

# Concienciación

Reduciendo la superficie de exposición de mi organización

Miguel Ángel Arroyo Moreno



# C0r0n4Con: Colaboración con Cruz Roja frente al COVID-19

Cruz Roja Española

## Plan Cruz Roja RESPONDE frente al COVID-19

En el marco del Estado de Alarma Nacional, lanzando el Plan Cruz Roja RESPONDE frente al COVID-19 para las personas en situación de vulnerabilidad y población general, en coordinación con todas las administraciones públicas. Un plan concreto de actuación y respuesta para los próximos dos meses y que pretende alcanzar a más de 1,350.000 personas con un presupuesto estimado de 11,000.000 €, al que podrá sumarse a todo aquel que quiera contribuir. El plan pretende movilizar a más de 40.000 personas voluntarias que materializarán las respuestas previstas en todo el Estado a través de sus más de 1.400 puntos de atención..

SITIO DE DONACIONES DE CRUZ ROJA



## ***Nos pasamos el día gestionando riesgos***

*Identificando **amenazas**, que **probabilidad** hay que se materialicen y qué **impacto** podrían tener.*

***Ejemplos;** salir a calle en cuarentena, coger el coche sin cinturón...*

# Gestión de riesgos como piedra angular de la ciberseguridad





## ***Cantidad y calidad de la información publicada de una organización en Internet.***

*¿Qué sabe Internet de nosotros?*

*¿Qué información podría obtener un posible atacante?*

# IoE: Indicadores de Exposición

Servicios publicados en la red  
Fugas de información (intencionado)  
Revelación de información sensible (no intencionado)  
Una dirección IP  
Una dirección URL  
Un subdominio  
**Una cuenta de correo**  
Versión de un software  
Un nombre de usuario  
Nombres y apellidos  
Aficiones  
Lugar de trabajo  
Lugar de estudio  
Una localización

...

# Superficie de exposición: ¿Información irrelevante?

- ¿Información irrelevante?

“Las **notas** musicales son sólo cinco, pero sus melodías son tan numerosas que no podemos oírlas todas.

Los **colores** primarios son sólo cinco, pero sus combinaciones son tan infinitas que no podemos verlas todas.

Los **gustos** son sólo cinco, pero sus mezclas son tan variadas que no podemos saborearlas todas.”

*Sun Tzu, El arte de la guerra*

- **Evitar la publicación innecesaria**
- **Amenaza:** Información interesante para cometer **fraudes**



*Famoso estratega militar chino*

**Fraudes:** Existen diferentes tipo de fraudes, entre los que destaca...

***Engaño económico con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado.***

(Por desgracia, no es nada nuevo)



