

# Informe OSINT

## Índice

1. Finalidad del documento: .....	3
2. Información del objetivo .....	3
2.1 Introducción: .....	3
2.2 Contacto y redes sociales.....	3
3. Información administrativa .....	4
3.1 Datos fiscales .....	4
3.2 Datos comerciales .....	5
4. Información técnica .....	6
4.1 Direcciones IP:.....	8
4.2 Servidor: .....	9
4.2.1 Máquina virtual: .....	11
4.2.2 Servidor: .....	11
4.2.4 Tecnologías Utilizadas.....	12
5. Información corporativa .....	14
5.1 Equipo directivo .....	14
5.2 Personal de la empresa.....	14

## 1. Finalidad del documento:

Estamos creando un documento sobre la empresa SEVERAL ENERGY S.L que se crea con el propósito de recopilar, analizar y presentar información relevante obtenida a través de fuentes de acceso público, como sitios web, redes sociales, bases de datos públicas y otras fuentes disponibles en línea.

## 2. Información del objetivo

### 2.1 Introducción:

En SEVERAL ENERGY S.L, ofrecen servicios de consultoría energética. Su objetivo es proporcionar soluciones personalizadas para optimizar el consumo de energía y reducir la huella ambiental de sus clientes.

Centran su atención en ofrecer soluciones a medida que permitan maximizar el ahorro en las facturas de luz y gas. Se comprometen a implementar medidas eficientes tanto en entornos domésticos como empresariales, con el objetivo de optimizar los recursos energéticos disponibles.

### 2.2 Contacto y redes sociales.

Utilizando la herramienta MR.Homles obtuvimos la siguiente información, la cual nos daba respuesta a las distintas redes sociales relacionadas con dicha empresa.

```
[N]CONNECTION-ERROR ... TRYNG WITH NO PROXIES
[v]USERNAME severalenergy FOUND
[v]LINK: https://facebook.com/severalenergy
[I]TAGS:[Social,Chatting]

[+]TRYING ON: Disqus

[N]CONNECTION-ERROR ... TRYNG WITH NO PROXIES
[!]USERNAME severalenergy NOT FOUND

[+]TRYING ON: Pinterest

[N]CONNECTION-ERROR ... TRYNG WITH NO PROXIES
[v]USERNAME severalenergy FOUND
[v]LINK: https://pinterest.com/severalenergy
[I]TAGS:[Image,Social,Photo]

[+]TRYING ON: Passes

[N]CONNECTION-ERROR ... TRYNG WITH NO PROXIES
[v]USERNAME severalenergy FOUND
[v]LINK: https://passes.com/severalenergy
[I]TAGS:[Image,Social,Photo]
```

Facebook: several energy

Pinterest: several energy

Passes: several energy

InfoJobs: several energy → <https://www.infojobs.net/several-energy-sociedad-limitada./em-i98495456554548836986691023096225802243>

### 3. Información administrativa

#### 3.1 Datos fiscales

Several Energy se estableció en España y se encarga de gestionar las operaciones y cuestiones comerciales relacionadas con la energía en el mercado español y, posiblemente, en otros mercados de habla hispana. Su función incluye actividades como la gestión de energía.

Ubicación:

#### [Dirección y teléfono de SEVERAL ENERGY SOCIEDAD LIMITADA.](#)

Domicilio social actual	CALLE JOSE LUIS PEREZ PUJADAS (ED FORUM), 14 <a href="#">Ver Mapa</a>
Código Postal	18006
Municipio	GRANADA
Provincia	Granada

Información fiscal de la empresa:

#### [Información de SEVERAL ENERGY SOCIEDAD LIMITADA.](#)




Denominación	SEVERAL ENERGY SOCIEDAD LIMITADA.
CIF/NIF	B16870370
Número DUNS	<a href="#">4706...</a> ⓘ
Actividad Informa	Servicios prestados a las empresas ncop
CNAE	6399 - Otros servicios de información n.c.o.p.
SIC	7399 - Servicios comerciales SC
Objeto Social	Otros servicios de información. Otras actividades de apoyo a las empresas. Promoción inmobiliaria
Registro Mercantil	<a href="#">Registro Mercantil de Granada</a> - 2 actos en BORME publicados
Actualización Ficha Empresa	16/10/2023
Última consulta empresa	08/01/2024
Consultas Empresa Total	71
Consultas Último Trimestre	11

### 3.2 Datos comerciales

Se puede observar que la empresa que estamos investigando se trata de una pequeña sociedad dado los datos encontrados.

