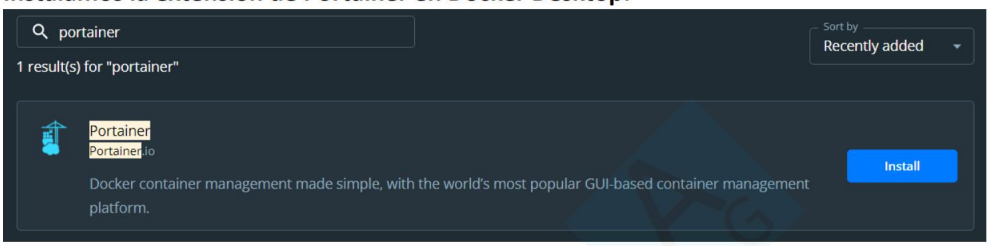
GoPhish propio

A.D.G.

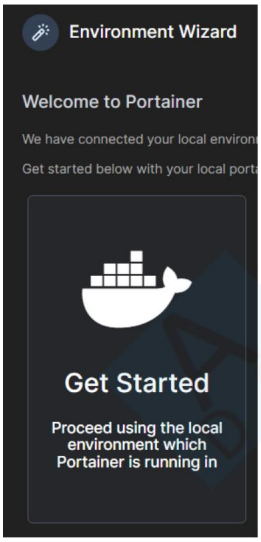
Descargamos el GoPhish a través del contenedor de docker mediante comando en la consola:

```
C:\Users\Andrei>docker pull gophish/gophish
```

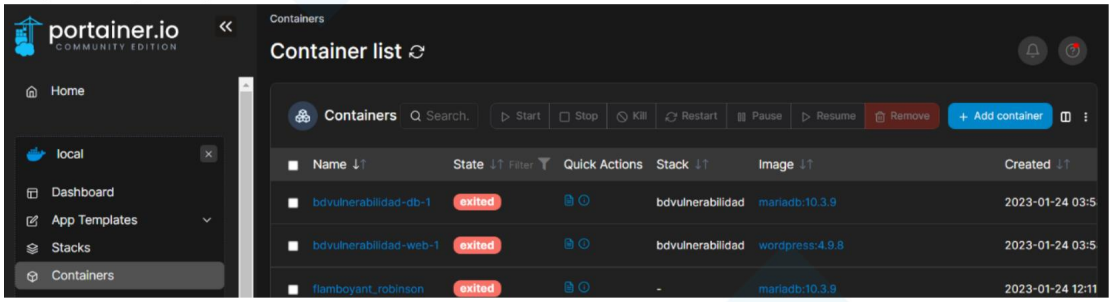
Instalamos la extensión de Portainer en Docker Desktop:



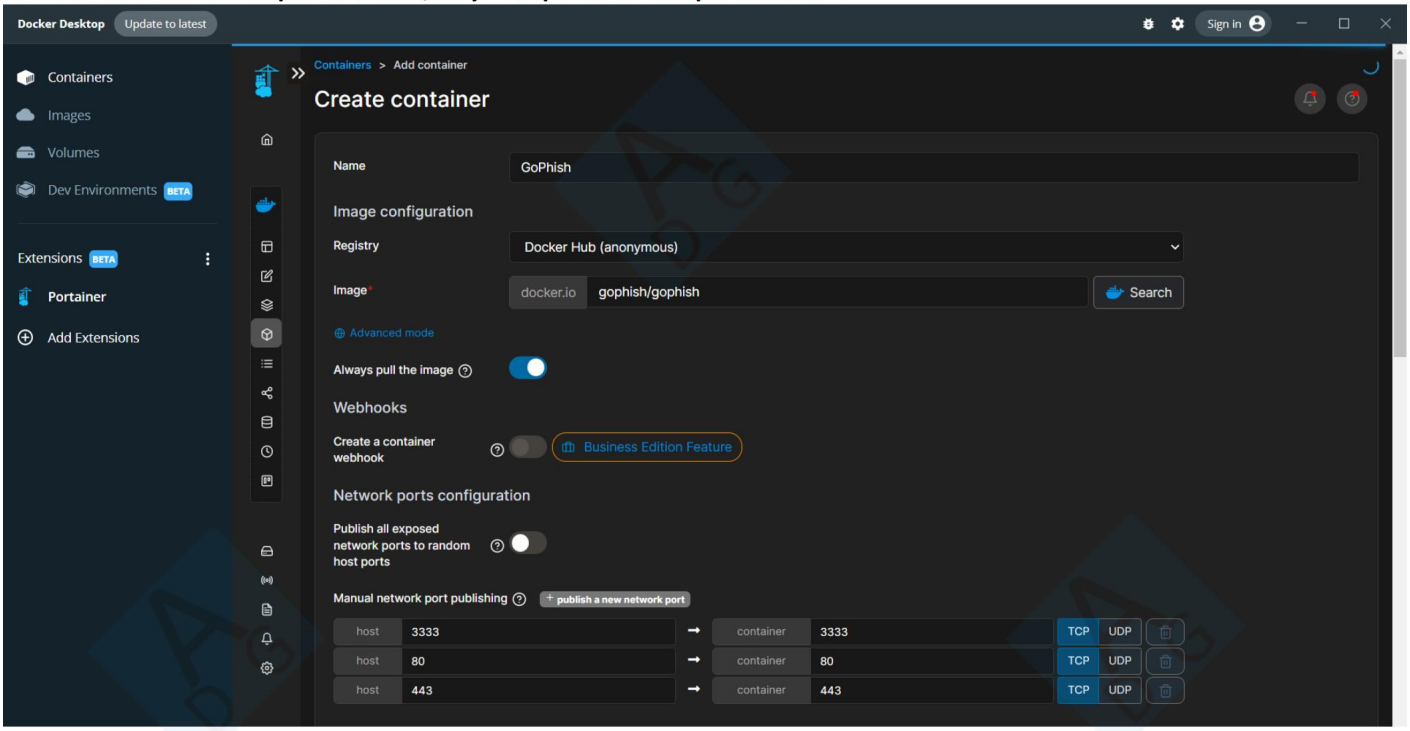
Clickamos en "Get Started":



Luego se llega al apartado de listar los contenedores en "Containers":



Creamos el contenedor. Le asignamos un nombre, le indicamos la imagen "gophish/gophish" y clickamos "Search". También se añadirán los puertos 3333, 80 y 443 que serán los que se usarán:

