https://doi.org/10.22201/dgtic.ctud.2023.1.1.18

Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 94 - 103

Integración de una aplicación PHP con el servicio de Identidad Digital Universitaria

Hugo Germán Cuéllar Martínez

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

hugo.cuellar@comunidad.unam.mx

ORCID: 0009-0005-1346-276X

Información del reporte:

Para citar este reporte técnico:

Cuéllar Martínez, H. C. (2023). *Integración de una aplicación PHP con el servicio de Identidad Digital Universitaria*. Cuadernos Técnicos Universitarios de la DGTIC, *1* (1), páginas (94 - 103). https://doi.org/10.22201/dgtic.ctud.2023.1.1.18

Resumen:

Se presenta el procedimiento técnico para realizar la interconexión entre una aplicación *PHP* y el servicio de Identidad Digital Universitaria (*IDU*), el cual ofrece un registro de identidad biunívoca para alumnos y trabajadores universitarios.

Palabras clave:

OAuth, Laravel, interconexión entre sistemas.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 95 - 103

1. INTRODUCCIÓN

Muchos servicios *TIC* universitarios cuentan con sus propios procesos para la identificación de personas, lo que origina que un usuario tenga muchos datos para iniciar sesión en los diversos sistemas que ofrece la UNAM. En contraste, el servicio de *IDU* toma como identidad digital la información que reconoce de manera unívoca a una persona como miembro de la UNAM, a partir de datos como la *CURP* y el *RFC*, con lo que se busca homologar los criterios para el control de acceso y la identificación de los usuarios.

Este reporte detalla el procedimiento técnico para realizar la comunicación entre un sistema desarrollado en el lenguaje de programación *PHP* y el marco de trabajo *Laravel*, a fin de integrarlo al uso del servicio de Identidad Digital Universitaria (*IDU*).

Este procedimiento técnico fue aplicado para la interconexión del sistema denominado "Sistema de seguimiento del proceso de titulación universitaria", el cual permite que en las entidades académicas se genere el expediente de titulación del alumno, quien puede consultar el avance del proceso de titulación desde el envío de su solicitud hasta el inicio del proceso de emisión del título.

El sistema propuesto cumple con la característica de ser un sistema institucional que maneja entre sus usuarios, a los alumnos de las entidades académicas, así como a trabajadores de las áreas de servicios escolares que dan seguimiento a cada trámite. Partiendo de este universo definido, en este reporte se describen los pasos y las rutas necesarias para la obtención de los datos de cada usuario, alumno o trabajador.

2. OBJETIVO

Documentar el procedimiento necesario para replicar la incorporación del servicio de Identidad Digital Universitaria (*IDU*) al Sistema de seguimiento del proceso de titulación universitaria a fin de contribuir con el manejo y protección de los datos del usuario, obteniendo solamente los datos necesarios para el uso del sistema.

3. DESARROLLO

3.1 ANTECEDENTES

El servicio de Identidad Digital Universitaria (*IDU*) permite que cada miembro de la comunidad universitaria cuente con una identidad digital única, con la visión de evitar el manejo de múltiples cuentas de usuarios y de contraseñas por cada servicio TIC ofrecido en la Universidad Nacional Autónoma de México (UNAM). Promueve además un manejo adecuado de la información, al prevenir su duplicidad y/o pérdida.

En su origen, el servicio *IDU* fue desarrollado en su primera etapa con el lenguaje de programación Java, con un diseño y componentes complejos, lo que hacía difícil su actualización y ponía en riesgo la posibilidad de mantener altos estándares de seguridad. Posteriormente, el área a cargo de *IDU* implementó una herramienta capaz de administrar las identidades y los accesos a los usuarios de la comunidad universitaria a través de los diferentes servicios *TIC*, dando como resultado el surgimiento del actual servicio *IDU*.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 96 - 103

3.2 PROBLEMAS POR RESOLVER

Identificar e integrar el flujo de autorización y autenticación del servicio *IDU* al *Sistema de seguimiento del proceso de titulación universitaria*, implementado en el lenguaje de programación *PHP* y el marco de trabajo (*framework*) de *Laravel*. Adicionalmente, documentar las referencias del proceso de interconexión para su uso en futuras intercomunicaciones con otros sistemas universitarios.

