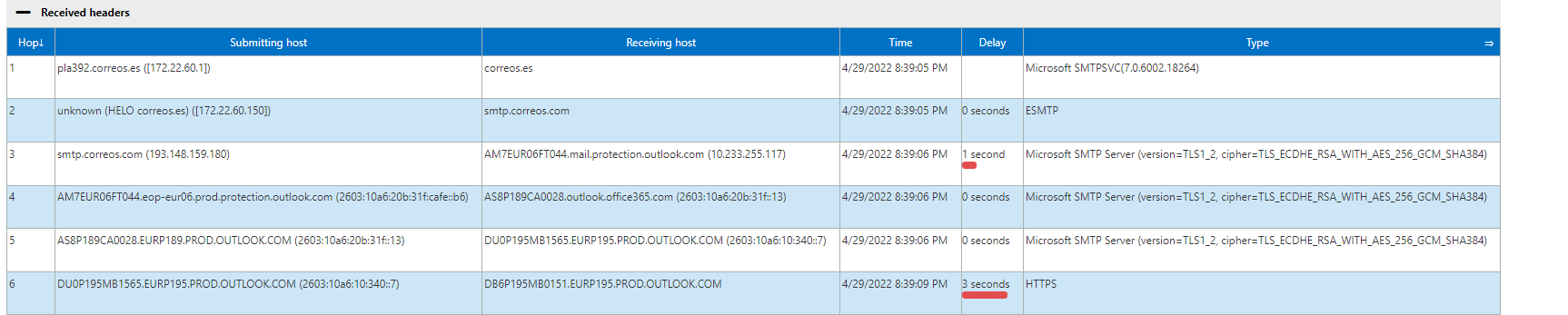
[**2.9.1 Correo 2**](#_dbcpsr9f6lmz) **9**

# **2. Actividades**

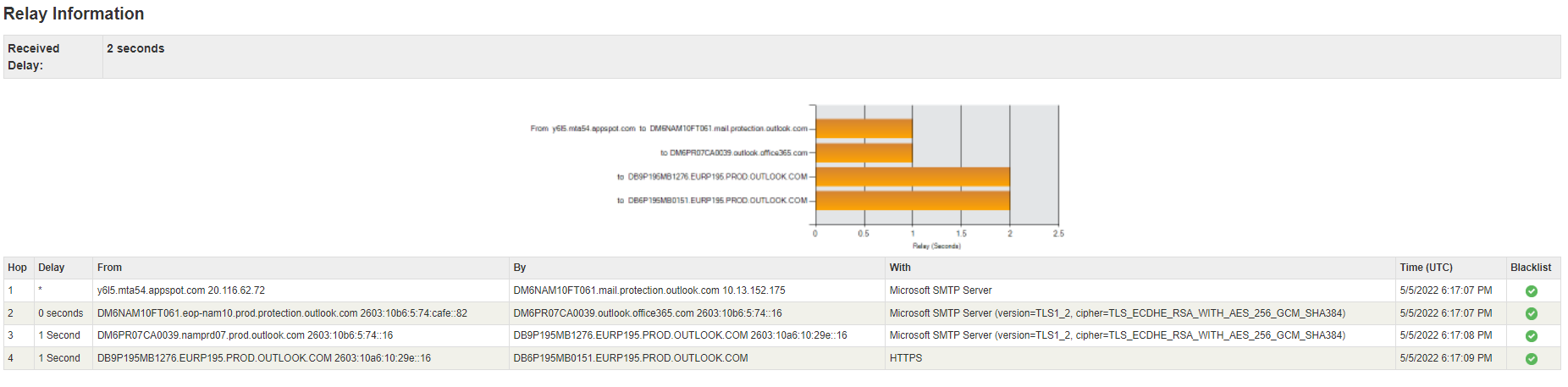
### **2.1 Analizar la cabecera para determinar los saltos que ha hecho el correo entre los distintos servidores y el tiempo en estos, para tratar de buscar algún comportamiento anómalo**

