



NORMATIVA Y LEGISLACIÓN EN MATERIA DE CIBERSEGURIDAD

En estas unidades hemos revisado toda la normativa asociada con Seguridad de la Información, a fin de cubrir los mínimos y máximos legales para diversas empresas del sector. En esta actividad se solicita que realice lo siguiente:

Identifique tres páginas web cuyos niveles de seguridad se encuentren por debajo de los mínimos establecidos y estudiados en esta unidad. Preste especial atención a la normativa desarrollada en el apartado 2 del Manual de esta lección e identifique cuáles serán las infracciones o fallas de seguridad que observa desde un enfoque legal e informático.

Se sugiere realizar capturas de pantalla y detallar el diagnóstico que observa (por ejemplo: falta de políticas de cookies, avisos legales desactualizados, comercio electrónico sin medidas de seguridad, falta de medidas de seguridad efectivas, etc.). Asocie cada problema con la transgresión de alguno de los dispositivos normativos establecidos en el manual. Aporte qué cambios implementaría.



1. Análisis “TioSpanish.org”, escuela de español online

Se trata de un servicio para el aprendizaje del idioma español en modalidad online en el que se ofrecen distintos cursos de español para diferentes niveles conforme el [Marco Común Europeo de Referencia para las Lenguas](#).

Se ha analizado la página y se ha comprobado que, **en apariencia**, la página no recoge datos de usuario –no ofrece formularios de ni entrada de datos de ningún tipo– que puedan requerir un tratamiento conforme normativa legal, de forma que, a priori, tan solo expone información propia del servicio en la dirección única creador → consumidor. Como se ha comentado, esto es solo en apariencia ya que, si se analiza el código fuente de la página se observa –ver **ilustración 1**– lo siguiente...

```
35 <meta name="generator" content="WPML ver:4.4.9 stt:1,2;" />
36 <link rel="icon" href="https://tiospanish.org/wp-content/uploads/2021/05/cropped-favicon-ti
37 <link rel="icon" href="https://tiospanish.org/wp-content/uploads/2021/05/cropped-favicon-ti
38 <link rel="apple-touch-icon" href="https://tiospanish.org/wp-content/uploads/2021/05/croppe
39 <meta name="msapplication-TileImage" content="https://tiospanish.org/wp-content/uploads/202
40 <!-- Global site tag (gtag.js) - Google Analytics -->
41 <script async src="https://www.google.com/tagmanager/js?id=UA-78705605-1"></script>
42 <script>
43   window.dataLayer = window.dataLayer || [];
44   function gtag(){dataLayer.push(arguments)}
45   gtag('js', new Date());
```

Ilustración 1: captura parcial del código fuente de la página tiospanish.org en la que se aprecia el uso de *Google Analytics*.

En la imagen previa, capturada del código fuente de la página web analizada, se observa que hace uso de **Google Analytics**.

Google Analytics –en adelante, **GA**– es una herramienta que emplea diferentes tipos de cookies para rastrear a los usuarios de un sitio, medir audiencias, analizar el comportamiento de sus usuarios y mejorar la estrategia para captar y ampliar tráfico. Se trata, por tanto, de cookies **no necesarias** para que funcione el sitio web, como podrían ser las cookies técnicas cuyo uso no requiere el consentimiento de los usuarios y, por tanto, hay que atender a lo que expresa la normativa al respecto: **informar sobre ellas y recabar el consentimiento de los usuarios antes de usarlas conforme principio de licitud**.

Se ha de notar que, aunque **GA** no recopila información personal identificable, como el nombre o el correo electrónico, el RGPD define que la información personal identificable incluye identificaciones persistentes

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

M^a del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



como ID de cliente, ID de usuario y dirección IP, edad, género, intereses, dispositivos, ubicación... información que se rastrea y almacena en **GA**. Dado que, **se comparte** esa información personal identificable de los visitantes **con un tercero** (GA), es necesario informar de ello y, además, ofrecer la opción de elegir al visitante si permite o no que sus datos sean recopilados y procesados.