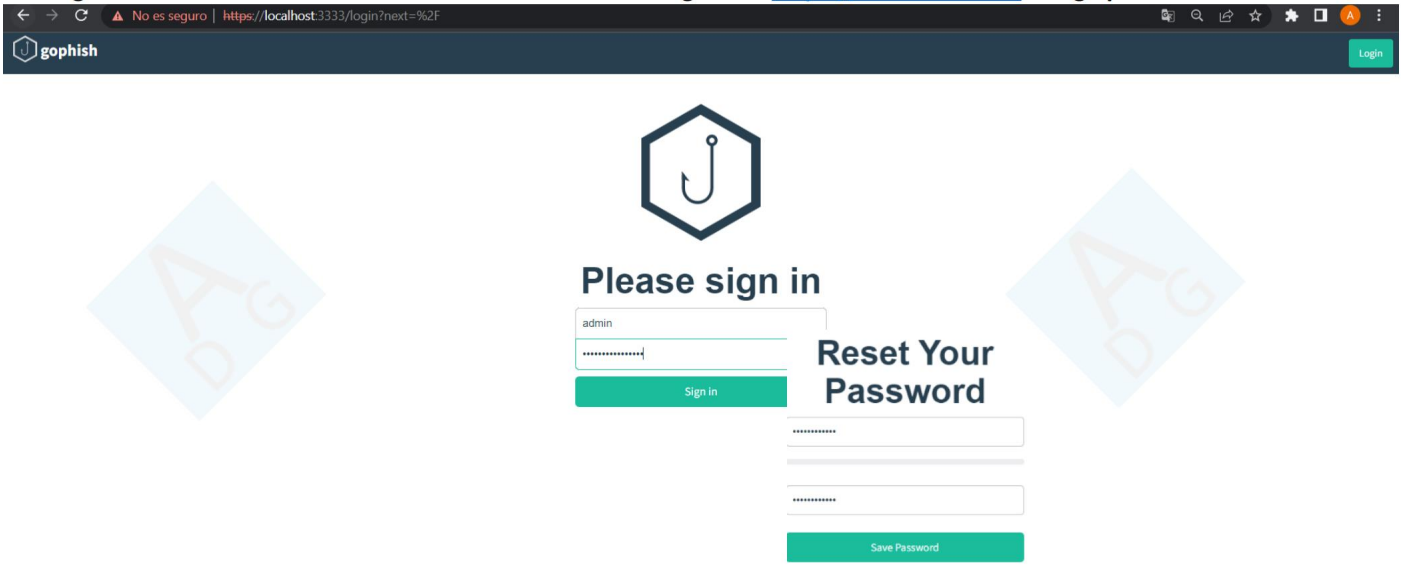


Para ver el usuario y la contraseña, escribir en consola “docker logs GoPhish” y mirar abajo “ Please login with the username “admin” and the password “d71bd0f1d091cb94” “:

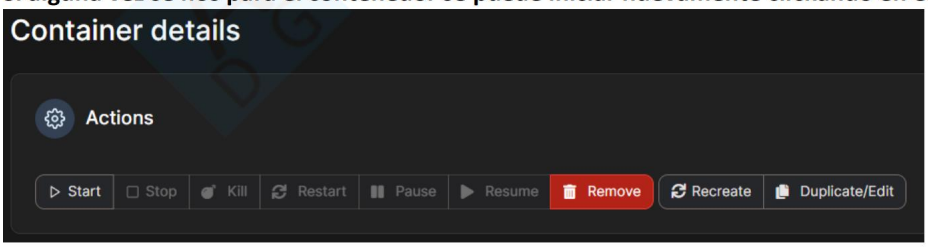
```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2546]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Andrei>docker logs GoPhish
Runtime configuration:
{
        "admin_server": {
                "listen_url": "0.0.0.0:3333",
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key",
                "trusted_origins": []
        },
        "phish_server": {
                "listen_url": "0.0.0.0:80",
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
time="2023-01-24T11:16:32Z" level=warning msg="No contact address has been configured."
time="2023-01-24T11:16:32Z" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK    20160118194630_init.sql
OK    20160131153104_0.1.2_add_event_details.sql
OK    20160211211220_0.1.2_add_ignore_cert_errors.sql
OK    20160217211342_0.1.2_create_from_col_results.sql
OK    20160225173824_0.1.2_capture_credentials.sql
OK    20160227180335_0.1.2_store-smtp-settings.sql
OK    20160317214457_0.2_redirect_url.sql
OK    20160605210903_0.2_campaign_scheduling.sql
OK    20170104220731_0.2_result_statuses.sql
OK    20170219122503_0.2.1_email_headers.sql
OK    20170827141312_0.4_utc_dates.sql
OK    20171027213457_0.4.1_maillogs.sql
OK    20171208201932_0.4.1_next_send_date.sql
OK    20180223101813_0.5.1_user_reporting.sql
OK    20180524203752_0.7.0_result_last_modified.sql
OK    20180527213648_0.7.0_store_email_request.sql
OK    20180830215615_0.7.0_send_by_date.sql
OK    20190105192341_0.8.0_rbac.sql
OK    20191104103306_0.9.0_create_webhooks.sql
OK    20200116000000_0.9.0_imap.sql
OK    20200619000000_0.11.0_password_policy.sql
OK    20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK    20200914000000_0.11.0_last_login.sql
OK    20201201000000_0.11.0_account_locked.sql
OK    20220321133237_0.4.1_envelope_sender.sql
time="2023-01-24T11:16:32Z" level=info msg="Please login with the username admin and the password d71bd0f1d091cb94"
time="2023-01-24T11:16:32Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2023-01-24T11:16:32Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
```

Nos logueamos con esas credenciales entrando desde el navegador a https://localhost:3333. Luego pedirá resetear la clave:

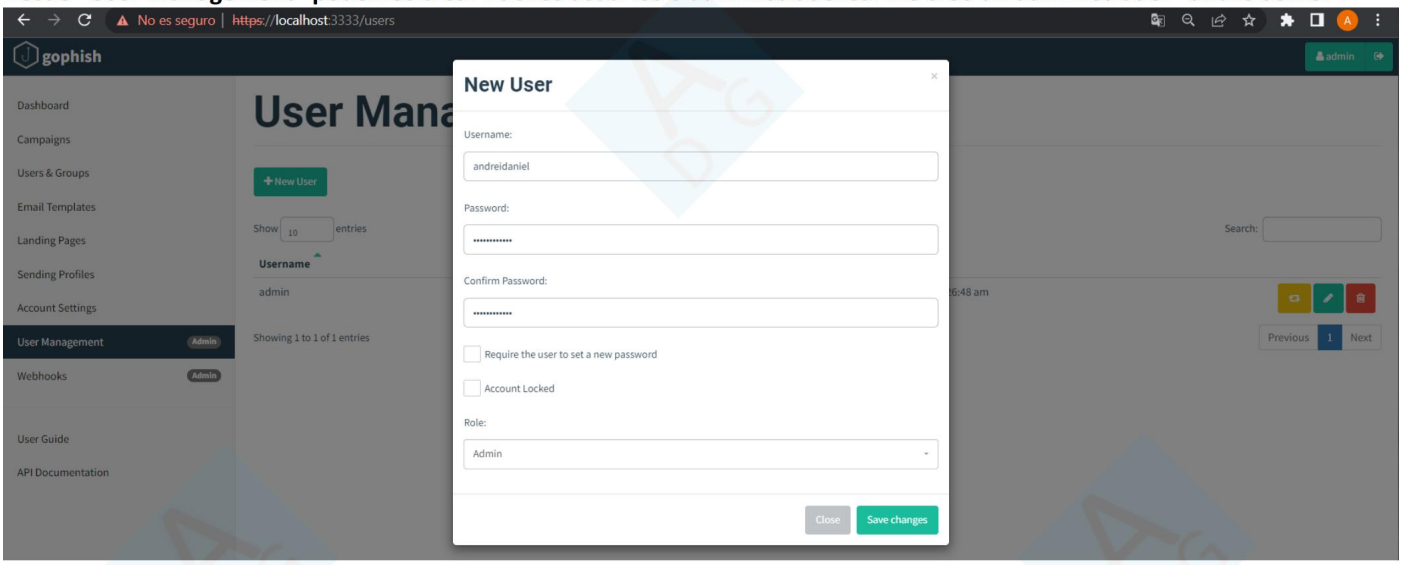


Si alguna vez se nos para el contenedor se puede iniciar nuevamente clickando en el contenedor y “Start”:

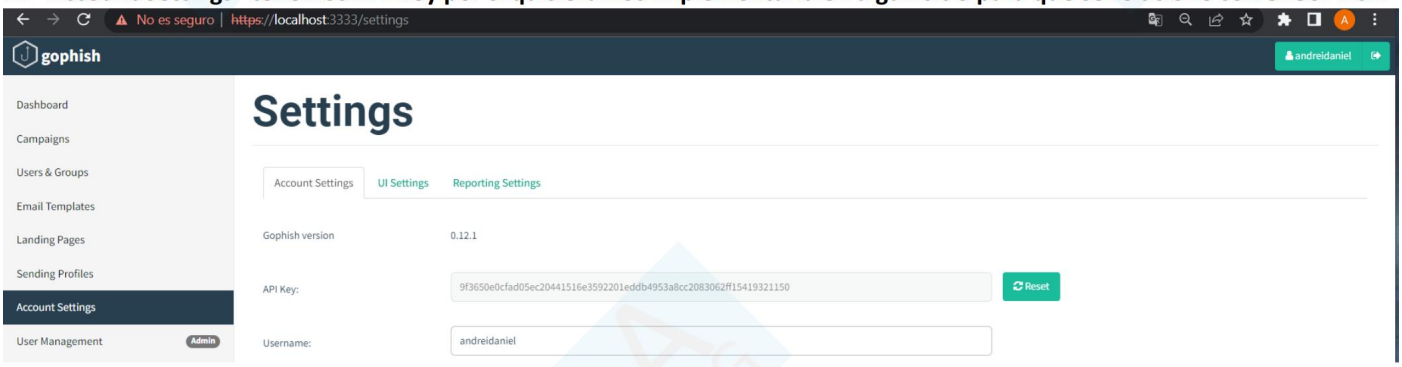


Ahora pasamos a las configuraciones adentro del GoPhish:

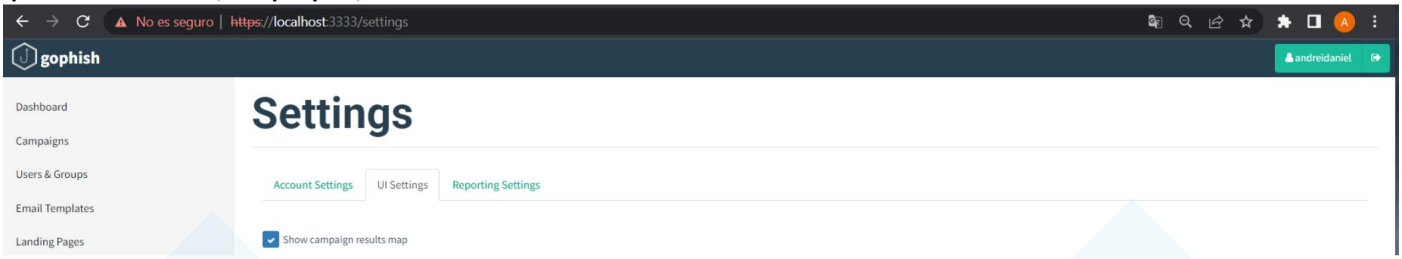
Desde “User Management” podemos crear nuevos usuarios ó administradores. Me creo un administrador “andreidaniel”:



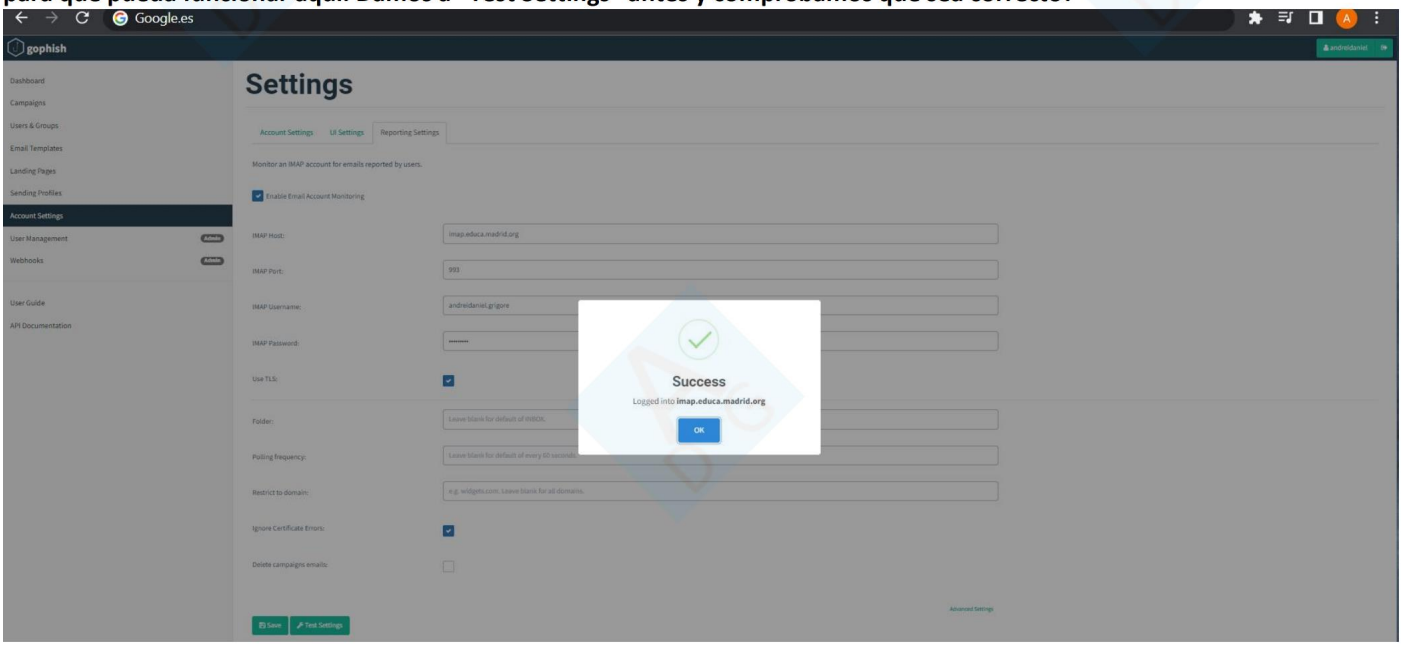
En “Account Settings” tenemos API Key por si quisiéramos implementarla en algún sitio para que se relacione con el GoPhish.



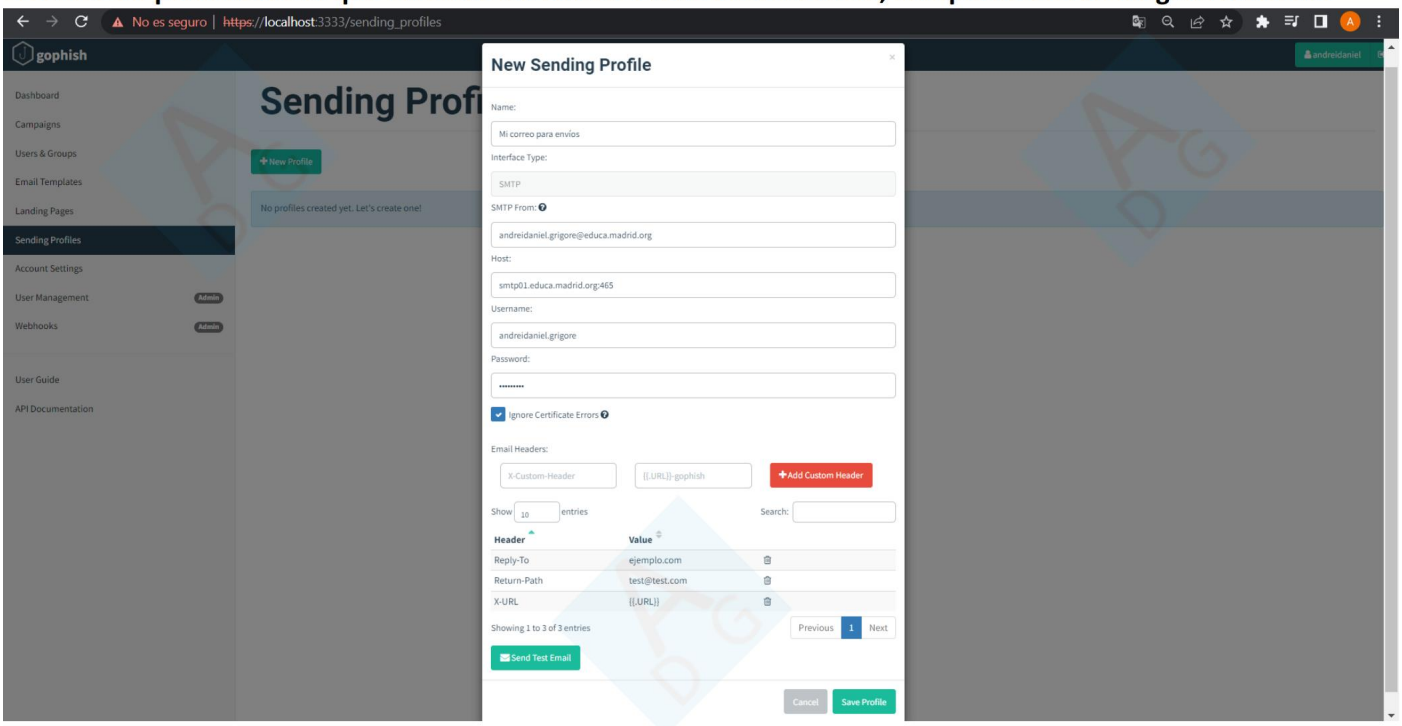
Dejaré activado en “UI Settings” la opción “Show campaign results map, para que muestre al final un mapa según región de quiénes accedieron, de qué país, zona…