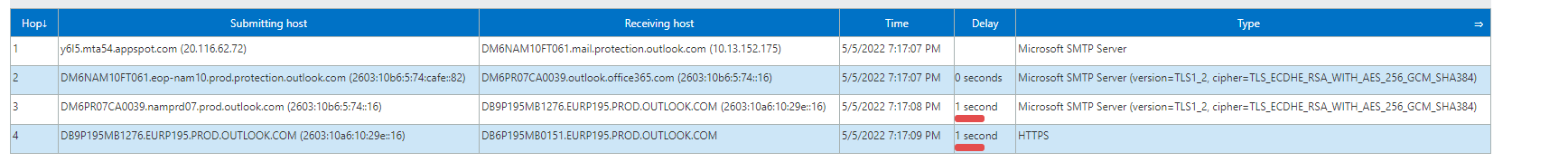
#### **2.1.1 Correo 1**





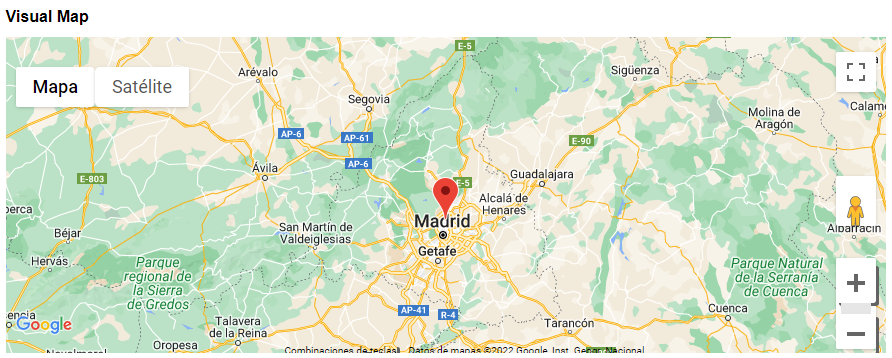
#### **2.1.2 Correo 2**



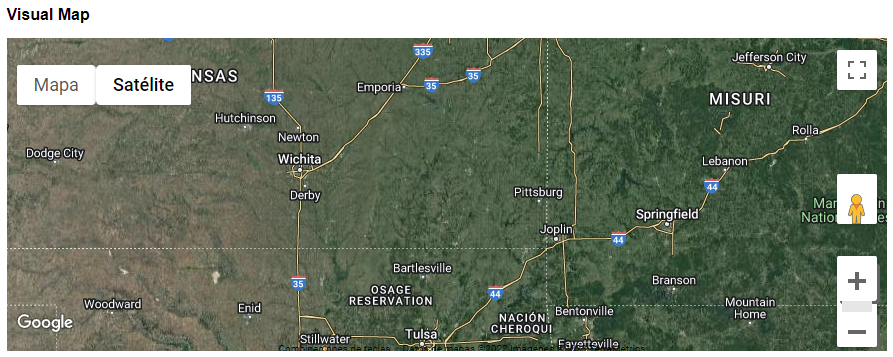


### **2.2 Determinar el lugar de origen (localización física) del envío del correo.**

#### **2.2.1 Correo 1**

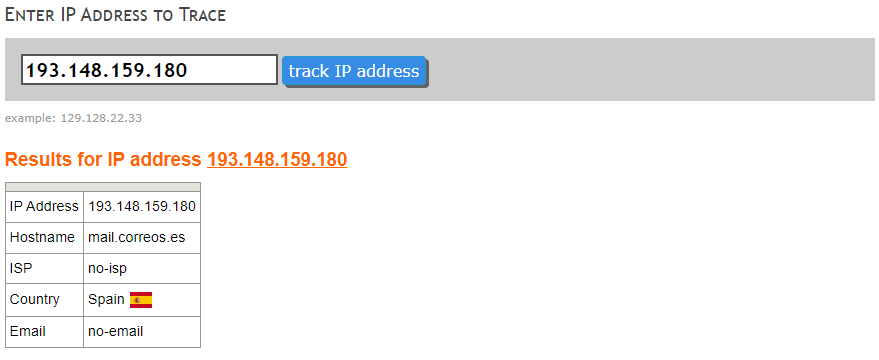


#### **2.2.2 Correo 2**

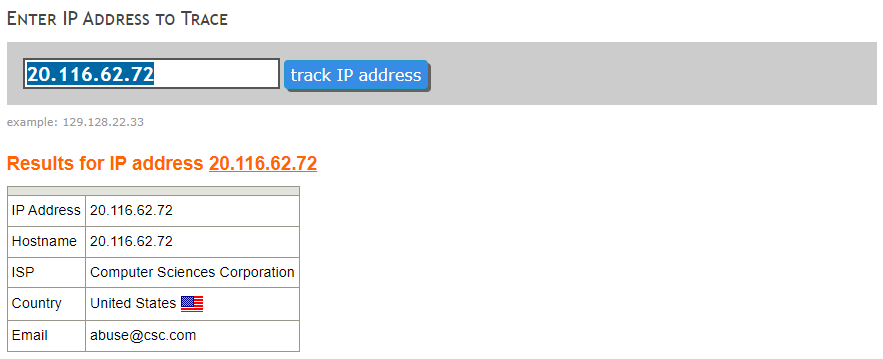


### **2.3 Indicar la IP desde donde se originó el mensaje.**

#### **2.3.1 Correo 1**



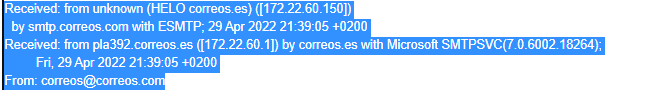
#### **2.3.2 Correo 2**



### **2.4 Analizar si se ha suplantado el nombre o el dominio del emisor del correo que ve el usuario receptor del mail (sin conocimientos técnicos), así como determinar si el dominio usado existe realmente (usando comando dig).**

#### **2.4.1 Correo 1**

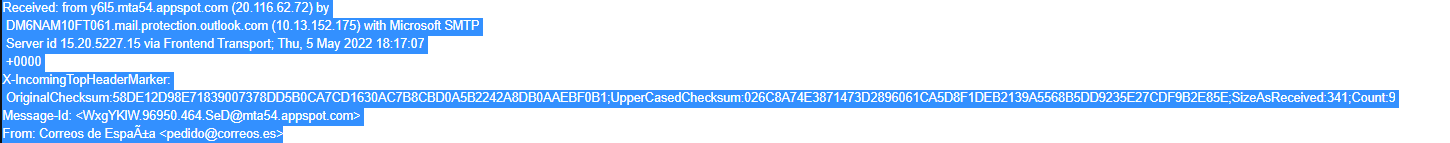