3.3 *OAUTH*

La interconexión de *IDU* con el *Sistema de seguimiento de titulación universitaria*, se realiza mediante el protocolo denominado *OAuth*, cuya versión más reciente y estable es la 2.0 (*OAuth 2.0*, 2012). Este protocolo permite la autorización segura de forma estándar, lo que garantiza que el usuario comparta su información con otra aplicación sin revelar toda su identidad.

OAuth funciona mediante el intercambio de un token que genera el proveedor y este es enviado al cliente, que en este caso es el *Sistema de seguimiento de titulación universitaria*. Este *token* está integrado por una cadena de caracteres que identifican al usuario, al cliente y a la duración del acceso.

Entre las ventajas de utilizar *OAuth* se encuentran:

- Evitar que el usuario comparta sus credenciales con aplicaciones o sitios web de terceros, lo que reduce el riesgo de robo o filtración.
- Permite definir el nivel de información; es decir, determinar los datos que se van a compartir, así como la duración del acceso, lo que reduce el riesgo de abuso o mal uso de la información del usuario.
- Es un protocolo muy utilizado por grandes compañías como son *Google*, *Facebook*, *Microsoft*, *GitHub* entre otros, ya que permite compartir información de sus cuentas con otras aplicaciones.

3.4 INTEGRACIÓN DE IDU CON EL SISTEMA DE SEGUIMIENTO DE TITULACIÓN UNIVERSITARIA

Una vez revisado el funcionamiento del protocolo *OAuth*, a continuación se detalla cómo se implementó la intercomunicación de *IDU* con el sistema de seguimiento.

Antes de empezar a integrar el proceso de autenticación y autorización de *IDU* al *Sistema de seguimiento de titulación universitaria*, es importante solicitar el servicio al área responsable, que requiere la siguiente información:

- **Nombre del cliente:** Corresponde al nombre de la aplicación.
- ***URL*[1] de redirección:** Se trata de la dirección electrónica (*URL*) a la que el servidor de autorización regresará la información cuando se realice el inicio de sesión.
- **URL de redirección de cierre de sesión:** Es la dirección electrónica (*URL*) a la que el servidor de autorización regresará la información al cierre de la sesión.
- ***Scopes:*** Especifica los grupos de parámetros a los que la aplicación solicitará el acceso, entre otros: nombre, *CURP*, correo electrónico.

[1] *URL* es el acrónimo que significa Localizador Uniforme de Recursos por sus siglas en inglés. Una *URL* es una secuencia de caracteres que identifica y localiza un recurso en Internet.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 97 - 103

- **Consentimiento:** Define si se muestra o no la página de consentimiento de *IDU* al usuario, en el que pueda ver e indicar explícitamente los datos que compartirá con el sistema.
- **Descripción:** Se refiere a la información adicional que se quiera mostrar referente a la aplicación.

Con estos datos el servicio *IDU* identificará a la aplicación, así como el *URL* para recibir y enviar los datos que sean solicitados.

Una vez concluído el registro de la aplicación al servicio *IDU* es importante resguardar la información enviada, ya que incluye los datos para realizar la autenticación, su autorización y consulta, como sigue:

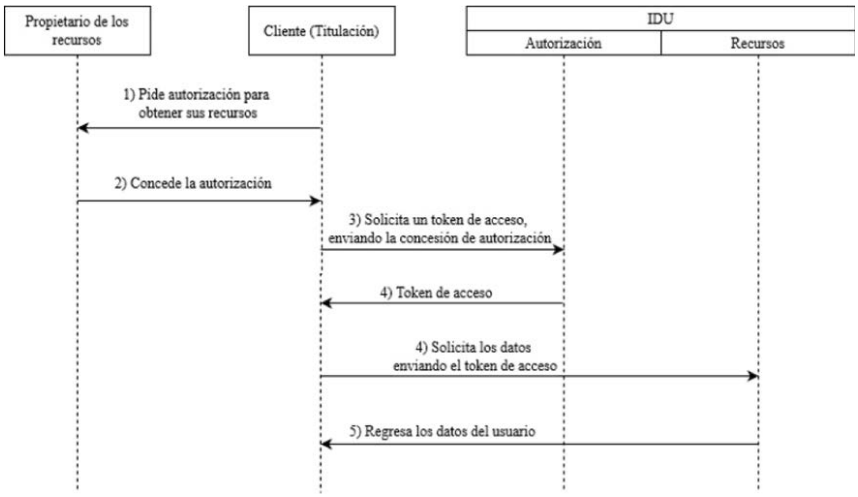
- ***Issuer:*** Es la dirección electrónica (*URL*) donde está el servidor *IDU* (https://idu.unam.mx/sso/oauth2/unam).
- **ID del cliente:** Corresponde al identificador único de la aplicación registrada en *IDU*.
- **Clave del cliente:** Es una cadena secreta (similar a una contraseña) que solamente es conocida por la aplicación y el servidor *IDU*.