## Victor Lustig – “El hombre que vendió la Torre Eiffel dos veces”



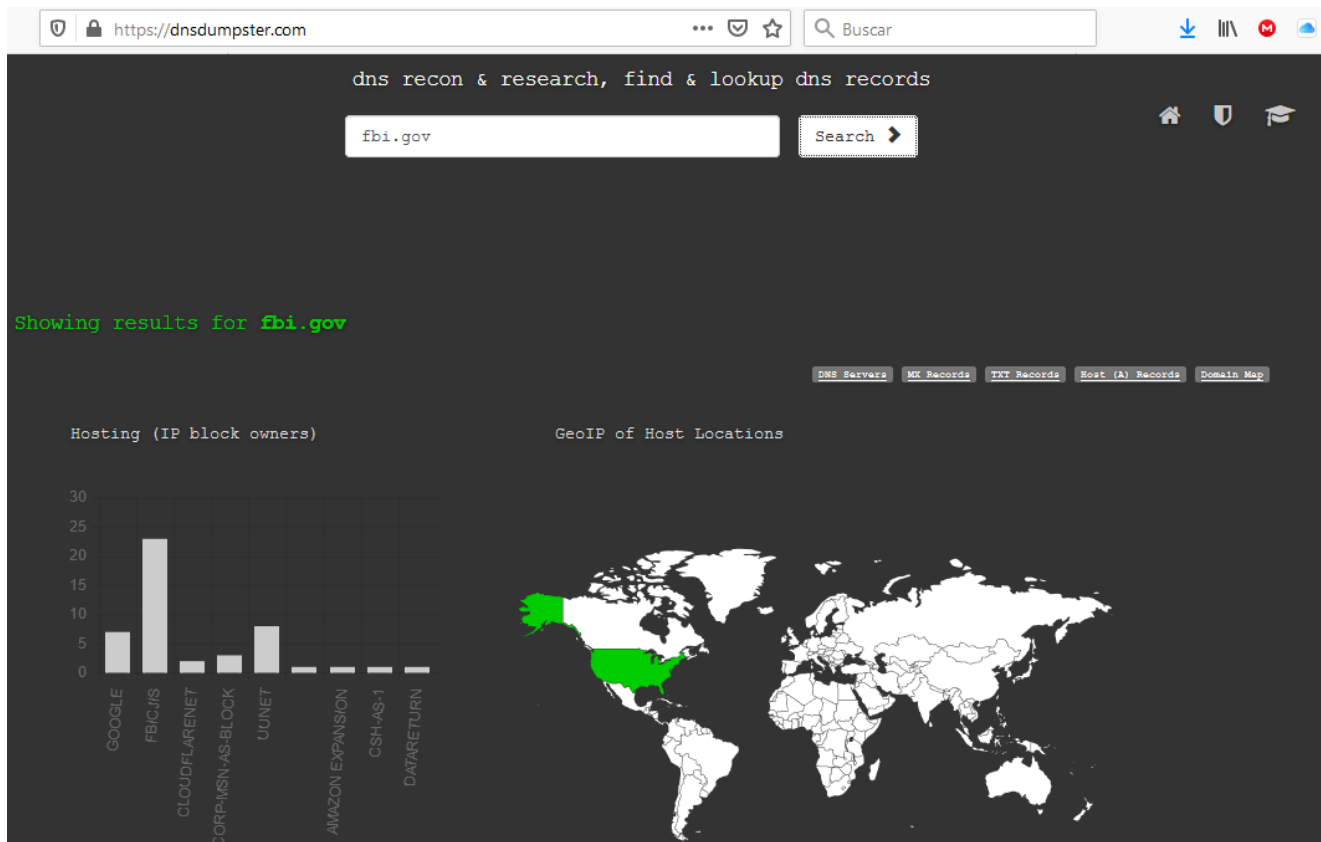
# Limitaciones Espacio / Tiempo



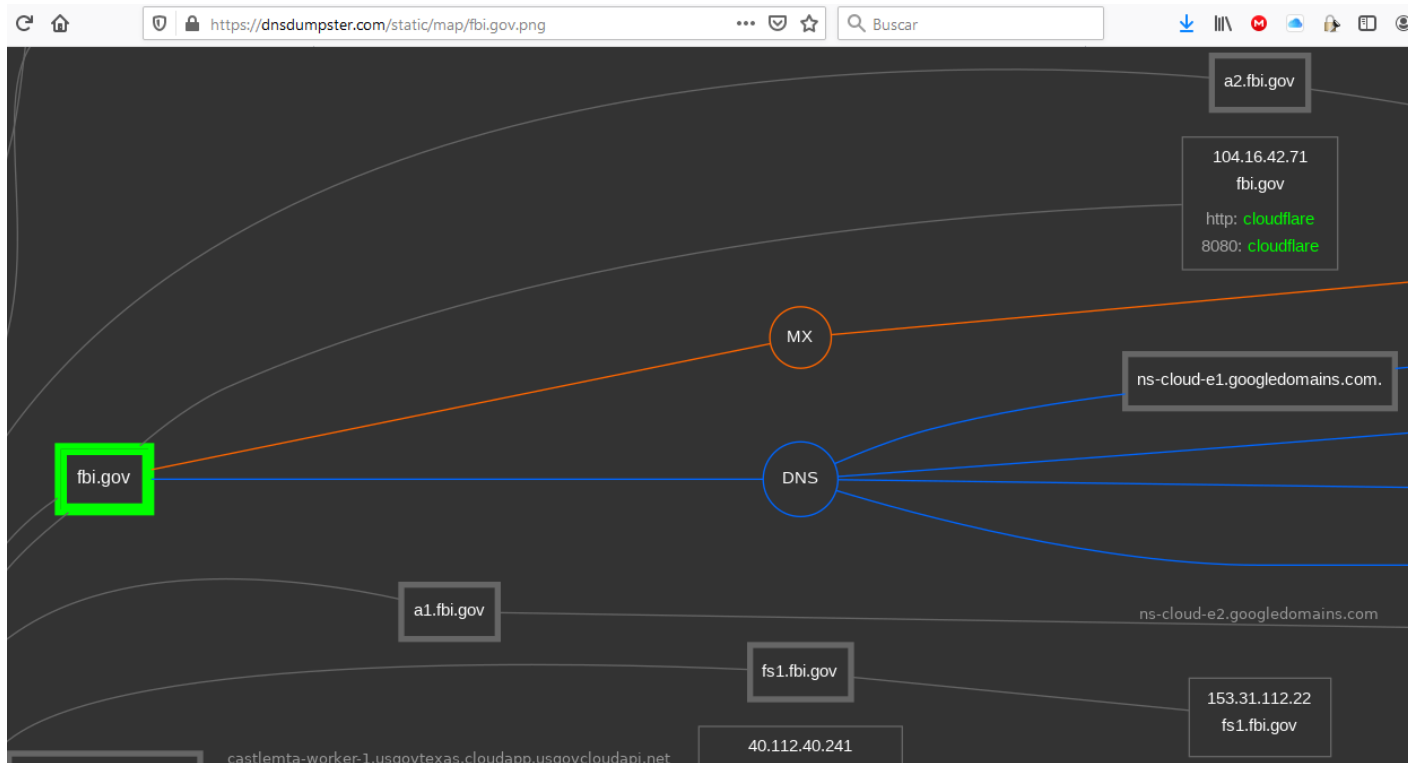
¿Todo es cuestión de (mala) suerte?



