

# Google Dorking en Seguridad Ofensiva: Técnicas OSINT reales para mapear empresas expuestas



**Daniel Espinosa Delgado**

La superficie de ataque no siempre empieza en la red... a veces empieza en Google



# Google Dorking en Seguridad Ofensiva:

## *Técnicas OSINT reales para mapear empresas expuestas*

### Introducción

**Google Dorking**, también conocido como **Google Hacking**, es una técnica que utiliza operadores avanzados de búsqueda en Google para encontrar información específica en la web que no es visible mediante búsquedas convencionales.

Se usa para localizar:

- Archivos confidenciales
- Contraseñas
- Correos electrónicos
- Logs
- Bases de datos
- Paneles de administración
- Cámaras abiertas
- Y más...

Esta guía está diseñada para ayudarte a utilizar Google de forma efectiva como herramienta de **inteligencia de código abierto (OSINT)** y **auditoría de seguridad**.

---

### Fundamentos: Operadores Lógicos y Básicos

#### Lógica de búsqueda

- palabra1: Búsqueda directa.
  - palabra1 palabra2: Busca ambas palabras, juntas o por separado.
  - palabra1 OR palabra2 o palabra1 | palabra2: Encuentra una u otra.
  - palabra1 AND palabra2 o palabra1 && palabra2: Ambas deben estar.
  - palabra1 -palabra2: Excluye palabra2.
  - palabra1 +palabra2: Obliga a incluir palabra2.
  - "palabra1 palabra2": Búsqueda exacta.
  - \*palabra: Comodín de búsqueda popular.
-



## Operadores Clave en Google Hacking

Operador	Función
site:	Limita la búsqueda a un dominio específico.
filetype:	Filtra por tipo de archivo: filetype:pdf, filetype:sql.
inurl:	Filtra por palabras dentro de la URL.
intitle:	Filtra por palabras en el título de la página.
intext:	Busca contenido dentro del texto de la web.
allinurl:	Todas las palabras deben estar en la URL.
allintitle:	Todas las palabras deben estar en el título.
ext:	Alternativa a filetype:.
cache:	Muestra la versión en caché de un sitio.
info:	Muestra información general sobre una página.

---

## Encontrar Correos Electrónicos

### Dork básico:

site:nasa.gov inurl:contact "@nasa.gov"

### Correos dentro de documentos:

site:nasa.gov filetype:doc OR filetype:xls OR filetype:txt "@nasa.gov"

✅ *Tip:* combiná estos resultados con herramientas como [Intelligence X](#) para comprobar si hay credenciales expuestas.

---

## Directory Listings

Visualiza archivos abiertos accidentalmente en el servidor:

site:nasa.gov intitle:index.of

👉 También podés buscar por palabras clave como sql, backup, logs:

site:nasa.gov intitle:index.of sql

---

## Archivos de Configuración

Estos archivos suelen contener claves, rutas y configuraciones sensibles:

site:nasa.gov ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp |  
ext:cfg | ext:txt | ext:ora | ext:ini

---



## Base de Datos y SQL Errors

### Buscar archivos SQL:

site:nasa.gov ext:sql

### Buscar errores de SQL visibles:

site:nasa.gov intext:"SQL syntax near" | intext:"Warning: mysql\_connect()" |  
intext:"ORA-"

Estos mensajes pueden indicar vulnerabilidades de inyección SQL (SQLi) o exposición de backend.

---

## Archivos de Logs

### Logs del sistema o aplicaciones:

site:nasa.gov ext:log

### Logs con posibles contraseñas:

site:nasa.gov "password" filetype:log

---

## Herramientas Automáticas

 [Pentest-tools.com](https://pentest-tools.com)

Ofrece automatización de dorks organizados por categoría (admin pages, sensitive files, directory listing...).

 [Exploit-DB Google Hacking Database](https://www.exploit-db.com/google-hacking-database/)

Base de datos con miles de dorks clasificados por servicio y tipo de vulnerabilidad.

---

## Cloud Dorks – Archivos en la Nube

Servicio	Dork
Google Drive	site:docs.google.com inurl:"/d/" "example.com"
OneDrive	site:onedrive.live.com "example.com"
Dropbox	site:dropbox.com/s "example.com"
Box	site:box.com/s "example.com"
Firebase	site:firebaseio.com "example"
Amazon S3	site:s3.amazonaws.com "example.com"
Azure Blob	site:blob.core.windows.net "example.com"
Google APIs	site:googleapis.com "example.com"



## Google Dorks para Vulnerabilidades

### XSS:

`inurl:q= | inurl:s= | inurl:search= | inurl:query= site:example.com`

### Open Redirect:

`inurl:url= | inurl:return= | inurl:next= | inurl:redirect= inurl:http  
site:example.com`

### Bug Bounty Programs:

`site:openbugbounty.org inurl:reports intext:"yahoo.com"`

---

## Dorks por CMS

CMS	Dork
WordPress	<code>inurl:/wp-admin/admin-ajax.php</code>
Drupal	<code>intext:"Powered by" &amp; intext:Drupal &amp; inurl:user</code>
Joomla	<code>site:*/joomla/login</code>

---

## Combinaciones Avanzadas y Ejemplos Creativos

- Reducir resultados irrelevantes:

`site:tesla.com -www -shop -careers`

- Búsqueda de endpoints de subida de archivos:

`(site:tesla.com | site:teslamotors.com) & "choose file"`

- Código publicado en sitios de developers:




`site:pastebin.com | site:codepen.io | site:jsfiddle.net "tesla.com"`

---

## Casos de uso en OSINT

- ✓ Recolectar datos de organizaciones
- ✓ Detectar errores de configuración
- ✓ Localizar documentos internos filtrados
- ✓ Descubrir superficie de ataque digital
- ✓ Verificar fugas de información personal




-  [Google Hacking - Pentest Tools](#)
-  [Exploit-DB Google Hacking Database](#)
-  [OSINT Framework](#)



---


## Conclusión

Google Dorking es una técnica poderosa en las manos adecuadas. Usado éticamente, puede ayudarte a descubrir información que **no debería estar accesible públicamente**.


 **Advertencia legal:** acceder o explotar información sin autorización puede ser ilegal. Esta guía tiene fines educativos y de concienciación para mejorar la ciberseguridad.

---

 **Autor: Daniel Espinosa Delgado**

 Fecha: Abril 2025

 Contacto: danyjerez@proton.me

 Licencia: Uso educativo y profesional – se permite compartir con atribución.

---