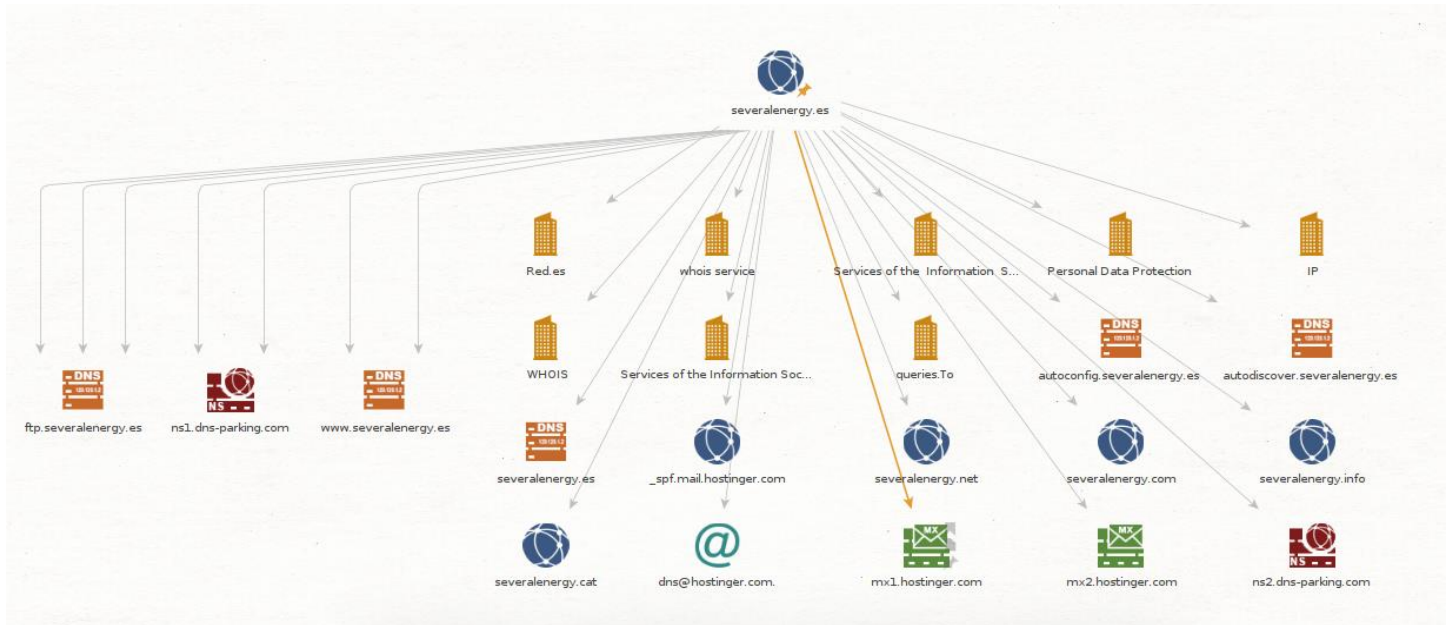
Datos Comerciales de <b>SEVERAL ENERGY SOCIEDAD LIMITADA.</b>	
<a href="#">Estructura Corporativa</a>	
Administrador Único	<a href="#">Disponible</a>
<a href="#">Estructura Legal</a>	
Forma Jurídica	Sociedad limitada
Capital Social	3.000 €
Cotiza en Bolsa	NO
<a href="#">Último Acto BORME</a>	16/09/2021 Nombramientos
<a href="#">Información Comercial</a>	
Fecha Constitución	09/09/2021
Actividades Internacionales	No constan
<a href="#">Otra Información de Interés</a>	
Fecha último dato	16/10/2023

En la siguiente imagen se muestran las posibles subvenciones a la empresa.