Conforme a lo expuesto, se estarían incumpliendo los siguientes artículos del Reglamento General de Protección de Datos –en adelante, RGPD–:

- Tratamiento ilícito de los datos del interesado – conforme [Artículo 6 RGPD](#): “Licitud del tratamiento”. Conforme **1.a** el tratamiento solo será lícito con el consentimiento explícito previo del usuario, ya que la información recopilada no es necesaria para la prestación del servicio y se cede a un tercero.
- No facilitar información suficiente al interesado sobre el tratamiento que se va a hacer de sus datos – [Artículo 13 RGPD](#): “Información que deberá facilitarse cuando los datos personales se obtengan del interesado”. Y es que, al obtener información y compartirla con un tercero, se debe informar a este sobre identidad y datos del responsable, el DPO, los fines del tratamiento, destinatarios, la intención de transferir la información hacia un país u organización internacional –Artículo 13 apartado 1.f–, el plazo de conservación, derechos –reclamación–, etc.

Además, como puede comprobarse en las capturas siguientes de la cabecera –ilustración 2– y pie de página –ilustración 3– del sitio web analizado, se observa que no se facilita en ningún momento información requerida para cumplir con la normativa RGPD.

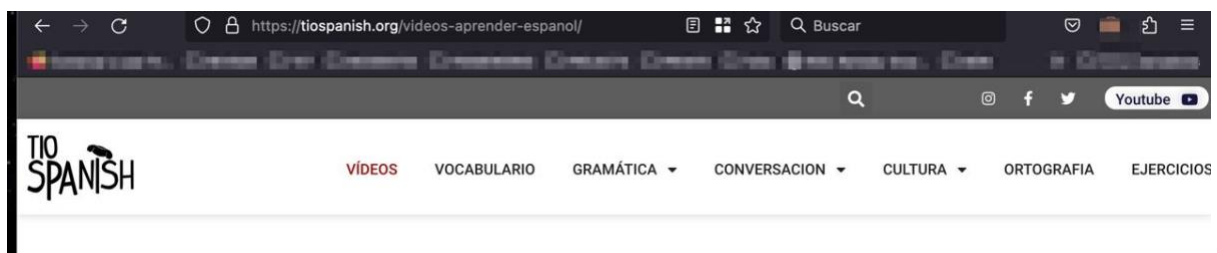


Ilustración 2: captura parcial cabecera de la escuela de español en la que se aprecia la carencia de referencias o enlaces hacia información de índole legal.



Ilustración 3: captura parcial del pie de página de tiospanish.org en la que se aprecia que no existen los habituales enlaces a las políticas -aviso legal, política de cookies, privacidad-, términos de uso, etc.

Y es que no se ha encontrado en toda la web, ni enlaces de la barra de navegación o cabecera, ni a pie de página, enlaces hacia textos legales necesarios que debería cumplir, como por ejemplo un Aviso legal, una Política de privacidad o una Política de cookies. Se ha de notar que, el sitio web analizado, tampoco informa ni permite la selección de las cookies, tal y como obligan tanto el RGPD como el LOPDGDD.

En cuanto a vulnerabilidades software se encontró que el sitio web, creado con WordPress, utiliza un componente o plugin, en jerga técnica, llamado WPML –WordPress Multilingual– en su versión 4.4.9, como se aprecia en la siguiente captura parcial.

```
85 <meta name="generator" content="WPML ver:4.4.9 stt:1,2;" />
86 <link rel="icon" href="https://tiospanish.org/wp-content/uploads/2021/05/cropped-favicon-t
87 <link rel="icon" href="https://tiospanish.org/wp-content/uploads/2021/05/cropped-favicon-t
88 <link rel="apple-touch-icon" href="https://tiospanish.org/wp-content/uploads/2021/05/cropp
```

Ilustración 4: captura parcial en la que se aprecia que se hace uso de una versión vulnerable del plugin WPML, utilizado para mostrar la web en múltiples idiomas.

Se ha comprobado que existe un **par de vulnerabilidades graves** en dicho componente que afecta a WPML en versiones previas a 4.6.1, como puede comprobarse en el siguiente [boletín de seguridad del fabricante](#).

Se trata de una vulnerabilidad XSS que permite inyectar scripts en la página y un CSRF con muy alta puntuación –8,8 conforme CVSS v 3.1– ya que deriva en RCE, siglas en inglés de ejecución remota de código.