No se ha suplantado.

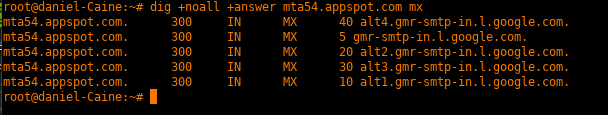




#### **2.4.2 Correo 2**

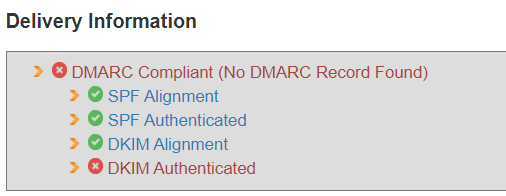
Sí, se ha suplantado.



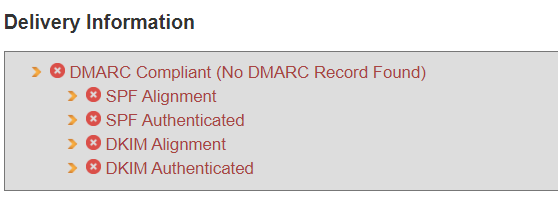


### **2.5 Comprobar si se cumplen los protocolos de autenticación.**

#### **2.5.1 Correo 1**

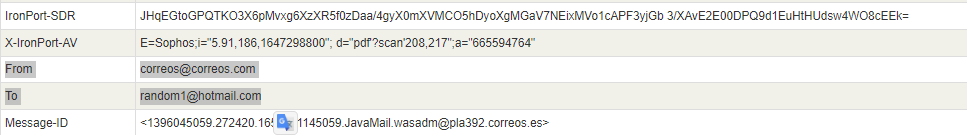


#### **2.5.2 Correo 2**



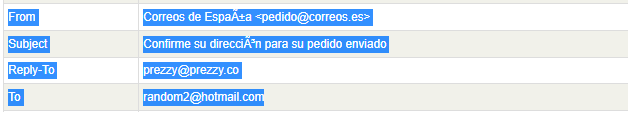
### **2.6 Verificar cuál es la dirección de respuesta del correo, comentando si es diferente a la del remitente. Analizar esta dirección.**

#### **2.6.1 Correo 1**

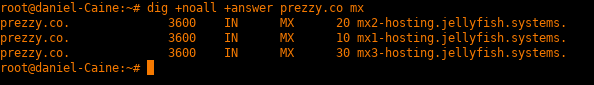


En este caso no hay dirección de respuesta.