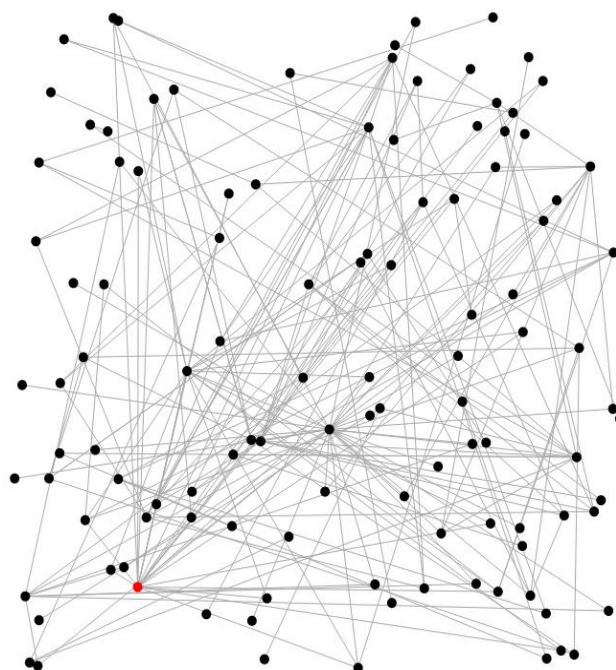
Posibles subvenciones para empresas similares a SEVERAL ENERGY SOCIEDAD LIMITADA.	
	<a href="#">Ayudas para programas de prevención de riesgos laborales.</a> <a href="#">Consultar</a>
Categorías:	Formación, Prevención Riesgos Laborales, Asesorías, Auditorías y Consultorías Externas, Comercio
Beneficiarios:	Asociaciones, Cooperativas y Sociedades Laborales no Agrarias, Entidades sin ánimo de lucro, Fundaciones, Organizaciones Empresariales y Sindicales
Provincia:	Andalucía
	<a href="#">Ayudas para la realización de actividades y proyectos de mejora en materia prevención...</a> <a href="#">Consultar</a>
Categorías:	Prevención Riesgos Laborales, Asesorías, Auditorías y Consultorías Externas
Beneficiarios:	Autónomos, Cooperativas y Sociedades Laborales no Agrarias, Microempresas (menos de 10 empleados), Pymes (menos de 250 empleados), Sociedades Civiles
Provincia:	Andalucía
	<a href="#">Subvenciones para la digitalización de las pymes.</a> <a href="#">Consultar</a>
Categorías:	Equipamientos informáticos y Tecnología, Asesorías, Auditorías y Consultorías Externas
Beneficiarios:	Autónomos, Cooperativas y Sociedades Laborales no Agrarias, Microempresas (menos de 10 empleados), Pymes (menos de 250 empleados), Sociedades Civiles
Provincia:	Andalucía

#### 4. Información técnica

En este caso hemos utilizado Maltego para observar los diferentes sitios webs asociados a esta empresa, los diferentes DNS's y también podemos ver correos asociados a ella. Además de utilizar esta herramienta también probamos con otra la cual quizás es más intuitiva de usar.



Utilizamos la herramienta SpiderFoot y pudimos obtener información similar a la anterior, se obtiene tanto un diagrama de barras como un diagrama en tres dimensiones; los cuales explicaremos a continuación



A network graph visualization showing connections between various entities. The nodes are represented by black dots, and the edges are thin gray lines. The entities and their connections are as follows:

- abuse@stepn-bayc.com** is connected to **abuse@pana.red**, **umac-128-etm@openssh.com**, **141.136.43.138**, **Datos Personales**, **Datos DPR**, and **abuse@cloudflare.com**.
- abuse@pana.red** is connected to **abuse@cloudflare.com**.
- umac-128-etm@openssh.com** is connected to **141.136.43.138**.
- 141.136.43.138** is connected to **Datos Personales**.
- Datos Personales** is connected to **Datos DPR**.
- Datos DPR** is connected to **abuse@cloudflare.com**.
- abuse@cloudflare.com** is connected to **a**.