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

M^a del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



Se cita literal el comunicado del fabricante en la siguiente ilustración.

We have just released WPML 4.6.1, which includes an important security fix. We strongly recommend updating WPML to the latest version on all your websites as soon as possible.

In the meantime, we have released WPML 4.6.2 which resolves an issue with PHP 5.6 compatibility.



Two days ago, we received a report about an XSS vulnerability in WPML. Due to security reasons, we cannot provide further details at this time.

While we don't know of any sites that have been affected, we always advise updating WPML whenever a new release addresses security issues – big or small.

All you need to do is update all your sites running WPML to the latest version, WPML 4.6.1.

Ilustración 5: captura parcial del comunicado del fabricante rogando encarecidamente la actualización urgente a la última versión del componente WPML.

No se ha encontrado nada más relevante en cuanto a vulnerabilidades o incumplimiento ya que realmente se trata de una web muy sencilla que no recoge datos de forma interactiva y el grueso de información fluye desde el servicio hacia el consumidor. De esta forma las recomendaciones para solucionar los errores normativos detectados sería simplemente incorporar las habituales secciones para informar sobre cookies y políticas asociadas, eso sí, con toda la información que cada uno de estos apartados debe incluir.

En cuanto a las vulnerabilidades se recomienda conforme Magerit versión 3.0, lo siguiente:

| Cod. | Amenaza | Cod. | Control |
|------|---------------------------|-------|--|
| E.20 | Vulnerabilidades software | H.VM | Gestión de vulnerabilidades. Aplicar un correcto ciclo de identificación de vulnerabilidades y seguimiento hasta corrección. |
| E.21 | No actualización software | SW.CM | Cambios (actualizaciones y mantenimiento) |



2. Análisis de la página web del Ayuntamiento de Arganda

Contexto previo: a finales de junio el Ayuntamiento de Arganda comunicó a la Guardia Civil que había sido víctima de un ataque informático, [ver noticia completa al respecto](#).



Ilustración 6: captura cabecera de la noticia del ataque al Ayuntamiento de Arganda.

En la noticia se informa que el ataque fue perpetrado por el grupo **Rhysida**, se trata de un incidente de tipo **ransomware**. Se ha de notar que, en el artículo se informa de la comunicación en tiempo conforma ley a las autoridades –Guardia Civil informada antes de las 72 h que marca artículo 33 del RGPD–, sin embargo, no se indica en ningún momento si se ha comunicado la violación de seguridad a los interesados como marca el artículo 34, RGDP.

Se ha analizado la web del ayuntamiento sin encontrar referencia alguna al incidente. También se ha consultado a ciudadanos de Arganda del Rey –conocidos por el analista, Carmen– si han recibido información al respecto, sin encontrar constancia de ello.

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

M^a del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



Se investigó el grupo Rhysida, agente amenaza autor del ataque, encontrando que se trata de un grupo de reciente creación –que aparece por primera vez este mismo año– dedicado al secuestro y exfiltración de información de sus víctimas para proceder, posteriormente, a la conocida como *doble extorsión*, chantaje en el que se amenaza a la víctima con hacer pública la información exfiltrada si no paga un rescate que, para este grupo, consiste en 25 BTCs –Bitcoin–, aproximadamente unos 700.000€ en el momento del incidente. La elección del pago en criptoactivos es probable debido a la dificultad para interceptar o anular transferencias dada la inmutabilidad de la tecnología de cadena de bloques subyacente, además, por supuesto, del anonimato asociado a este tipo de transacciones.

Durante la investigación del agente amenaza se descubrió que posee un sitio oficial en el que hace pública la información robada a sus víctimas, el sitio se encuentra en la red Tor en la siguiente URL:

`hXXp://rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad[.]onion/`

El uso de un servidor en la red Tor, red descentralizada, se elige habitualmente por este tipo de grupos de cibercrimen para mantener el anonimato e impedir el bloqueo del sitio oficial del grupo en el que se negocia con la víctima y se publica la información en represalia si la negociación no prospera.