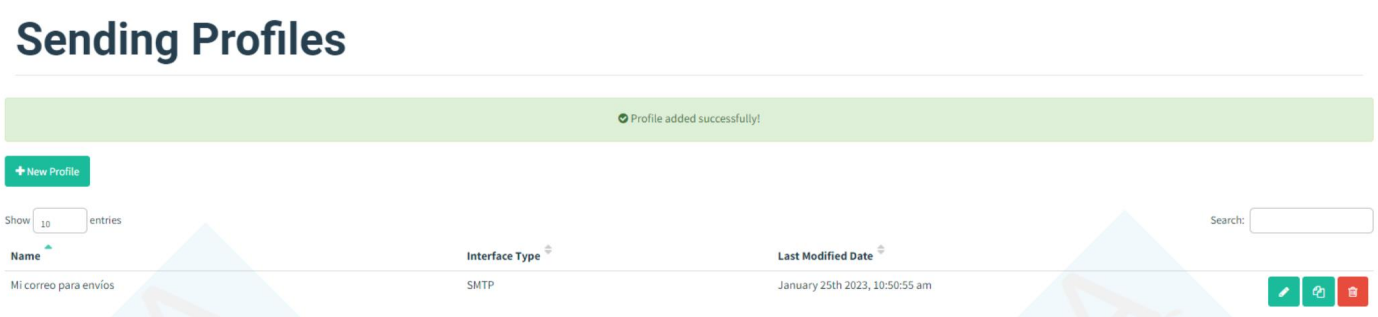


En “Reporting Settings” podemos establecer una cuenta de correo IMAP para recibir allí una notificación de quiénes y cuándo reportaron el email que uso para hacer la campaña al servidor de correo. Usamos TLS e Ignoramos errores de certificados para que pueda funcionar aquí. Damos a “Test Settings” antes y comprobamos que sea correcto:

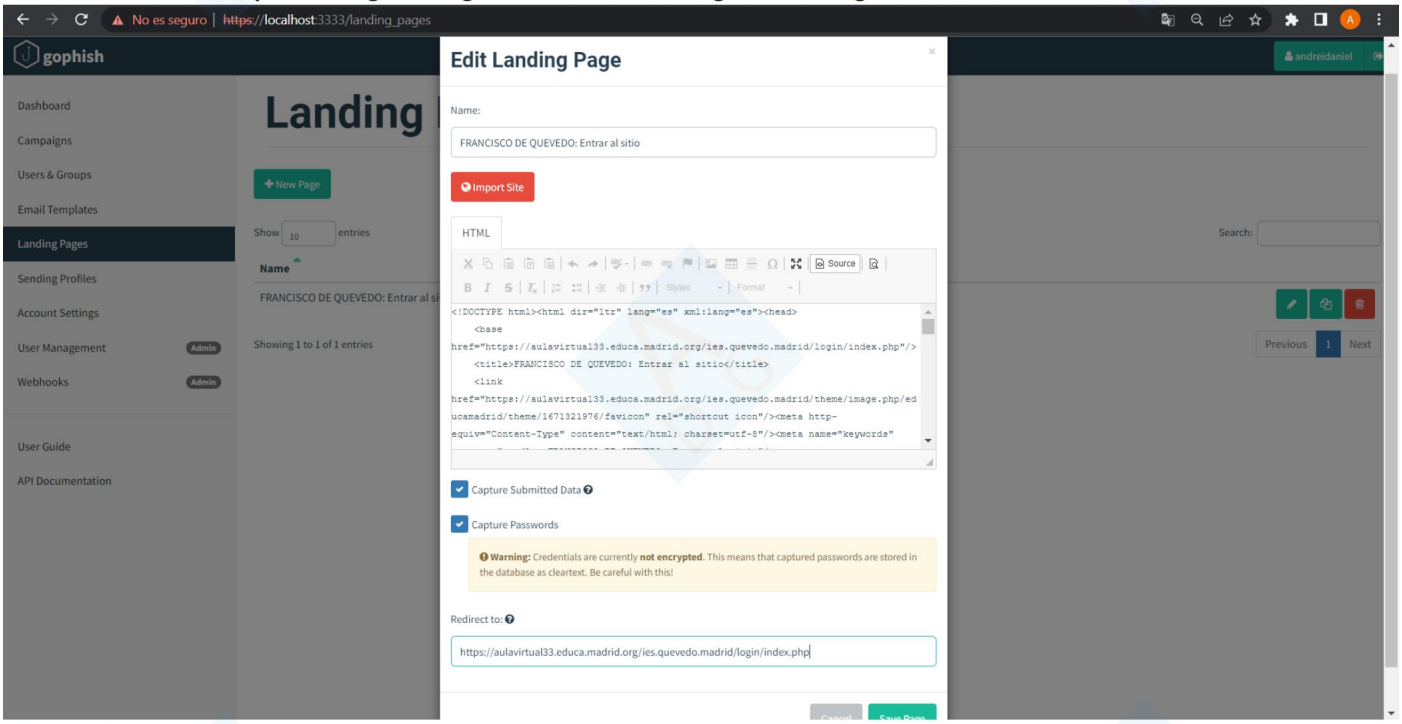


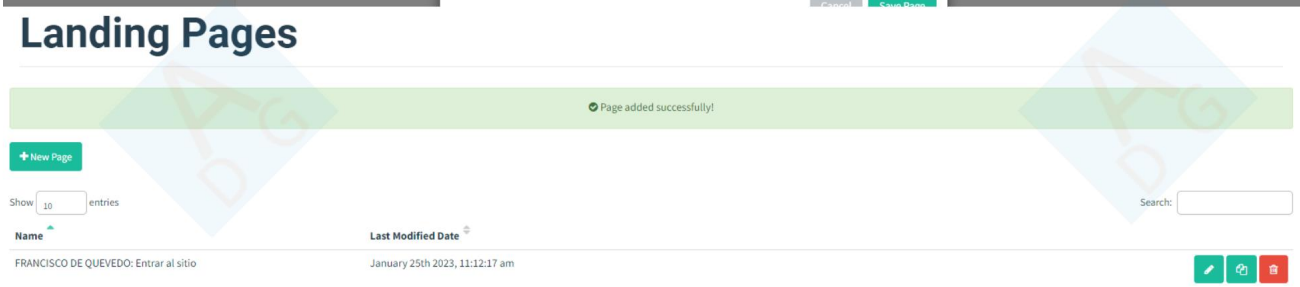
Creamos un perfil desde el que haremos los envíos. Probé unos Headers, aunque no dieron ningún resultado:



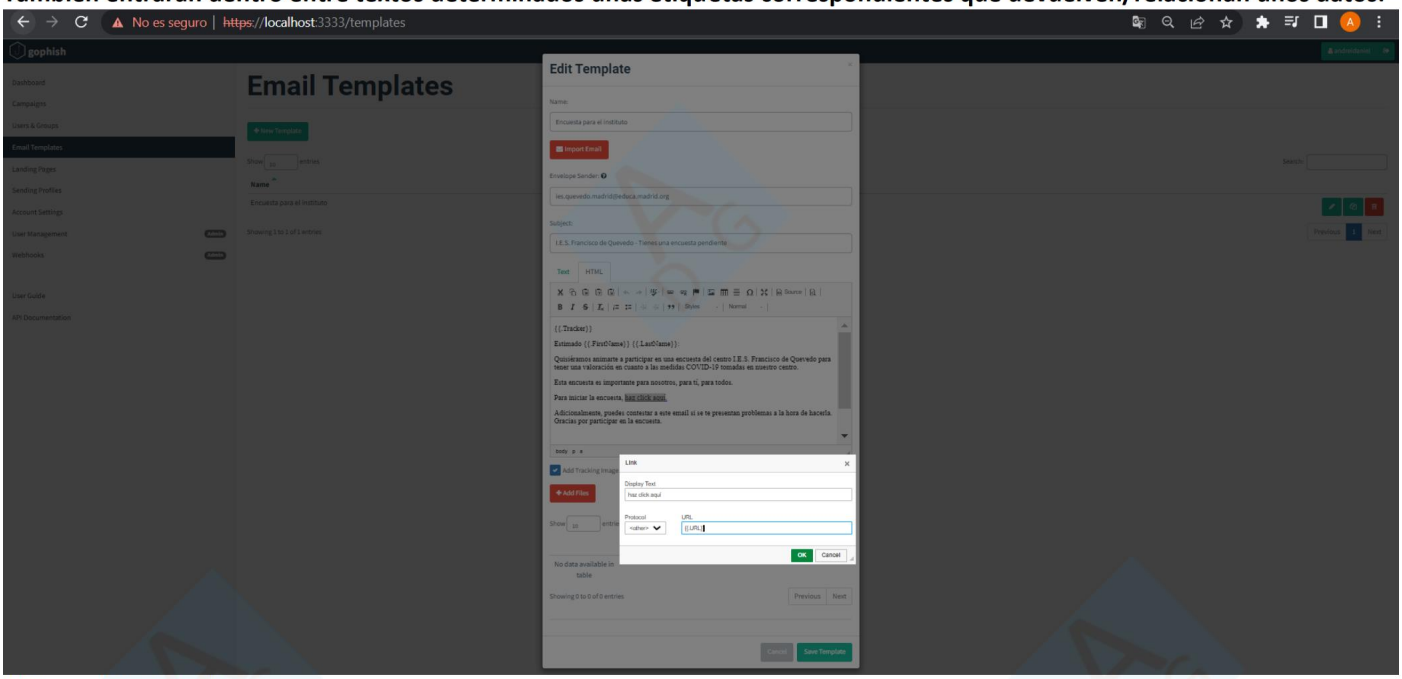


Ahora toca poner la página que les aparecerá cuando entren en el enlace del email. Se accede a "Landing Pages", se da a "New Page" y luego se dará a "Import Site" especificando la URL de la que se quiere copiar el HTML para imitarla. También pondré el mismo nombre que aparece en la original. Capturamos que diga si se introdujo datos y también ver contraseña y le redireccionaremos después de ingresar algún dato en la Land Page al sitio original del aula virtual de Educa Madrid de FdQ:





Se accede a "Email Templates", se selecciona HTML y se ingresa un texto para hacerle creer al receptor que es cierto el email. También entrarán dentro entre textos determinados unas etiquetas correspondientes que devuelven/relacionan unos datos:



{{.Rid}}	The target's unique ID
{{.FirstName}}	The target's first name
{{.LastName}}	The target's last name
{{.Position}}	The target's position
{{.Email}}	The target's email address
{{.From}}	The spoofed sender
{{.TrackingURL}}	The URL to the tracking handler
{{.Tracker}}	An alias for
{{.URL}}	The phishing URL
{{.BaseURL}}	The base URL with the path and rid parameter stripped. Useful for making links to static files

Email Templates

Template added successfully!

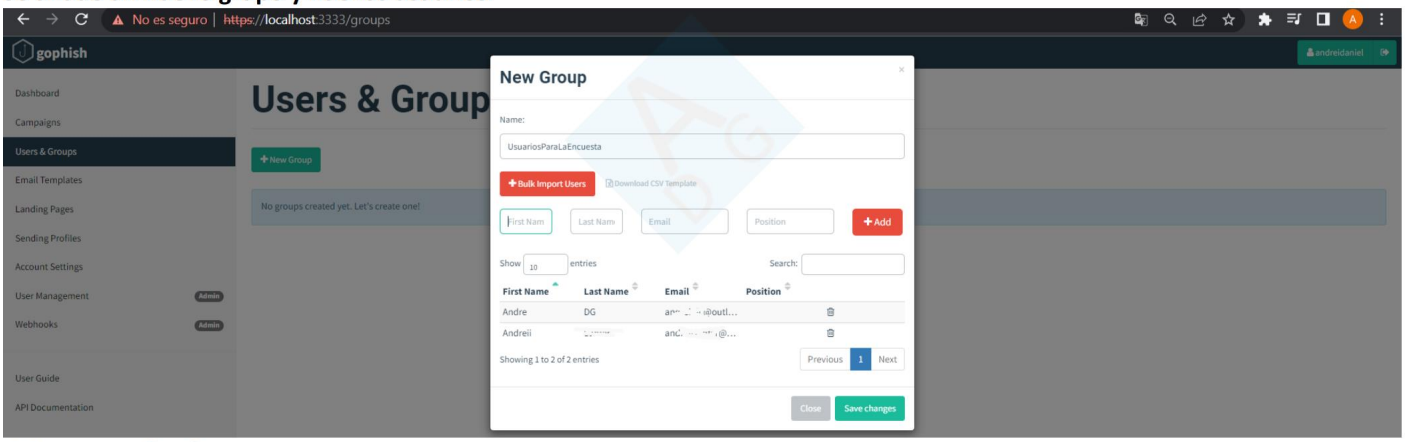
+ New Template

Show 10 entries

Search:

Name	Modified Date
Encuesta para el instituto	January 26th 2023, 10:39:48 am

Se añade un nuevo grupo y nuevos usuarios:



Users & Groups

Group added successfully!