# DNS Dumpster: Dominios y subdominios como IoE



# DNS Dumpster: Dominios y subdominios como IoE



# Vectores de ataque: *Correo electrónico como el más rápido y simple*





# Vigila tus cuentas de correo: ¿Te has buscado alguna vez en Google?



"morganalan99@live.co.uk"



Todo

Noticias

Maps

Imágenes

Shopping

Más

Configuración

Herramientas

Aproximadamente 4 resultados (0,27 segundos)

## Facebook Free Accounts Hacked By Deepika Dixit - Username List

[username-list.blogspot.com/.../facebook-free-accounts-hacked.html](https://username-list.blogspot.com/.../facebook-free-accounts-hacked.html) ▼ Traducir esta página

11 abr. 2018 - Facebook Free Accounts Hacked By Deepika Dixit. Email & Password:

**morganalan99@live.co.uk**:Morganalan99, proxy: 159.65.110.167:3128

# Credenciales robadas: ...y publicadas en la red

```
some free facebook accounts all cracked by ring
```

```
Email & Password: morganalan99@live.co.uk:Morganalan99,  
proxy: 159.65.110.167:3128
```

```
=====
```

```
Email & Password: soccer1232008@aol.com:lucky2006,  
proxy: 166.78.156.213:3128
```

```
=====
```

```
Email & Password: javivc1334@outlook.com:Javigenial123,  
proxy: 80.211.4.187:8080
```

```
=====
```

```
Email & Password: jonhoaglin@gmail.com:Beer0204,  
proxy: 159.65.110.167:3128
```

```
=====
```

```
Email & Password: toby.vankaathoven@gmail.com:23twa888vAn,  
proxy: 80.211.4.187:8080
```

```
=====
```

```
Email & Password: blu76@windowslive.com:Blu!733210,  
proxy: 166.78.156.213:3128
```

```
=====
```

```
Email & Password: jossylvia@kpnmail.nl:molen123,  
proxy: 89.236.17.106:3128
```

# Email Harvesting: Búsqueda de correos en fuentes abiertas

https://hunter.io/search/fbi.gov


hunter Product Pricing Sign in Sign up








fbi.gov Find email addresses

Most common pattern: {f}{last}@fbi.gov 1,153 email addresses

d elino@fbi.gov	2 sources
j hweitzer@fbi.gov	1 source
d tizer@fbi.gov	1 source

# LinkedIn como indicador de exposición (IoE): Cuentas de correo





 Inicio  Mi red  Empleos  Mensajes  Notificaciones  Yo  Productos Abónete gratis a Premium

Gente ▼ **NASA - National Aeronautics and Space Administration ▼** Contactos ▼ Ubicaciones ▼ Todos los filtros Quitar 1

Quality. Simplified. - Easy to use SOP, document control and training software. 30-day Free Trial! Anuncio ...