**Data Types**

Data Type	Percentage of Unique Elements
Affiliate - Domain Name	0.5
Affiliate - Email Address	0.5
Affiliate - IP Address	5.8
Affiliate - Internet Name	4.8
Affiliate - Name Unresolved	0.5
Affiliate - BGP AS Membership	1.2
Blacklisted Affiliate IP on Same Subnet	0.2
Blacklisted Site	0.5
Co-Hosted Site	0.5
Country Name	1.5
DNS SRV Record	1.0
DNS TXT Record	1.2
Email Gateway	0.2
Email Address	0.2
HTTP Status Codes	0.2
HUMAN Code	13.8
IP Number	1.2
IPV6 Address	1.2
Internet Name	0.2
Internal URL - Internal	0.5
Linked URL - External	0.5
Malicious IP on Same Subnet	2.0
Malicious IP on Same Subnet	16.5
Network DNS Records	1.2
Network Membership	1.5
Non-Standard HTTP Header	0.2
Open TCP Port	0.2
Operating System	1.5
Physical Address	1.8
Raw Data from pfs/pfs	0.2
Raw File Metadata	0.5
SSL Certificate Issued by	1.2
SSL Certificate Host	1.5
SSL Certificate Raw Data	6.2
URL Mismatch	2.5
URL (Purely Static)	0.2
URL Uses Javascript	1.2
Web Content	3.5
Web Content Server	9.2
Web Technology	1.8
Web Server	0.2

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	3	8	2024-01-10 11:20:58
Affiliate - Email Address	33	64	2024-01-10 11:21:02
Affiliate - IP Address	27	29	2024-01-10 11:20:58
Affiliate - IPv6 Address	3	4	2024-01-10 10:31:42

Como resultado final se obtuvieron tres direcciones IP's relacionadas con la Sociedad.

Browse <b>IP Address</b>				
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	141.136.43.154	severalenergy.es	sfp_dnsresolve	2024-01-10 10:09:49
<input type="checkbox"/>	141.136.43.154	www.severalenergy.es	sfp_dnsresolve	2024-01-10 11:04:45
<input type="checkbox"/>	153.92.2.19	autodiscover.severalenergy.es	sfp_dnsresolve	2024-01-10 11:05:25

#### 4.1 Direcciones IP:

Con *dnsenum* confirmamos lo hallado con la anterior herramienta, obtuvimos las siguientes direcciones IPs.

```
dnsenum VERSION:1.2.6
severalenergy.es

Host's addresses:
severalenergy.es. 1784 IN A 141.136.43.154

Name Servers:
ns1.dns-parking.com. 14400 IN A 162.159.24.201
ns2.dns-parking.com. 14400 IN A 162.159.25.42

Mail (MX) Servers:
mx1.hostinger.com. 5 IN A 172.65.182.103
mx2.hostinger.com. 176 IN A 172.65.182.103

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for severalenergy.es on ns1.dns-parking.com ...
AXFR record query failed: NOTIMP
Trying Zone Transfer for severalenergy.es on ns2.dns-parking.com ...
AXFR record query failed: NOTIMP
```

Con las IPs obtenidas utilizamos Shodan para realizar un análisis mayor ya que en esta página podemos observar los puertos que utilizan, donde se encuentra alojada la máquina y las tecnologías utilizadas para crear la página web.



**141.136.43.154** Vista normal > Datos sin procesar

**Información general**

Nombres de host: cpl90. **hosting24.com**  
hstgr.io

Dominios: HOSTING24.COM HSTGR.IO

País: **Reino Unido**

Ciudad: **Manchester**

Organización: **Hostinger Internacional Limitada**

ISP: **Hostinger Internacional Limitada**

ASN: **AS47583**

**Tecnologías web**

Alojamiento: Hostinger

Misceláneas: HTTP/3

Esta IP tiene los puertos 43 y 80 abiertos.