En el análisis de las distintas víctimas en el “muro de la fama” del sitio oficial del grupo Rhysida, se encontró al Ayuntamiento de Arganda. Además, se ha descubierto que **ya se ha publicado el 50 % de la información exfiltrada**. De forma que **información privada, PII y datos protegidos de ciudadanos** se encuentran accesibles a cualquiera que conozca el sitio oficial y disponga de

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

Ma del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



un navegador compatible con la red Tor como, por ejemplo, el proyecto **Tor Browser**.

En la siguiente ilustración, la 7ª, se aprecia el resumen que el grupo facilita sobre la víctima, notar que afirman disponer de más de 400.000 ficheros.

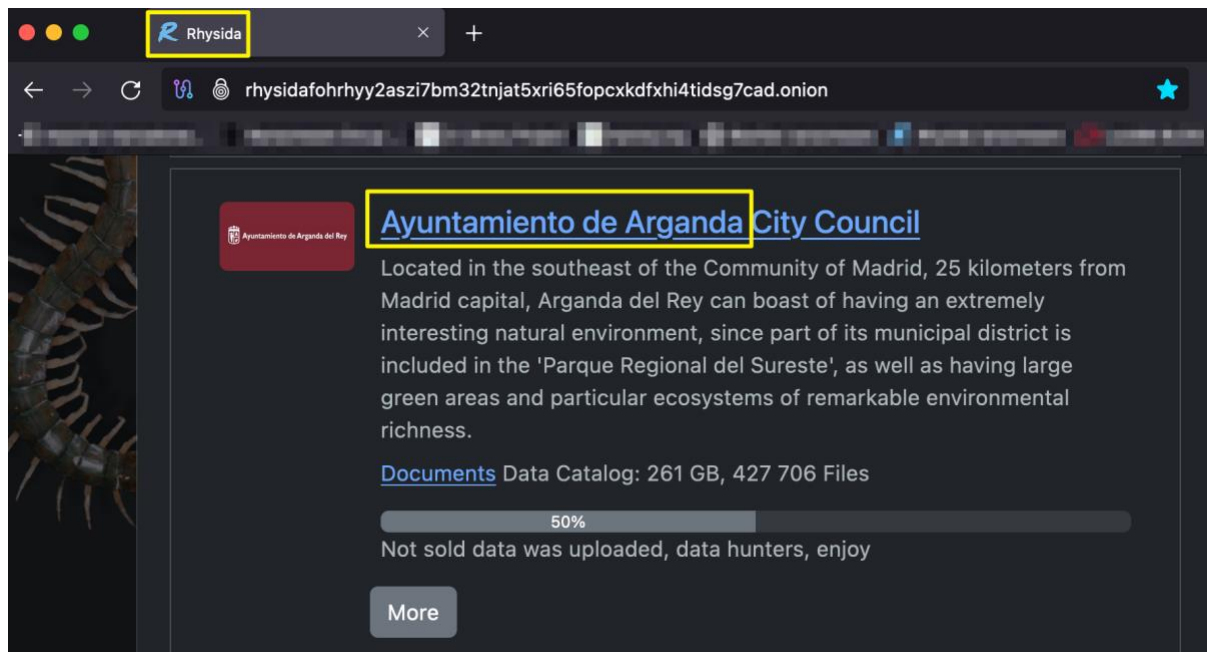


Ilustración 7: captura parcial sitio oficial grupo Rhysida en la red Tor, se aprecia que hay 261 GB de información exfiltrada del Ayuntamiento de Arganda.

Se ha comprobado que la información disponible contiene **datos especialmente protegidos** de ciudadanos de la ciudad de Arganda del Rey, como capturas completas de DNI o pasaporte, listados de ayudas públicas que incluyen nombre, DNI y cuenta corriente, facturas, etc.

Se considera que, además de notificar a las autoridades, el Ayuntamiento **debería haber informado a los ciudadanos afectados** –prácticamente todos los que habiten en el municipio– de que en foros de contrabando clandestinos se está ofreciendo información especialmente sensible, como su DNI. Notar que, **en ningún lugar, ni noticias ni web del ayuntamiento, se ha encontrado referencia alguna a que se haya podido robar información sensible...** tan solo se habla de incidente que bloqueó los sistemas informáticos pero que “ya se ha solucionado”.