IDU cuenta con tres procesos o servicios para obtener la información:

- El primer servicio consiste en solicitar una autorización al usuario, donde explícitamente se le informa qué datos se van a compartir (*scopes*); el usuario debe dar su consentimiento, el cual puede ser requerido por una única ocasión al ingresar la primera vez al *Sistema de seguimiento de titulación universitaria*, y la respuesta es almacenada dentro de *IDU* para próximas conexiones. Si este consentimiento es aceptado, se recibirá una concesión de autorización (*autorization grant*).
- El segundo servicio implica la obtención de un *token* de acceso (*access token*); para solicitar este *token* es necesario enviar la concesión de autorización previamente solicitada, lo que demuestra que es un cliente válido y que el usuario decidió compartir su información. Si todo lo anterior se cumple, el servicio emite el *token* de acceso (*access token*), y se considera que la autorización ha sido completada.
- El tercer servicio se refiere a recibir los recursos, es decir, a obtener los datos de la persona, para eso se necesita enviar el *token* de acceso que fue proporcionado en el servicio anterior; *IDU* se encargará de verificar y validar el token, y devolverá la información de la persona.

Figura 1

Diagrama donde se muestra la interacción del sistema de titulación con IDU



Nota. Se muestran los procesos para obtener la información del usuario descrita anteriormente.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 98 - 103

Una vez revisado el flujo para la obtención de datos, se trabajó en la integración con *Laravel* para lograr la comunicación entre ambos sistemas.

En un primer paso se revisó *Guzzle* (2021), la librería que provee Laravel para hacer peticiones "http"[2], y se resolvió el envío de los datos solicitados al servicio de *IDU*. El uso correcto de esta librería requiere definir las rutas y cabeceras manualmente, y al no contar con toda esa información se recibían respuestas de error, además de tener que implementar la comunicación con las librerías de autenticación, manejo de usuarios y permisos.

En la búsqueda de otras librerías o componentes que realizaran la conexión, se encontró la librería llamada "*Socialite*" la cual está pensada precisamente para autenticarse con *OAuth* para servicios como *Google*, *GitHub*, *Facebook*, *LinkEdit*, *Slack*, entre otros, permitiendo personalizar el propio conector para un servicio personalizado como lo es *IDU*, e integrándose correctamente a las demás librerías de autenticación y manejo de usuarios que ofrece *Laravel*.

Para solicitar la autorización es necesario realizar una petición *GET*[3] al servidor; se envían como parámetros el identificador del cliente, la URL de redirección, los alcances o permisos (*scopes*) y el tipo de respuesta o tipo de autorización que se requiere que devuelva el servicio *IDU*. Un ejemplo de esta petición sería:

https://idu.unam.mx/sso/oauth2/unam/authorize?client_id=sistema-firma-documentos&redirect_uri=http://localhost:5000/callback&scope=openid+profile+email&response_type=code

Aquí se puede notar que en el parámetro *response_type* tiene como valor la cadena "***code***", el cual indica al servicio *IDU* que queremos que nos devuelva un flujo de Autorización (para obtener recursos y confirmar que se concede dicha autorización). Si todo es correcto se obtiene lo que se muestra en la figura 2.

Figura 2

Pantalla de autenticación IDU

Nota: Adaptado de Iniciar sesión [Captura de pantalla], por IDU-UNAM, 2023, *IDU* (https://idu.unam.mx/sso/oauth2/unam/authorize?client_id=seguimiento-algo&redirect_uri=https%3A%2F%2Fseguimientotitulacionpre.unam.mx%2Flogin%2Fidu%2Fcontrol&scope=openid+profile+email&response_type=code)

[2] *HTTP* es un protocolo de comunicación que permite las transferencias de información a través de archivos.

