Para que tus subdominios de acceso interno no aparezcan en Google (o en otros buscadores), puedes combinar varias medidas “manuales” y de configuración en tu servidor o plataforma:

1. Autenticación obligatoria

• HTTP Basic Auth (.htpasswd) o formulario de login front-end.

• Sin credenciales no se devuelve ni siquiera un 200 OK, de modo que los crawlers no pueden indexar nada.

2. Código de estado 401/403 para bots

• En función del agente de usuario (user-agent) identifica bots (Googlebot, Bingbot…) y devuélveles 401 o 403.

• Para usuarios reales, tras autenticación, sirves el 200.

3. Archivo robots.txt

• Crearlo en la raíz de cada subdominio con:

User-agent: \*

Disallow: /

• Nota: es una directiva voluntaria; puede que bots maliciosos la ignoren.

4. Metaetiqueta y cabecera HTTP No-Index

• Añade en el <head> de tu HTML:

<meta name="robots" content="noindex,nofollow">

• O bien, como cabecera HTTP en tus respuestas (Apache, Nginx):

X-Robots-Tag: “noindex, nofollow”

5. No publicar enlaces externos

• No debes enlazar (ni desde tu web pública ni desde páginas de terceros) a esos subdominios.

• Google los descubre siguiendo enlaces, así que si no existen referencias públicas, es muy poco probable que los linkees en su índice.

6. Remoción de URLs ya indexadas

• Google Search Console > Eliminación de URL: solicita la retirada temporal de URLs ya indexadas.

• Una vez fuera, mantén los métodos anteriores para que no se reindexen.

7. DNS y configuración de red

• Usa un registro DNS interno (nombre interno, sólo resoluble en tu red LAN o VPN).

• Si lo necesitas públicamente, configura un firewall o regla de red que permita sólo IPs de tu organización.

8. Single Sign-On tipo Office365

• Implementa un proveedor de identidad (Azure AD, Okta, Auth0).

• Sin token válido, la conexión es redirigida a una página de login: sin login no hay contenido accesible ni indexable.

Recomendación rápida para un entorno mixto “manual” y seguro:

1) Protege con autenticación básica + redirige bots a 401.

2) Pon robots.txt y meta noindex.

3) Elimina de Search Console las URLs antiguas.

4) Si puedes, mueve esos subdominios a DNS internos o sólo resuelve tras VPN/SSO.

Con esta combinación reduces drásticamente la posibilidad de que Google (y la mayoría de bots) vea e indexe tus subdominios de acceso.

Para proteger los subdominios y evitar que aparezcan en los resultados de búsqueda de Google, puedes implementar varias estrategias. A continuación, se detallan algunas formas de hacerlo manualmente sin publicar la página:

### 1. \*\*Uso de Archivos Robots.txt\*\*

El archivo `robots.txt` es una forma estándar de indicar a los motores de búsqueda qué partes de tu sitio web no deben ser indexadas.

- \*\*Descripción\*\*: Crea un archivo `robots.txt` en la raíz de tu subdominio.

- \*\*Implementación\*\*:

- Crea un archivo llamado `robots.txt` en la raíz del subdominio.

- Añade las siguientes líneas para bloquear el acceso a todos los motores de búsqueda:

```plaintext

User-agent: \*

Disallow: /

```

- Esto indicará a los motores de búsqueda que no deben indexar ninguna parte del subdominio.

### 2. \*\*Metaetiquetas Noindex\*\*

Puedes añadir una metaetiqueta en el `<head>` de tus páginas HTML para indicar que no deben ser indexadas.

- \*\*Descripción\*\*: Añade una metaetiqueta en el `<head>` de cada página que no deseas que sea indexada.

- \*\*Implementación\*\*:

- Añade la siguiente línea en el `<head>` de cada página:

```html

<meta name="robots" content="noindex">

```

### 3. \*\*Configuración de DNS\*\*

Asegúrate de que los subdominios no estén configurados para ser accesibles públicamente si no es necesario.

- \*\*Descripción\*\*: Revisa la configuración de DNS y asegúrate de que los subdominios no estén apuntando a direcciones IP públicas si no deben ser accesibles.

- \*\*Implementación\*\*:

- Accede a la configuración de DNS de tu proveedor de servicios.

- Asegúrate de que los registros DNS para los subdominios no estén configurados para resolver a direcciones IP públicas.

### 4. \*\*Autenticación Básica\*\*

Implementar autenticación básica para proteger el acceso a los subdominios.

- \*\*Descripción\*\*: Configura la autenticación básica en el servidor web.

- \*\*Implementación\*\*:

- Para Apache, puedes usar un archivo `.htaccess`:

```apache

AuthType Basic

AuthName "Restricted Area"

AuthUserFile /path/to/.htpasswd

Require valid-user

```

- Para Nginx, puedes configurar la autenticación básica en el archivo de configuración del servidor:

```nginx

location / {

auth\_basic "Restricted Area";

auth\_basic\_user\_file /path/to/.htpasswd;

}

```

### 5. \*\*Configuración de Seguridad en el Servidor\*\*

Asegúrate de que tu servidor esté configurado para no permitir el acceso a los subdominios sin las credenciales adecuadas.

- \*\*Descripción\*\*: Configura las reglas de acceso en el servidor para restringir el acceso a los subdominios.

- \*\*Implementación\*\*:

- Para Apache, puedes usar módulos como `mod\_rewrite` para redirigir o bloquear el acceso.

- Para Nginx, puedes usar directivas como `deny` y `allow` para controlar el acceso.

### 6. \*\*Uso de Herramientas de Seguridad\*\*

Considera el uso de herramientas de seguridad que ofrezcan características de ocultación y protección de subdominios.

- \*\*Descripción\*\*: Investiga soluciones de seguridad que se adapten a tus necesidades y que ofrezcan protección adicional.

- \*\*Implementación\*\*:

- Herramientas como Cloudflare pueden ofrecer protección adicional y configuraciones de seguridad avanzadas.

### 7. \*\*Configuración de Google Search Console\*\*

Utiliza Google Search Console para gestionar la indexación de tus subdominios.

- \*\*Descripción\*\*: Añade tu subdominio a Google Search Console y solicita la eliminación de URLs específicas.

- \*\*Implementación\*\*:

- Añade tu subdominio a Google Search Console.

- Usa la herramienta de inspección de URL para solicitar la eliminación de URLs específicas.

### Ejemplo de Implementación en Apache

A continuación, se muestra un ejemplo de cómo configurar la autenticación básica en Apache:

1. \*\*Crear el archivo `.htpasswd`\*\*:

- Usa la herramienta `htpasswd` para crear un archivo de usuarios:

```sh

htpasswd -c /path/to/.htpasswd username

```

- Sigue las instrucciones para establecer la contraseña.

2. \*\*Configurar el archivo