Problemas con redirecciones de correo a Gmail

Tengo mi dirección de correo de la UNED redirigida a mi dirección de correo de Gmail y los mensajes que me envían desde Yahoo no llegan. En su lugar recibo un informe de error incomprensible.

Vaya por delante que a día de hoy la única solución a este problema es cancelar la redirección de la cuenta de correo de la UNED hacia Gmail. Si quiere seguir usando la interfaz de Gmail para leer su cuenta de correo de la UNED deberá configurar un acceso POP o IMAP a la cuenta UNED desde su cuenta de Gmail.

La solución a largo plazo pasa por que Microsoft programe SRS *(*Sender Rewriting Scheme*)* en la plataforma Office365. La única posibilidad de conseguirlo pasa por votar en esta url: https://office365.uservoice.com/forums/289138-compliance-protection/suggestions/12857109-implement-sender-rewriting-scheme-srs-to-resolve

El mensaje de error

```
Error Details
Reported error:    550 5.7.23 The message was rejected because of
                   Sender Policy Framework violation -> 550 5.7.1
                   Unauthenticated email from yahoo.es is not
                   accepted due to domain's;DMARC policy. Please
                   contact the administrator of yahoo.es domain
                   if;this was a legitimate mail. Please visit;
                   https://support.google.com/mail/answer/2451690
                   to learn about the;DMARC initiative.
                   u78si5937673oif.187 - gsmtp
Retry count:       1
DSN generated by:  HE1PR0701MB2668.eurprd07.prod.outlook.com
Remote server:     mx.google.com
```

Es decir, el servidor de Office365, HE1PR0701MB2668.eurprd07.prod.outlook.com, ha intentado pasarle el mensaje de correo enviado desde yahoo.es al servidor de correo de Gmail, mx.google.com. El servidor mx.google.com ha rechazado el mensaje alegando que no se cumplen las condiciones de la política de correo de yahoo.es *(*DMARC policy*)* porque no se está cumpliendo con SPF *(*Sender Policy Framework*)*.
Es decir, el servidor HE1PR0701MB2668.eurprd07.prod.outlook.com no es un servidor de Yahoo y por tanto no acepto nada que sea de Yahoo y venga de ti.

¿Y cómo sabe Gmail cual es la política de correo de Yahoo?

Las organizaciones expresan sus políticas de correo usando el DNS y dando valores con significado a tipos de registro conocidos. Por eso Gmail sabe cuál es la política de Yahoo, porque pregunta al servicio DNS por los registros concretos donde Yahoo especifica su política y los interpreta adecuadamente.

Para conocer la política de yahoo.es se consulta al DNS por el valor del registro de texto *"_dmarc.yahoo.es"*.

¿Cuál es la política de correo de yahoo.es?

Para conocer la política de yahoo.es ejecutamos la consulta al DNS que nos da el valor del registro de texto *"_dmarc.yahoo.es"*. Es decir, *dig -t txt _dmarc.yahoo.es +short*. El resultado es:

```
"v=DMARC1; p=reject; pct=100; rua=mailto:dmarc_y_rua@yahoo.com;"
```

El valor devuelto especifica que yahoo.es quiere que todos los mensajes, *"pct=100"*, se rechacen, *"p=reject"*, si no se cumplen sus requisitos de autenticación.

Los requisitos de autenticación a los que se refiere DMARC son:

1. que se cumplan con la especificación SPF publicada por yahoo.es, y
2. que la firma DKIM (DomainKeys Identified Mail) del mensaje sea correcta.

¿Cuál es la especificación SPF de yahoo.es?

Para conocer la especificación SPF publicada por yahoo.es ejecutamos la consulta al DNS que nos da el valor del registro de texto *"yahoo.es"*. Es decir, *dig -t txt yahoo.es +short*. El resultado es:

```
"v=spf1 redirect=_spf.mail.yahoo.com"
```

Esto quiere decir que para conocer la especificación SPF debemos consultar el registro DNS *"_spf.mail.yahoo.com"*. Es decir, *dig -t txt _spf.mail.yahoo.com +short*. El resultado es:

```
"v=spf1 ptr:yahoo.com ptr:yahoo.net ?all"
```

El valor devuelto especifica que sólo las direcciones IP cuyo nombre en el DNS terminan en yahoo.com o yahoo.net están autorizadas a enviar mensajes de correo con remitente en el dominio yahoo.es.