**Open Ports**

80 443

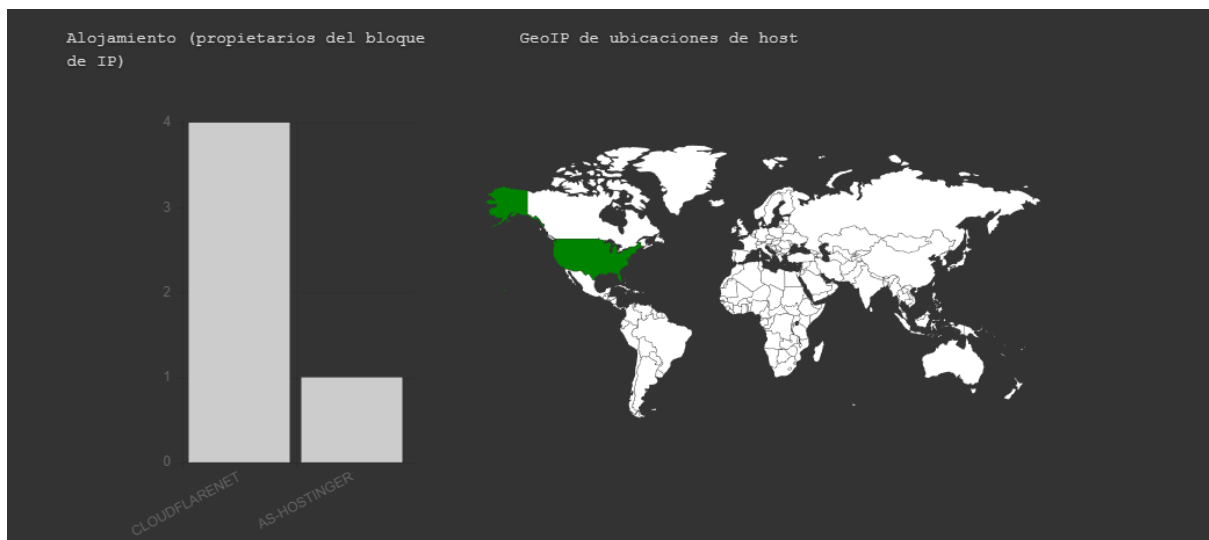
Al realizar el análisis no se han encontrado vulnerabilidades muy graves. Por ejemplo, en el puerto 443 al ser una conexión de manera predeterminada insegura la envía directamente al “*error 403 forbidden*”.

## 4.2 Servidor:

Los servidores que tiene Several Energy son los siguientes.

```
Name Servers:
ns1.dns-parking.com.      14400  IN  A      162.159.24.201
ns2.dns-parking.com.      14400  IN  A      162.159.25.42
```

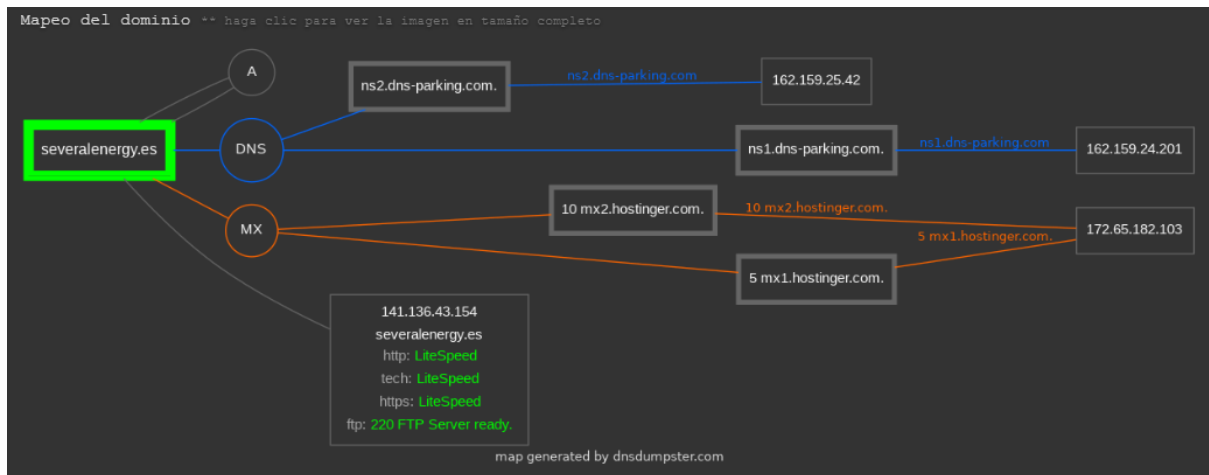
Con *DNS Dumpster* hemos conseguido ver dónde están localizados los servidores a nivel global, podemos observar que principalmente se encuentran en América, concretamente Estados Unidos.



**Servidores DNS:** Los servidores DNS sirven para convertir las solicitudes de nombres en direcciones IP, con lo que se controla a qué servidor se dirigirá un usuario final cuando escriba un nombre de dominio en su navegador web.