En la siguiente captura, ilustración 8ª, se aprecia que entre los datos robados hay documentos identificativos de ciudadanos, facturas, hojas Excel, etc.

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

M^a del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



rhysidafohrhy2aszi7bm32tnjat5xri65fopcxdxfxhi4tidsg7cad.onion

Ayuntamiento de Arganda City Council

Ayuntamiento de Arganda City Council

Located in the southeast of the Community of Madrid, 25 kilometers from Madrid capital, Arganda del Rey can boast of having an extremely interesting natural environment, since part of its municipal district is included in the 'Parque Regional del Sureste', as well as having large green areas and particular ecosystems of remarkable environmental richness.

[Documents](#) Data Catalog: 261 GB, 427 706 Files

50%

Not sold data was uploaded, data hunters, enjoy

Located in the southeast of the Community of Madrid, 25 kilometers from Madrid capital, Arganda del Rey can boast of having an extremely interesting natural environment, since part of its municipal district is included in the 'Parque Regional del Sureste', as well as having large green areas and particular ecosystems of remarkable environmental richness. The remote origin of what is now the municipality of Arganda del Rey can well be placed more than 300 thousand years ago, which is the date of dating of the Paleolithic remains deposited in the Jarama Valley, discovered in the early 70s.

Ilustración 8: captura parcial sitio oficial grupo Rhysida en la red Tor, se aprecia que se han publicado información protegida de ciudadanos de la ciudad de Arganda del Rey.

Conforme a lo expuesto, se estima que, al menos, se han violado los siguientes artículos del RGPD:

[Artículo 32](#), “Seguridad del tratamiento”: este artículo hace referencia a la necesidad de **proteger los datos sensibles durante el tratamiento y almacenamiento** de la información, contemplando el estado del arte del

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

Ma del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



panorama actual de amenazas para garantizar el adecuado nivel de riesgo, para ello en este artículo se recomiendan distintas medidas, se citan algunas:

- Seudonimización/anonimización y cifrado de datos personales.
- Capacidad de garantizar triada CIA y resiliencia permanente de los sistemas y servicios de tratamiento.
- Capacidad de recuperación.

Artículo 34, “Comunicación de una violación de seguridad de los datos personales al interesado”: aunque se ha verificado que sí se ha cumplido el Artículo 33, “notificación a las autoridades de control de violación de seguridad”, no se ha conseguido verificar el cumplimiento del 34, ya que ni el ayuntamiento ha publicado nada al respecto en su web –se ha consultado tablón de anuncios, etc.– ni hay comentarios en las noticias publicadas, que tan solo hablan de la “interrupción del servicio” y no dicen nada de información altamente sensible disponible en foros clandestinos. Se ha contactado con conocidos residentes en el municipio que confirman que, hasta el momento, no han recibido un comunicado que indique que datos especialmente sensibles están publicados en foros clandestinos. De esta forma se cree que es muy probable que se haya omitido este dato, ya sea por **error o intencionadamente**.

Al tratarse de una Administración Pública, debería cumplir unos **requisitos mínimos conforme al ENS**, por ejemplo (entre otros):

- Análisis y gestión de los riesgos: que habrían detectado que hay un riesgo claro –existe precedente– de ataques contra ayuntamientos por parte de grupos ransomware.
- Seguridad por defecto.
- Protección de la información almacenada y en tránsito: se podría haber cifrado la información sensible, como los DNIs.
- Integridad y actualización del sistema: que solucionen posibles vulnerabilidades o debilidades que hayan podido ser aprovechadas por el grupo para infiltrarse en la red corporativa.
- Gestión de personal: por ejemplo, vía concienciación, ya que este grupo suele obtener el vector de entrada vía ataques de ingeniería social –phishing–.
- ...

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

M^a del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



Claramente la Administración Pública es una víctima prioritaria para este tipo de grupos ya que poseen cantidades ingentes de información – facturas, documentación identificativa, etc.– que permite ser utilizada en futuros escenarios de amenaza verosímiles –al contar con información real sobre las víctimas– contra proveedores, ciudadanos, etc.