Mostrando 19.089 resultados




**William (Tony) Cole** • 2º 

CTO Attivo Networks | NASA Advisory Council | (ISC)<sup>2</sup> Board of Directors | Bayshore Net...  
Área Metropolitana de Washington D.C., Estados Unidos

Actual: Member, NASA Advisory Council (NAC) en NASA - National Aeronautics and Space Administration


 21 contactos en común

Conectar




**Oscar Pérez Pinazo** • 2º

Astronaut & Payload Operations Director at NASA en NASA  
Valencia y alrededores, España

 2 contactos en común


Conectar



**Dr. Michael Jarrah** • 2º

NASA HQ, Head of Network Infrastructure  
Área Metropolitana de Washington D.C., Estados Unidos

Actual: Head of Network Infrastructure, TS en NASA HQ


 2 contactos en común

Conectar

Búsquedas guardadas

Guarda esta búsqueda y recibe notificaciones cuando haya nuevos resultados disponibles.

Crear alerta de búsqueda



# Email Assumption: Descubrir las a través de posibles combinaciones

## Email Assumptions

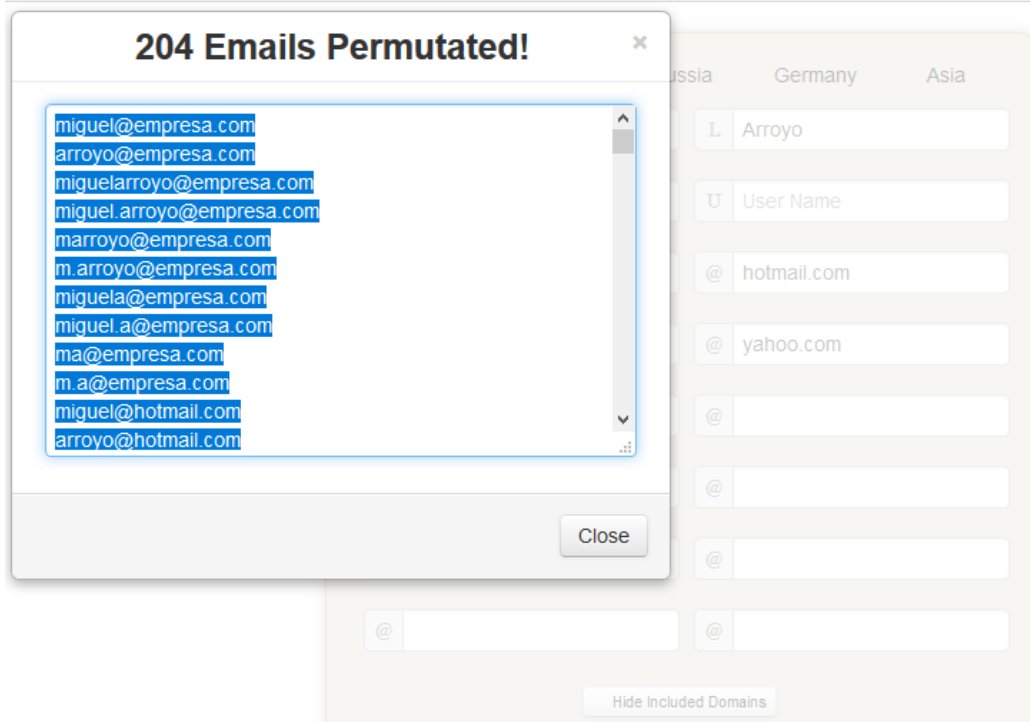
<u>Global</u>	<u>Americas</u>	Russia	Germany	Asia
F Miguel	L Arroyo			
M Middle Name	U User Name			
@ empresa.com	@ hotmail.com			
@ gmail.com	@ yahoo.com			
@ live.com	@			
@	@			
@ outlook.com	@			
@	@			