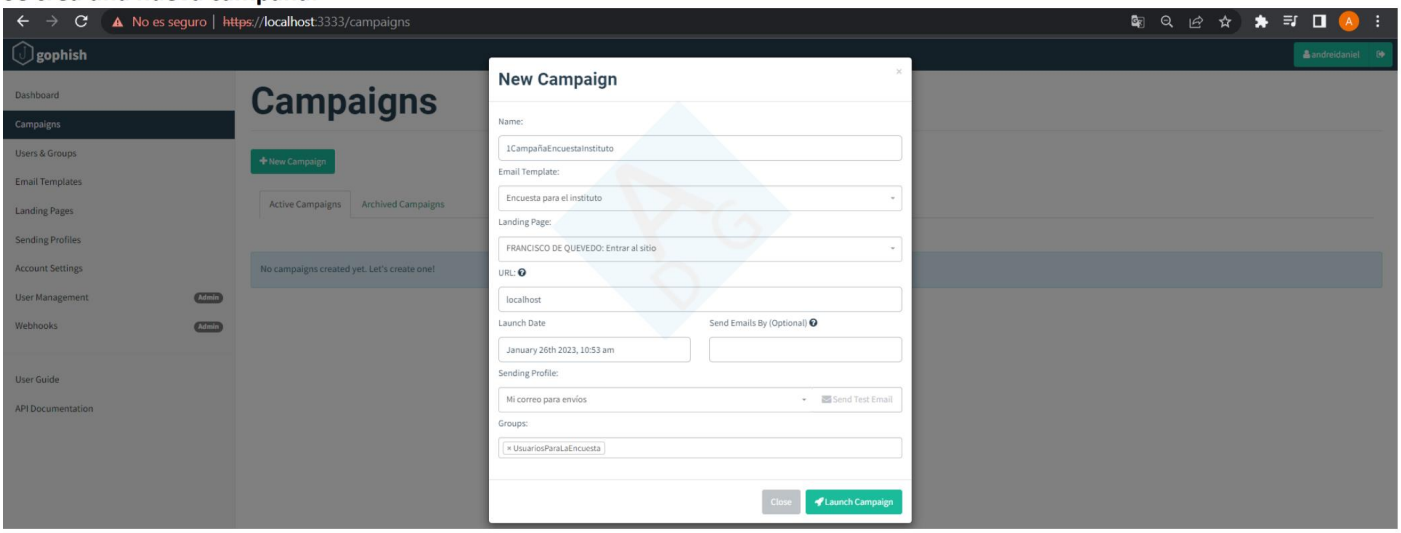
+ New Group

Show 10 entries

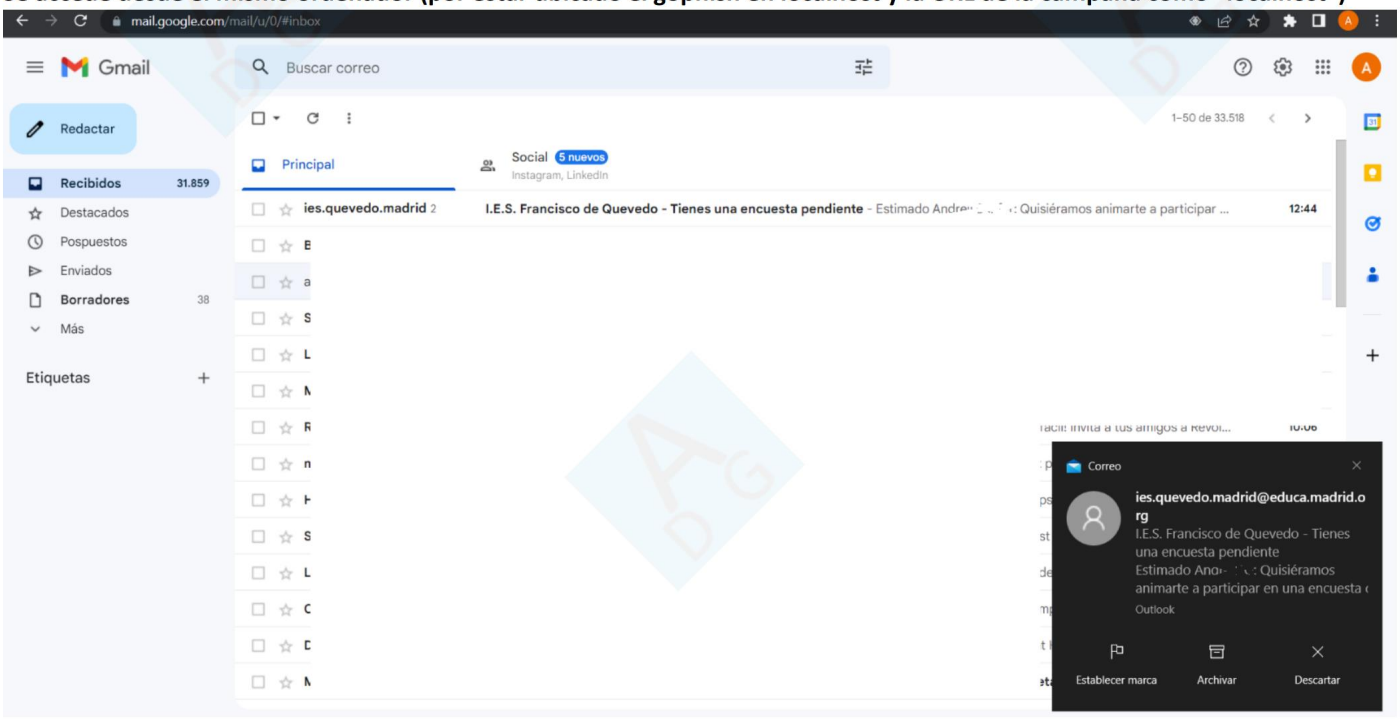
Search:

Name	# of Members	Modified Date
UsuariosParaLaEncuesta	2	January 26th 2023, 10:44:29 am

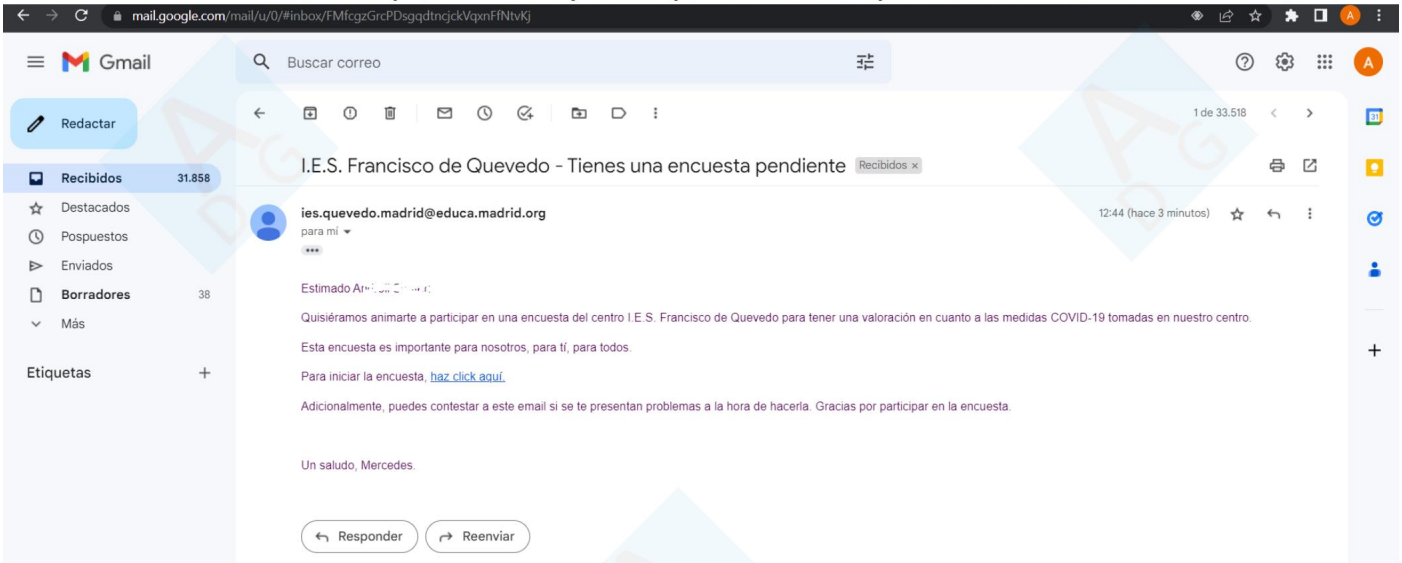
Se crea una nueva campaña:



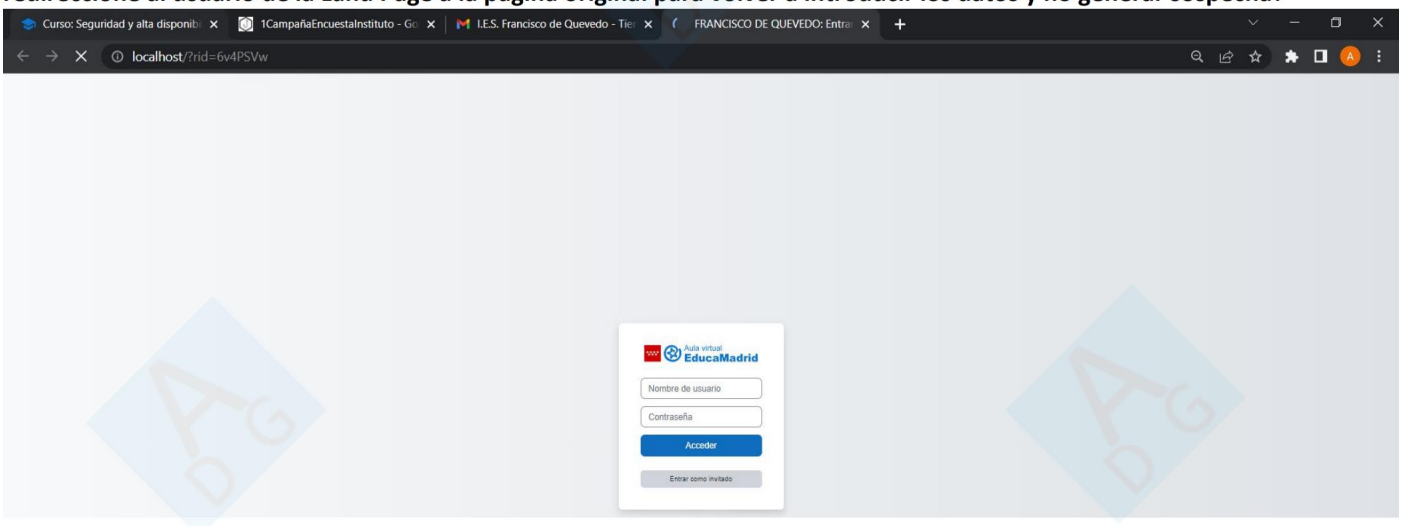
Se accede desde el mismo ordenador (por estar ubicado el gophish en localhost y la URL de la campaña como "localhost")