Se ha de notar que, conforme [Artículo 83 RGPD](#), “Condiciones generales para la imposición de multas administrativas”, si se demuestra que no hubo la adecuada diligencia debida, puede acarrear sanciones elevadas.

Medidas correctoras

Conforme Magerit v 3.0 se recomendarían las siguientes medidas/controles de seguridad.

| Cod. | Amenaza | Cod. | Control |
|------|---------------------------|---------------------|--|
| E.4 | Errores de configuración | H.tools.CC | Herramientas de chequeo de configuración. |
| E.8 | Difusión de malware | H.Tools.AV | Herramientas contra código dañito (perimetrales y en puesto de trabajo). |
| | | H.Tools.IDS | IDS/IPS. Herramientas de detección/prevención en base análisis de tráfico de red y reglas/firmas de amenazas. |
| E.19 | Fugas de información | H.Tools.DLP | Herramientas de monitorización de contenidos. Un servicio de inteligencia que rastree foros públicos y clandestinos también se puede contemplar. |
| E.20 | Vulnerabilidades software | H.VM | Gestión de vulnerabilidades. Aplicar un correcto ciclo de identificación de vulnerabilidades y seguimiento hasta corrección. |
| E.21 | No actualización software | SW.CM | Cambios (actualizaciones y mantenimiento) |
| E.23 | No actualización hardware | HW.CM | Cambios (actualizaciones y mantenimiento) |
| A.5 | Suplantación identidad | H.IA | Identificación y autenticación. Vía llaves hardware compatibles FIDO2, el ROI es muy bueno. |
| A.6 | Abuso privilegios | H.ST | Segregación de tareas. |
| | | H.AU | Aplicación principio menos privilegio necesario. Registro y auditoría, como disuasorio y cumplimiento. |
| A.8 | Difusión de malware | PS.AT H.tools.AV | Formación y concienciación. Herramienta contra código dañino, por ejemplo, un EDR, etc. |

MÓDULO 3 -Normativa y legislación. Ciberseguridad-

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)



| | | | |
|------|-------------------------------|----------------------------------|--|
| A.11 | Acceso no autorizado | H.AC H.IA H.Tools.HP | Control de acceso lógico. Identificación y autenticación. De nuevo con llaves hardware FIDO2 o al menos MFA (por ejemplo, con apps como Authy). Honey net/honey pot para detección de actividad extraña. |
| A.14 | Interceptación comunicaciones | D.C S.www S.email COM.C | Cifrado de información. Protección de servicios y aplicaciones web. Protección email. Protección criptográfica |
| A.19 | Divulgación información | H.tools.DLP | Herramientas de monitorización de fugas de información sensible. |
| A.25 | Robo | D.C D.A | Cifrado de la información, así, aunque exista robo no será accesible a terceros. Copias de seguridad (aunque realmente no se pide nada más que contemplar privacidad). |
| A.30 | Ingeniería social | PS.AT | Formación y concienciación. |

3. Análisis de la página web fontanerosmadrid.eu

Para el último ejemplo se ha localizado una web de servicios de fontanería de Madrid. Aunque la web cumplía todos los requisitos legales respecto a RGPD –informaba y permitía selección de cookies, incluye en pie de página aviso legal, política de cookies, política de privacidad, etc.– se encontró –ver ilustración 9ª– analizando los datos de sus registros DNS, lo siguiente:

```
carmentlorenteb@MacBook-Pro:~/projects/eip
> host -t mx fontanerosmadrid.eu
fontanerosmadrid.eu mail is handled by 10 mail.fontanerosmadrid.eu.
> host -t txt fontanerosmadrid.eu
fontanerosmadrid.eu has no TXT record
```

Define MX –Mail eXchange–

Sin embargo, no define registro TXT, de forma que no implementa spf, permitiendo suplantación del correo

Ilustración 9: se comprueba que la empresa define servicio de correo –registro MX– pero, sin embargo, no define registros TXT, necesarios para implementar políticas que eviten la suplantación, como el protocolo spf.