Hide Included Domains

Submit

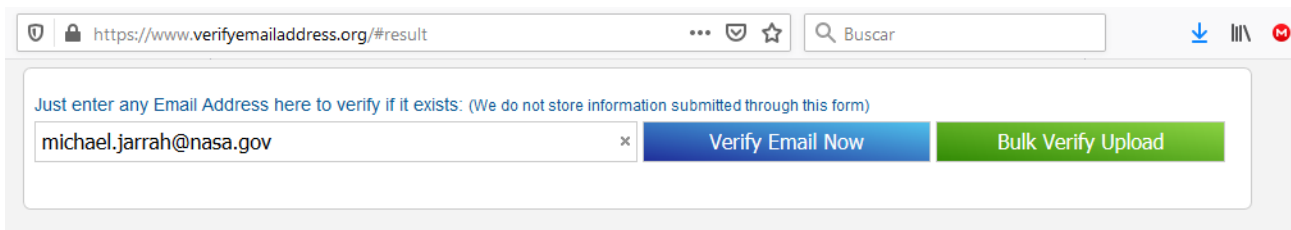
# Email Assumption: Descubrir las a través de posibles combinaciones

## Email Assumptions





# Comprobando existencia de una cuenta de correo...



The screenshot shows a web browser window with the URL <https://www.verifyemailaddress.org/#result>. The page has a search bar with the text "Buscar". Below the search bar, there is a text input field containing "michael.jarrah@nasa.gov" and a close button (x). To the right of the input field are two buttons: "Verify Email Now" (blue) and "Bulk Verify Upload" (green). Above the input field, there is a line of text: "Just enter any Email Address here to verify if it exists: (We do not store information submitted through this form)".

Your results for michael.jarrah@nasa.gov will be displayed below after processing.

## We found that:

- ✓ The Email Address Syntax is correct
- ✓ Connecting to ndjsvnpf102.ndc.nasa.gov worked
- ✓ We feel that michael.jarrah@nasa.gov is valid

[View Email Owner](#)

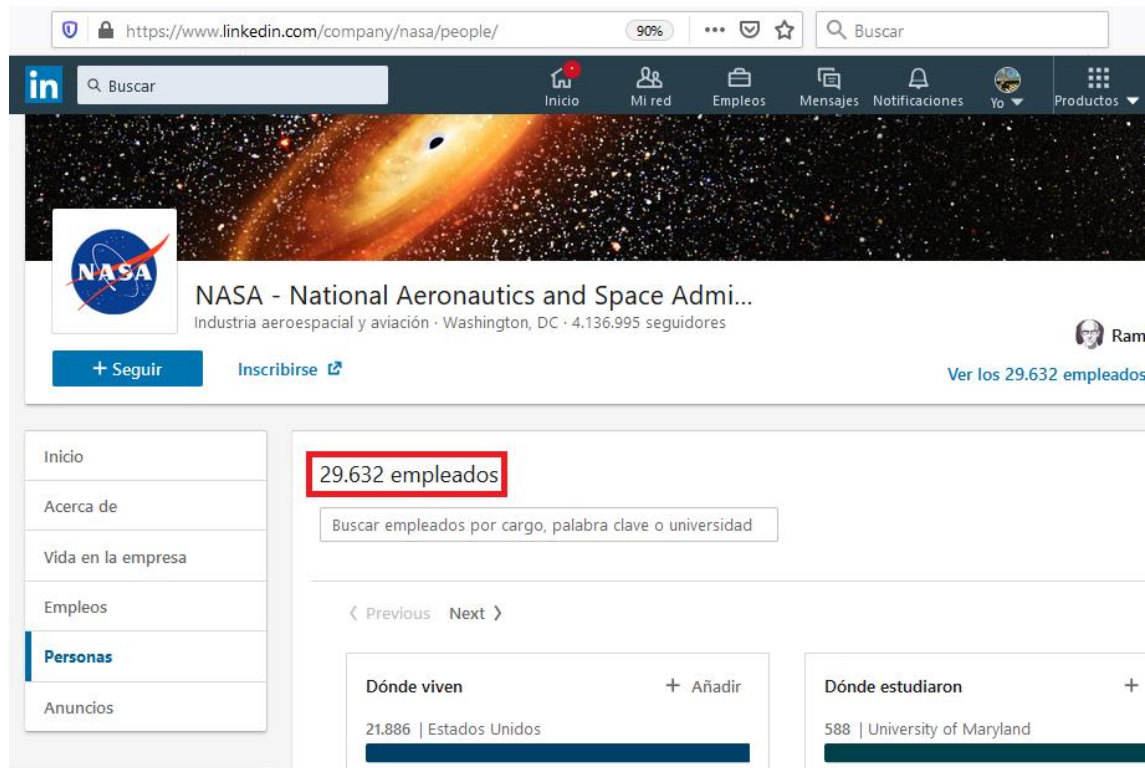
[Show details](#)