#### **2.6.2 Correo 2**

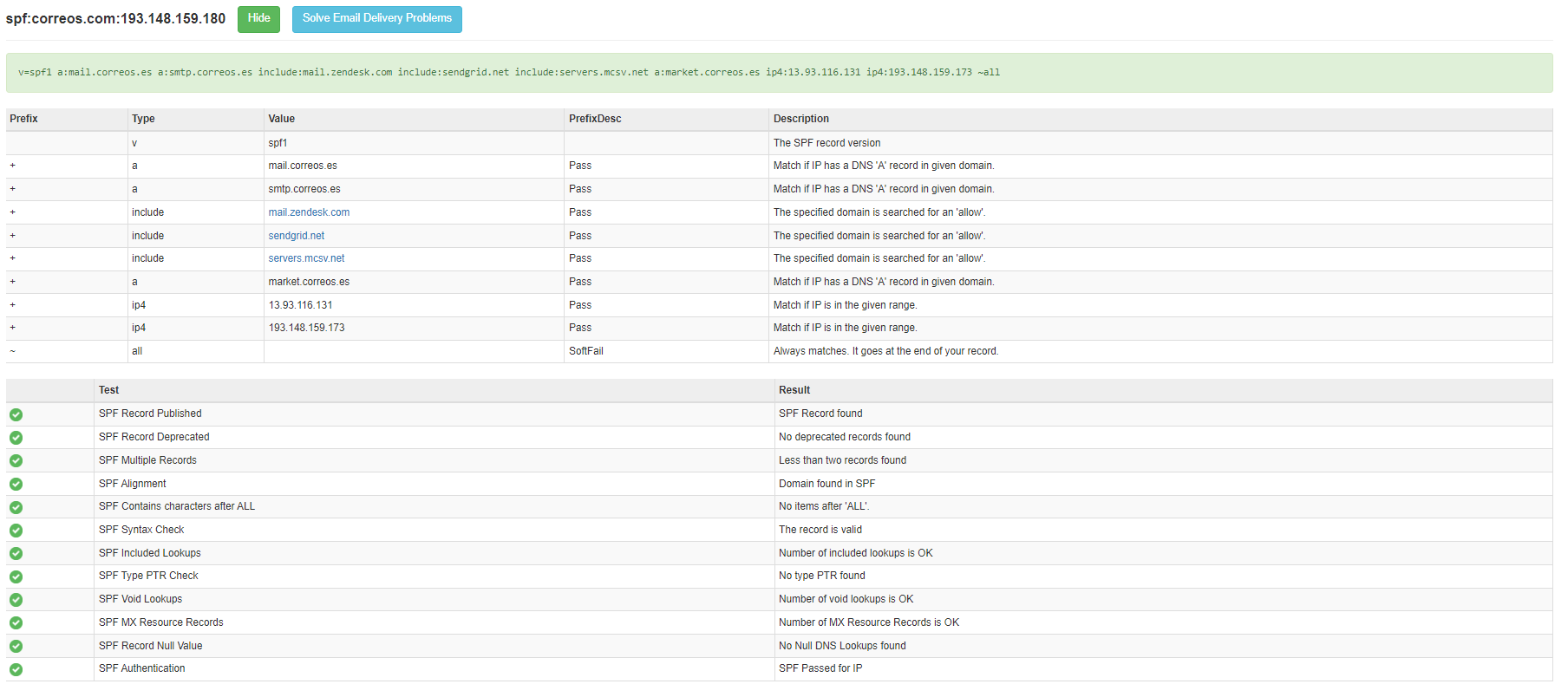


En este caso la dirección de respuesta es diferente tanto a la del emisor, como a la del receptor. La analizamos:



### **2.7 Verificar el valor del análisis SPF, explicando la razón del valor mostrado, profundizando en el análisis todo lo posible. ¿A qué bandeja habrá entrado cada correo?**

#### **2.7.1 Correo 1**



A la bandeja de recibidos ya que el valor del análisis SPF es positivo.