¿Cómo se verifica que la firma DKIM es correcta?

Lo primero que debe verificar el servidor que recibe el mensaje es que el mensaje viene firmado. Para ello busca la cabecera *"DKIM-Signature"*. Un ejemplo de la cabecera DKIM-Signature puesta por Yahoo a uno de los mensajes enviados desde yahoo.es:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
 d=yahoo.es; s=s2048; t=1487146982;
 bh=BWzNLM91bSuQwty19PcvBIbWU0CPzkbJOfsDigHiE58=;
 h=Date:From:Reply-To:To:Subject:References:From:Subject;
```

```
 b=YmMVDh3zyx9vw448FYRSmL0ryQ7LUVpjwK/wAfeoMvS0AO/QFDWG+rxfNybqZ
5zd04z02kwTbRvCnnjw1OZuVtVXUXQDBacsPqcMpwU+hj2Zq5gVj+1KR44CUVkD
Rf0/91sJP8B9+FjroLjDOC4MeshEun/YHw6ngjrkXY08ehK5ONYAKGhT/P3tyEGk
IDQnubOZMCCJ1xzZM1DoimehOZhxgbqoPWrMmQnhG0iX2ZVNx8qaNH5nn3gtiT3
YvKOO8A6SFI3bwRXL1Arg0o39xymioba2lONEPpVjNVQ0VTLGqnN7WMbDDglnCvr7f
TokBVD8WoKpcHF8PK57B/YQVw==
```

Lo que dice la cabecera es que la firma de los campos/cabeceras *"`Date:From:Reply-To:To:Subject:References:From:Subject`"* es el contenido de *"`b=`"*. La firma se puede verificar usando cifrado *"`rsa-sha256`"* y la clave pública para usar en el cifrado que se obtiene del DNS usando el selector s2048, valor de *"`s=`"*.

Para obtener la clave pública para verificar la firma DKIM ejecutamos la consulta al DNS que nos da el valor del registro de texto *"`s2048._domainkey.yahoo.es`"*, resultado de concatenar, separados por ".", el valor del campo *"`s`"*, el texto *"`_domainkey`"* y el valor del campo *"`d`"*. Es decir, `dig -t txt s2048._domainkey.yahoo.es +short`. El resultado es:

```
s2048._domainkey.yahoo.es. 6469 IN CNAME s2048._domainkey.yahoo.com.
s2048._domainkey.yahoo.com. 85669 IN TXT "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQE
FAAOCAQ8AMIIBCgKCAQEAuoWufgbWw58MczUGbMv176RaxdZGOMkQmn8OOJ/HGoQ6dalSMWiL
aj8IMcHC1cubJx2gz"
"iAPQHVPtFYayyLA4ayJUSNk10/uqfByiU8qiPCE4JSFrpxflhMIKV4bt+g1uHw7wLzguCf4Y
AoR6XxUKRsAoHuoF7M+v6bMZ/X1G+viWHkBl4UfgJQ6O8F1ckKKoZ5K"
"qUkJH5pDaqbgs+F3PpyiAUQfB6EEzOA1KMPRWJGpzgPtKoukDcQuKUw9GAul7kSIyEcizqrb
aUKNLGAmz0elkqRnzIsVpz6jdT1/YV5Ri6YUOQ5sN5bqNzZ8TxoQlkb"
"VRy6eKOjUnoSSTmSAhwIDAQAB;"
```

¿Y estas comprobaciones se hacen siempre y en todos los mensajes?

Sí. Estas comprobaciones se hacen siempre y sobre todos los mensajes que llegan a Gmail. También las hace Office365 sobre todos los mensajes que llegan a sus servidores.

Puede consultar el resultado de las comprobaciones que ha realizado el servidor sobre un mensaje si visualiza el contenido de la cabecera "`Authentication-Results`". Por ejemplo,

```
Authentication-Results: spf=pass (sender IP is 212.82.97.46)
 smtp.mailfrom=yahoo.es; csi.uned.es; dkim=pass (signature was verified)
 header.d=yahoo.es;csi.uned.es; dmarc=pass action=none
 header.from=yahoo.es;csi.uned.es; dkim=pass (signature was verified)
 header.d=yahoo.es;
```