## Now what would you like to do?

[Upload Entire List](#)

[Test Another Email](#)


# ¿Y si repetimos los mismos pasos con los diferentes empleados?



The screenshot shows the LinkedIn profile of NASA. The header includes the NASA logo and the text "NASA - National Aeronautics and Space Admini..." with "Industria aeroespacial y aviación · Washington, DC · 4.136.995 seguidores". Below this, a blue button says "+ Seguir" and a link says "Inscribirse". To the right, it says "Ver los 29.632 empleados". The left sidebar has a menu with "Inicio", "Acerca de", "Vida en la empresa", "Empleos", "Personas" (highlighted), and "Anuncios". The main content area shows "29.632 empleados" in a red box, followed by a search bar "Buscar empleados por cargo, palabra clave o universidad". Below are two sections: "Dónde viven" with "21.886 | Estados Unidos" and "Dónde estudiaron" with "588 | University of Maryland".

https://www.linkedin.com/company/nasa/people/ 90% Buscar

in Buscar Inicio Mi red Empleos Mensajes Notificaciones Yo Productos

 NASA - National Aeronautics and Space Admini...  
Industria aeroespacial y aviación · Washington, DC · 4.136.995 seguidores

+ Seguir Inscribirse Ver los 29.632 empleados

Inicio  
Acerca de  
Vida en la empresa  
Empleos  
**Personas**  
Anuncios

**29.632 empleados**

Buscar empleados por cargo, palabra clave o universidad

< Previous Next >

Dónde viven + Añadir  
21.886 | Estados Unidos

Dónde estudiaron +  
588 | University of Maryland

# Cuanto más cuentas de correo válidas, más probabilidad...

- **Ataque directo a uno de los eslabones más débiles**
- **Explotación de la ingeniería social**
  - Intento de engaño a la víctima que recibe el correo
- **¿Qué podemos hacer?**
  - Monitorizar cuentas publicadas directamente en internet
  - Monitorizar cuentas publicadas indirectamente en internet
  - Formación y concienciación a los usuarios
  - Software antimalware actualizado
  - Contemplar si perfiles sensibles (director financiero o CEO) pueden publicar dicha información en RRSS

Cuanto mayor sea el conocimiento de la amenaza, mejor

*“Sólo cuando  
conoces cada  
detalle de la  
condición del  
terreno puedes  
maniobrar y  
luchar”*

Sun  
Tzu's  
THE  
ART  
OF  
WAR



C0r0n4Con: Enviar justificante a [info@c0r0n4con.com](mailto:info@c0r0n4con.com)

Cruz Roja Española

## Plan Cruz Roja RESPONDE frente al COVID-19

En el marco del Estado de Alarma Nacional, lanzando el Plan Cruz Roja RESPONDE frente al COVID-19 para las personas en situación de vulnerabilidad y población general, en coordinación con todas las administraciones públicas. Un plan concreto de actuación y respuesta para los próximos dos meses y que pretende alcanzar a más de 1,350.000 personas con un presupuesto estimado de 11,000.000 €, al que podrá sumarse a todo aquel que quiera contribuir. El plan pretende movilizar a más de 40.000 personas voluntarias que materializarán las respuestas previstas en todo el Estado a través de sus más de 1.400 puntos de atención..

SITIO DE DONACIONES DE CRUZ ROJA



C0r0n4Con: Cerca de 30.000 euros recaudados, ¡30.000 GRACIAS!

Gratitude  
is the best  
Attitude