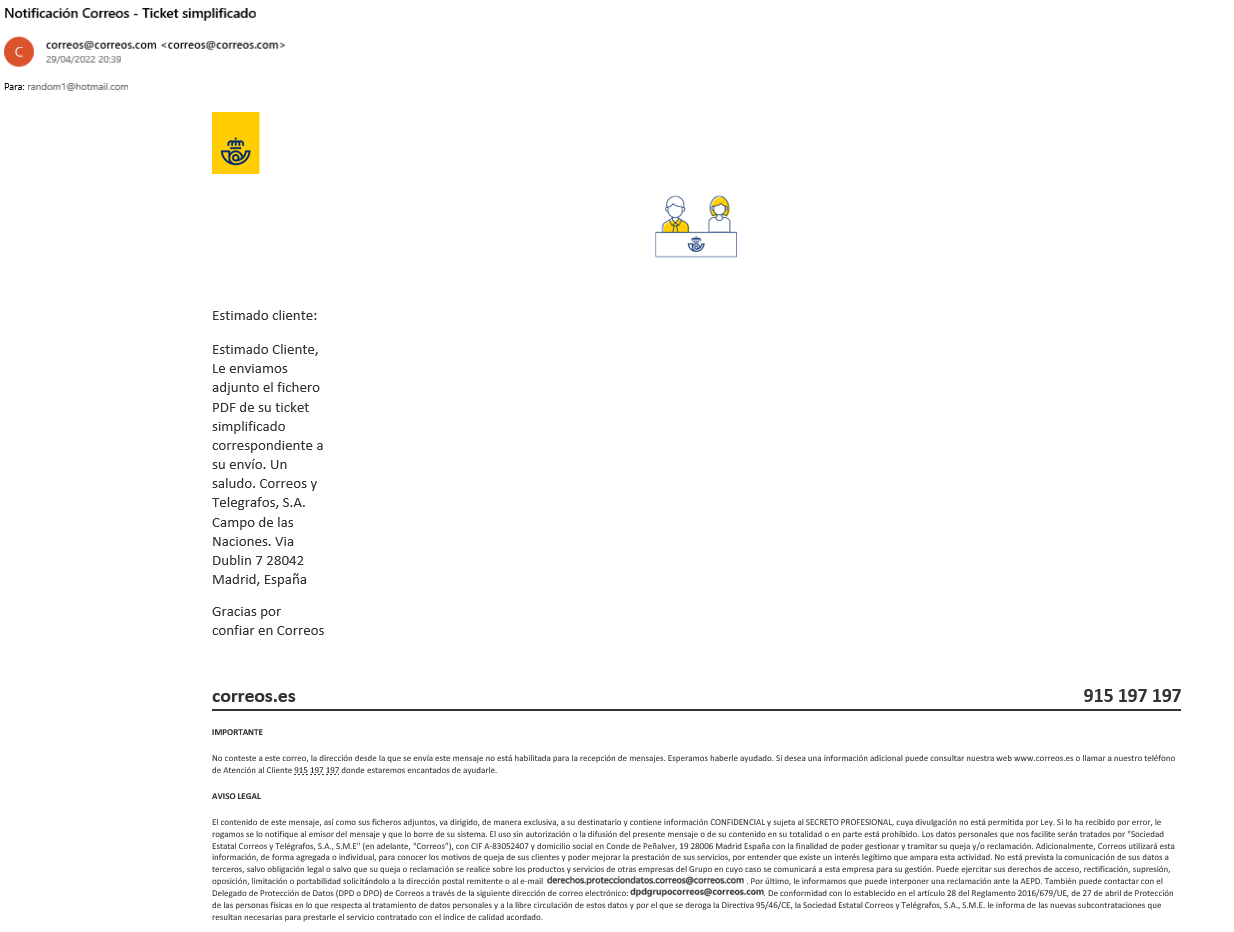
#### **2.7.1 Correo 2**



A la bandeja de SPAM o no deseados. Ya que el valor del análisis SPF es negativo.

### **2.8 Mostrar el cuerpo del correo tal y como lo vería el usuario, analizando el propósito del mismo y si existe algo sospechoso.**

#### **2.8.1 Correo 1**



Bastante estándar este correo, nada sospechoso, el formato se modificó un poco al utilizar esta aplicación.

#### **2.8.2 Correo 2**



Lo más sospechoso de este correo electrónico, son la cantidad de enlaces que podemos visualizar y acceder.

### **2.9 Analizar los enlaces del cuerpo si los tuviera.**

#### **2.9.1 Correo 2**

Estos son los enlaces que podemos encontrar en el cuerpo del correo, como podemos observar, uno es un intento de falsificación de la página oficial de correos, la cual es “correos.com”. Además el otro enlace es bastante sospechoso, intenta imitar un enlace para desuscribirse de estos correos.

"https://cerreos.page.link/6SuK"

"https://unsubdown2.com/unsubscribe/random2@hotmail.com/2/FR"