Servidores DNS		
ns2.dns-parking.com. 🌐 🔄 📶 📶 📶 📶	162.159.25.42 ns2.dns-parking.com	NUBEFLARENET desconocido
ns1.dns-parking.com. 🌐 🔄 📶 📶 📶 📶	162.159.24.201 ns1.dns-parking.com	NUBEFLARENET desconocido
Registros MX ** Aquí es donde va el correo electrónico del dominio...		
10mx2.hostinger.com. 🌐 🔄 📶 📶 📶 📶	172.65.182.103	CLOUDFLARENET Estados Unidos
5 mx1.hostinger.com. 🌐 🔄 📶 📶 📶 📶	172.65.182.103	CLOUDFLARENET Estados Unidos
Registros TXT ** Encuentre más hosts en las configuraciones del Marco de políticas del remitente (SPF)		
"v=spf1 incluye:_spf.mail.hostinger.com ~todos"		
Registros de host (A) ** Es posible que estos datos no estén actualizados ya que utiliza una base de datos estática (actualizada mensualmente)		
variasenergia.es 🌐 🔄 📶 📶 📶 📶 HTTP: <b>LiteSpeed</b> FTP: <b>Servidor FTP 220 listo.</b> TECNOLOGÍA HTTP: <b>LiteSpeed</b>	141.136.43.154 cpl90.hosting24.com	AS-HOSTINGER Reino Unido

El mapa del dominio permite utilizar varios dominios para una misma página web. Esto resulta muy útil cuando se utilizan sistemas de gestión de contenidos como WordPress ya que puedes estructurar múltiples dominios y subpáginas y conectarlos entre sí.



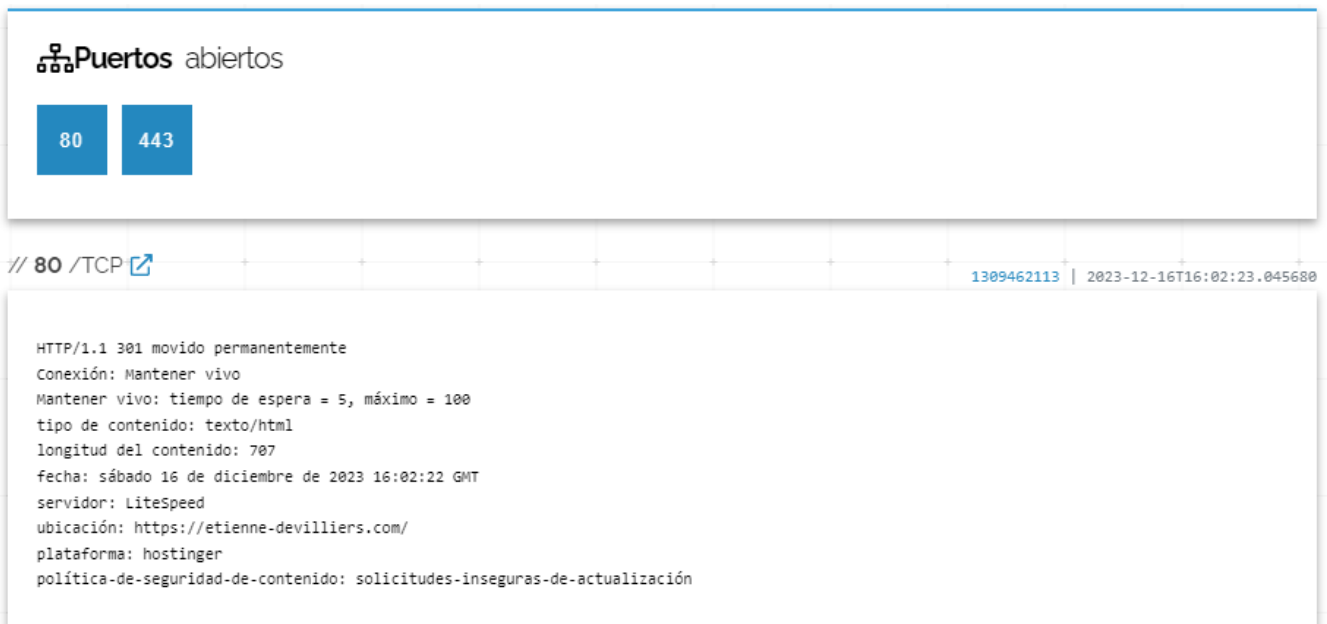
#### 4.2.1 Máquina virtual:

Mediante MR.Homles hemos podido conseguir información sobre la máquina virtual de la empresa.

```
+]SEARCH INFORMATION FOR: severalenergy.es
v]IP: 141.136.43.154
v]NATION: United Kingdom
v]NATION-CODE: GB
v]REGION-CODE: ENG
v]REGION-NAME: England
v]CITY: Manchester
v]TIMEZONE: Europe/London
v]ISP: Hostinger International Limited
v]ORG: Hostinger International Limited
v]AS: AS47583 Hostinger International Limited
v]LAT: 53.4788
v]LONG: -2.2585
v]ZIP/POSTAL-CODE: M61
```

#### 4.2.2 Servidor:

A continuación, buscaremos información de vulnerabilidades, información sobre los puertos que tiene abiertos e información más estricta sobre los servidores, por ejemplo saber dónde están alojadas las IP's, información sobre los certificados SSL y un largo etcétera.



Como ya hemos mencionado anteriormente dichos puertos se hallan abiertos, aunque los dos cuentan con requisitos de seguridad ante un posible ataque.

#### 4.2.4 Tecnologías Utilizadas

Aquí podemos observar las tecnologías utilizadas para poder crear la web. Cada *widget* visto en la siguiente imagen ha sido utilizado para diferentes funcionalidades, como por ejemplo *Wordpress Plugins* el cual ha sido utilizado para obtener más herramientas funcionales, de esta manera tendrá más ventajas a la hora de crear la página web dado que le dará una funcionalidad extra.

## Contact Form 7

[Contact Form 7 Usage Statistics](#) · [Download List of All Websites using Contact Form 7](#)

Specifically designed for wordpress blogs. Contact Form 7 can manage multiple contact forms, plus you can customize the form and the mail contents flexibly with simple markup.

Feedback Forms and Surveys

## Lightspeed Cache

[Lightspeed Cache Usage Statistics](#) · [Download List of All Websites using Lightspeed Cache](#)

Wordpress performance cache.

WordPress Plugins

## Google Font API

[Google Font API Usage Statistics](#) · [Download List of All Websites using Google Font API](#)

The Google Font API helps you add web fonts to any web page.

Fonts

## Wordpress Plugins

[Wordpress Plugins Usage Statistics](#) · [Download List of All Websites using Wordpress Plugins](#)

Plugins are tools to extend the functionality of WordPress. The website uses various plugins from WordPress to provide additional functionality. Some of them may be listed here.

## CrUX Dataset

[CrUX Dataset Usage Statistics](#) · [Download List of All Websites using CrUX Dataset](#)

CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.

### CrUX Top 10m

[CrUX Top 10m Usage Statistics](#) · [Download List of All Websites using CrUX Top 10m](#)

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 10 million.

## 5. Información corporativa

### 5.1 Equipo directivo

Ejecutivo de ventas: Julio Redondo Vicente

Ejecutivo de ventas: Inmaculada Serichol Lopez

Directora de proyectos: Yuleyxi Vallejo Tarira

Directora de proyecto: Natalia Juarez

Director de proyecto: Aitor Ortiz

Director comercial: Rafael Machin Torres

### 5.2 Personal de la empresa

Delegado de zona: Isael Cadenas Alvarez

Asesor Energetico: Oscar Gomez

Administrativo Energético: Miguel Angel Alava

Auxiliar administrativo: Celia Navarro Herrera

## 6. Recomendaciones

En rasgos generales no existen vulnerabilidades reseñables vistas, es cierto que al ser una microempresa la opción de búsqueda se reduce a poco y por tanto las posibles brechas de seguridad son menores.

Durante la realización del informe se percibió un fallo en la transferencia de zona lo cual es positivo ya que manifiesta una buena seguridad por parte de la empresa.

De manera general nuestras recomendaciones se centran en salvaguardar la integridad de la empresa contra posibles ciberamenazas, y por ende es crucial adoptar medidas como la capacitación contra phishing, el uso de comunicaciones seguras con VPN, máquinas virtuales actualizadas, contratación de expertos en ciberseguridad, mantenimiento constante de software y aplicando firewalls para proteger contra accesos no autorizados. Estas acciones fortalecen la seguridad de la empresa de manera integral.