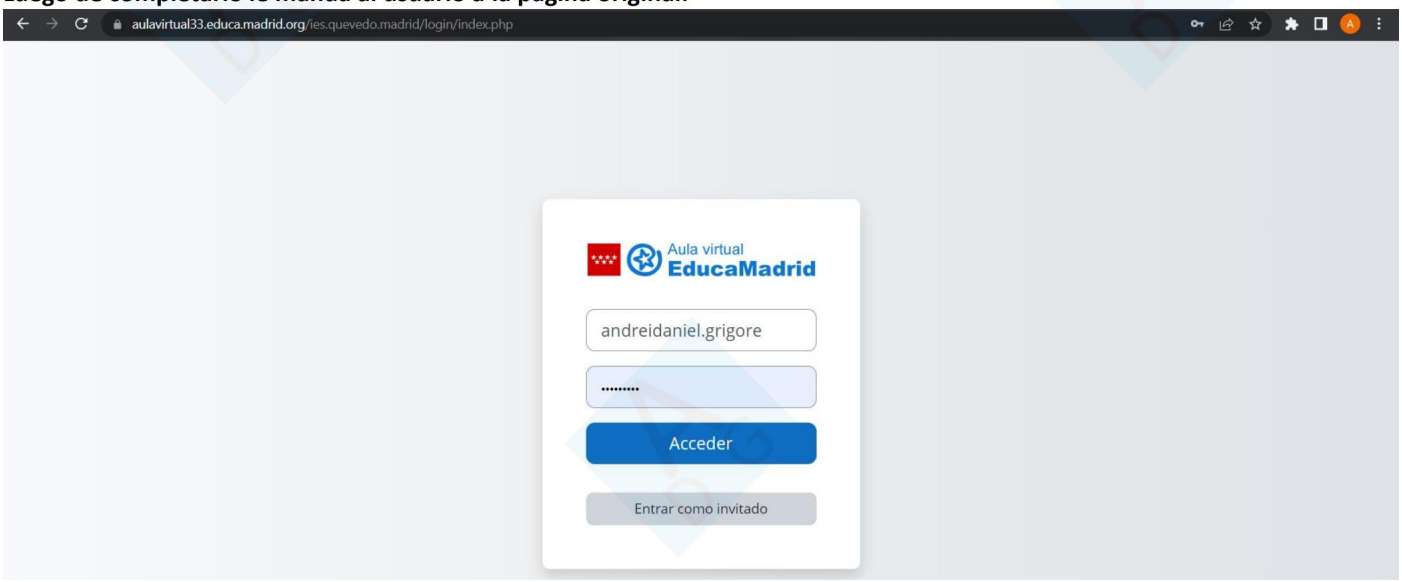
Entramos en el correo Gmail de mi primera cuenta y vemos que los datos nos aparece bien. Probamos acceder al enlace:



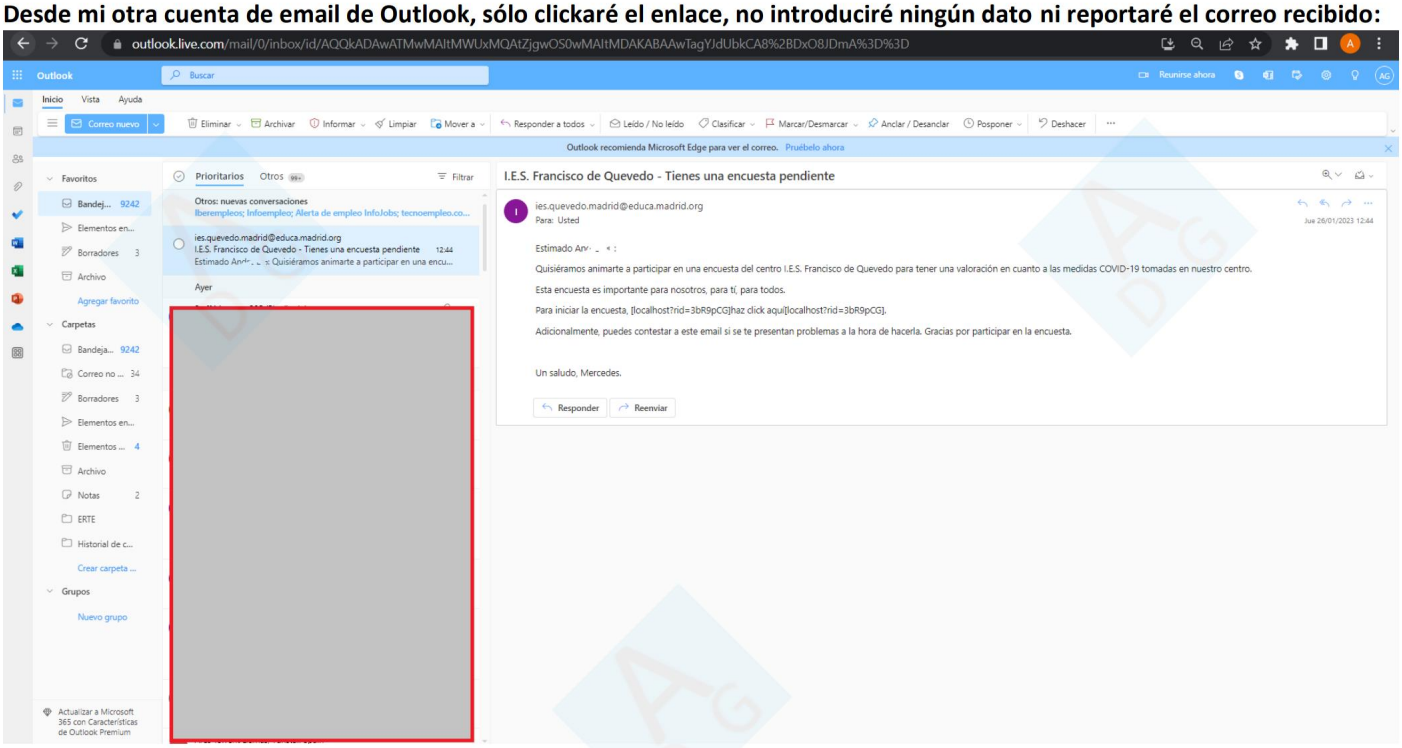
Nos mandará a esa URL y aparecerá la Land Page. Se espera que al introducir los datos, se envíen al GoPhish y luego le redireccione al usuario de la Land Page a la página original para volver a introducir los datos y no generar sospecha:



Luego de completarlo le manda al usuario a la página original:

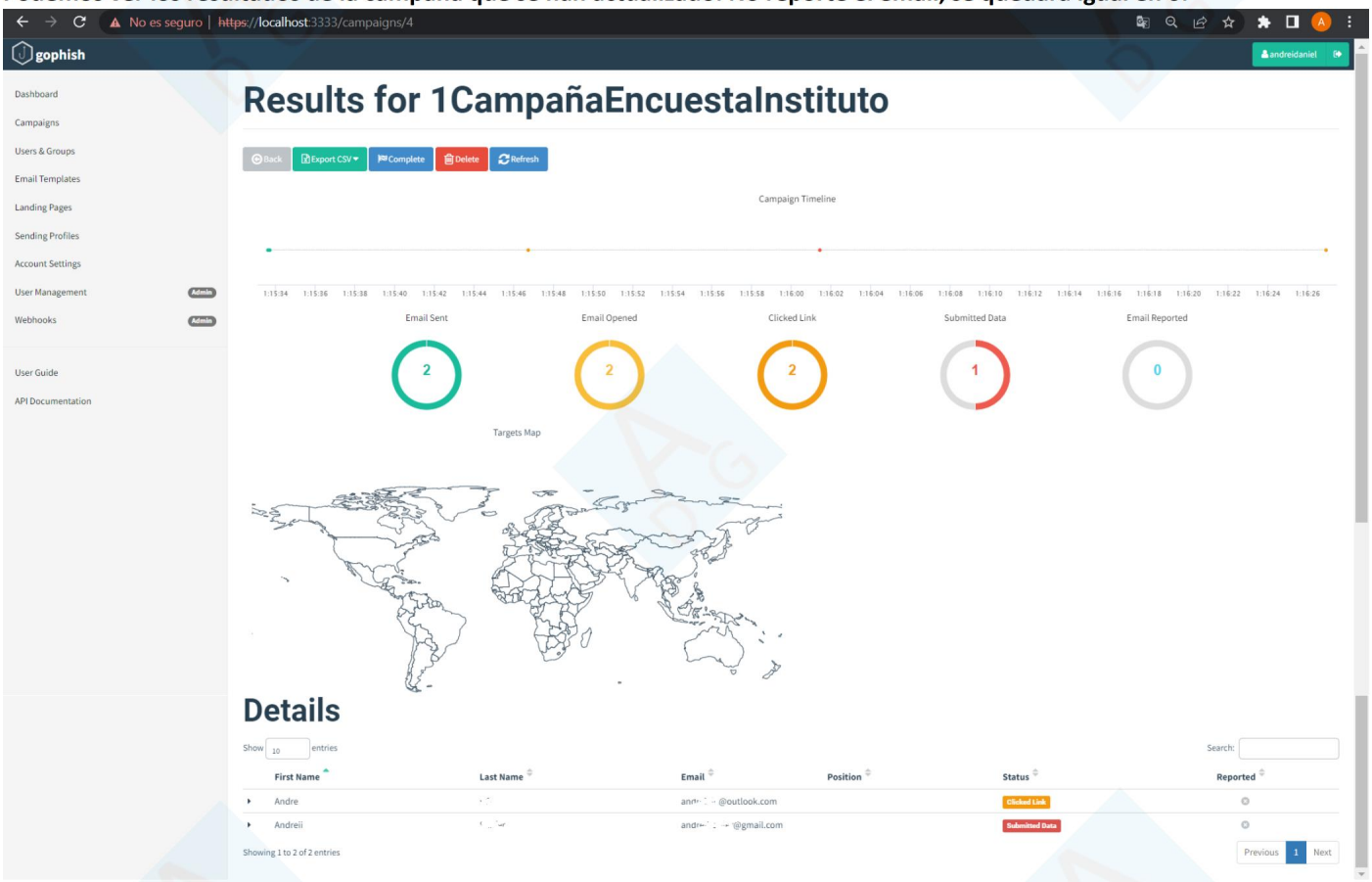


Desde mi otra cuenta de email de Outlook, sólo clickaré el enlace, no introduciré ningún dato ni reportaré el correo recibido:

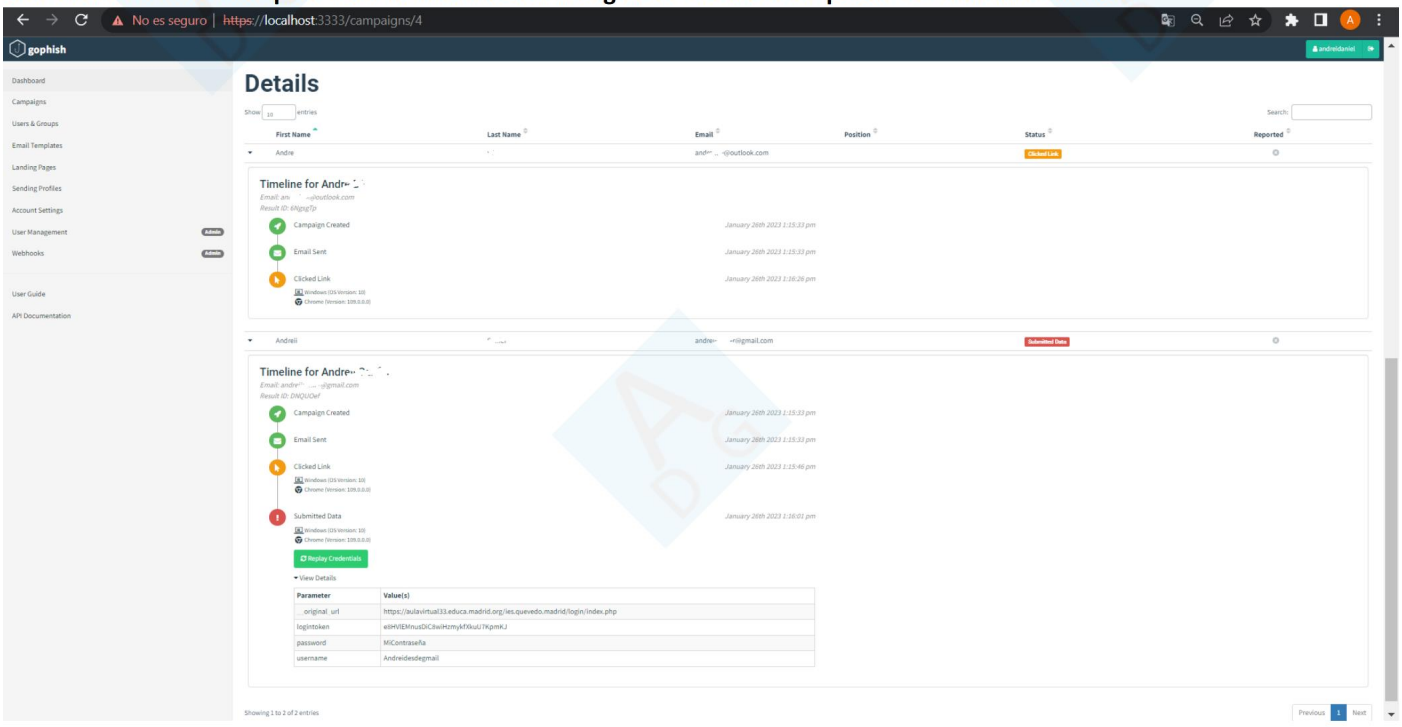


OBSERVACIÓN: Podemos observar que en Outlook el enlace no lo devuelve bien, en cambio en el Gmail sí. Lo copiaré a mano para que se muestre que alguien entró en él pero no completó nada… aunque lo suyo sería que venga en el enlace obvio:

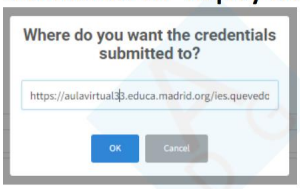
Podemos ver los resultados de la campaña que se han actualizado. No reporté el email, se quedará igual en 0:



Si se clicka en la flechita para abrir la información recogida de cada uno se puede ver más información:



Si clickamos en "Replay Credentials" escribirá los datos introducidos en la página web original:



Y obviamente el resultado será: Acceso inválido. Por favor, inténtelo otra vez. 😄

Si fuese el usuario y contraseña correctos entraría ya sea usando el *logintoken* ó si uno prefiere introducirlo a mano…