La empresa dispone de servicio de correo, ya que define un registro MX, sin embargo, no se implementa spf para indicar, conforme buenas prácticas, los emisores de correo válidos. De forma que se puede, fácilmente, emitir correo suplantando su dirección, por ejemplo, emitiendo una factura falsa

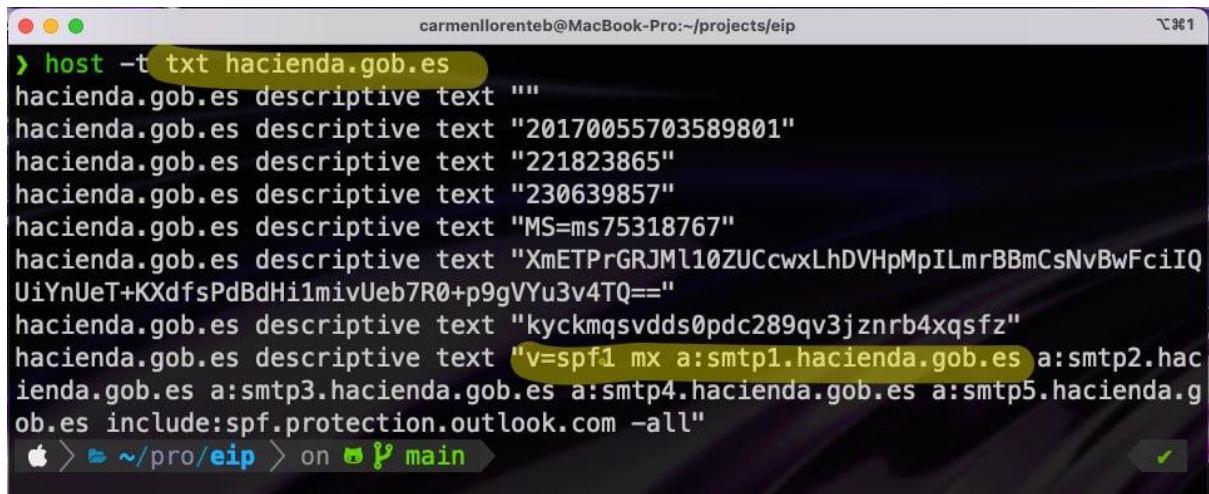
MÓDULO 3 -Normativa y legislación. Ciberseguridad-



M^a del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcillorente@eiposgrados.edu.es)

hacia clientes, solicitando el pago en una cuenta controlada por el agente amenaza. Este es un esquema habitual de fraude.

En la ilustración 10^a, a continuación, se ha utilizado como ejemplo de servicio web que sí configura correctamente su servicio de correo para evitar suplantaciones haciendo uso del protocolo spf en su versión 1. Se trata de la web de la Hacienda española.



```
carmentlorenteb@MacBook-Pro:~/projects/eip
> host -t txt hacienda.gob.es
hacienda.gob.es descriptive text ""
hacienda.gob.es descriptive text "20170055703589801"
hacienda.gob.es descriptive text "221823865"
hacienda.gob.es descriptive text "230639857"
hacienda.gob.es descriptive text "MS=ms75318767"
hacienda.gob.es descriptive text "XmETPrGRJmL10ZUCcwXLhDVHpMpILmrBBmCsNvBwFciIQ
UiYnUeT+KXdfsPdBDHi1mivUeb7R0+p9gVYu3v4TQ=="
hacienda.gob.es descriptive text "kyckmqsvdds0pdc289qv3jznr4xqsfsz"
hacienda.gob.es descriptive text "v=spf1 mx a:smtp1.hacienda.gob.es a:smtp2.hac
ienda.gob.es a:smtp3.hacienda.gob.es a:smtp4.hacienda.gob.es a:smtp5.hacienda.g
ob.es include:spf.protection.outlook.com -all"
```

Ilustración 10: ejemplo de web -administración pública- que sí define registros TXT y hace uso del protocolo spf en su versión 1 para evitar la suplantación de su correo electrónico por terceros.

A esta empresa de fontanería se le recomendaría que configure adecuadamente en su proveedor de dominio los registros dns para incorporar, conforme buenas prácticas, controles como spf y dmarc para evitar la suplantación del correo electrónico.