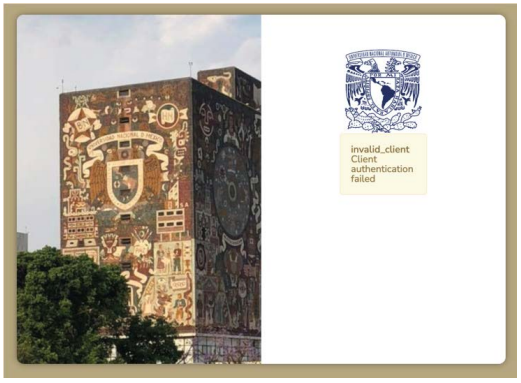
[3] *GET* es un método *HTTP* que se utiliza para solicitar datos al servidor web. El método *GET* envía los datos a través de la *URL*, lo que significa que se pueden ver en la barra de direcciones del navegador.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 99 - 103

Cabe aclarar que todos los parámetros deben estar registrados previamente, si alguno de ellos no se encuentra registrado se obtendría el mensaje de error "*invalid_client Client authentication failed*" que se muestra en la figura 3.

Figura 3

Pantalla de error al enviar un dato diferente a los capturados por IDU



Nota: Adaptado de Iniciar sesión [Captura de pantalla], por IDU-UNAM, 2023, *IDU* (https://idu.unam.mx/sso/oauth2/unam/authorize?client_id=seguimiento-algo&redirect_uri=https%3A%2F%2Fseguimientotitulacionpre.unam.mx%2Flogin%2Fidu%2Falumno&scope=openid+profile+email&response_type=code)

En este punto el usuario captura sus datos de ingreso y si es la primera vez que lo hace, el servicio *IDU* notificará al usuario la información que quiere ver, permitiendo que acepte o deniegue el acceso a su información, como se muestra en la figura 4.

Figura 4

Pantalla donde se muestra la autorización y concesión de los datos.

Nota: Adaptado de Iniciar sesión [Captura de pantalla], por IDU-UNAM, 2023, *IDU* (https://idu.unam.mx/sso/oauth2/unam/authorize?client_id=seguimiento-algo&redirect_uri=https%3A%2F%2Fseguimientotitulacionpre.unam.mx%2Flogin%2Fidu%2Falumno&scope=openid+profile+email&response_type=code)

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 100 - 103

Si el usuario previamente lo ha aprobado, se podría omitir este paso y enviar directamente la concesión a la *URL* dada para la redirección y un parámetro llamado "*code*". Un ejemplo del resultado es el siguiente:

http://localhost:5000/callback?code=MSEzR6ErbpglHhZJuTE25fNk6ho&iss=http//idu.unam.mx:8081/sso/oauth2/unam&client_id=sistema-firma-documentos

Para este punto ya se ha logrado la primera parte del flujo del protocolo para la concesión de autorización, ahora se solicita el token de acceso (access token) lo que demuestra que es un cliente válido y que se puede obtener la información a la que el usuario dio acceso.

Para obtener este token de acceso se realiza una petición POST[4] al servidor con los siguientes datos:

URL: https://idu.unam.mx/sso/oauth2/unam/access_token

Cabeceras (headers):

Content-Type: application/x-www-form-URLencoded

Authorization: Basic c2lzdGVtYS1hY3Rhcy10aXR1...

Cuerpo (body):

grant_type: authorization_code

code:MSEzR6ErbpglHhZJuTE25fNk6ho

redirect_uri: http://localhost:5000/callback

Donde:

content-type: define que se están enviando los datos desde un formulario.

Autorization: es el tipo de autorización que define el servidor, en este caso está compuesta de la palabra "*Basic*" seguido de una cadena *base64* donde incluye el identificador del cliente, dos puntos y la contraseña del cliente "i*d_cliente:client_secret*".

Grant_type: cadena de texto "*autorization_code*" que especifica el avance en el flujo de autorización.

Code: código que se recibe de la petición anterior, que solo se puede utilizar una vez para obtener el *token*.

Redirect_uri: esta es la *URL* donde se va a enviar la información, que debe coincidir con la que se envió en el proceso de autorización.

Ejemplo:

https://idu.unam.mx/sso/oauth2/unam/access_token

Cabeceras:

Authorization: Basic c2lzdGVtYS1hY3Rhcy10aXR1...

Content-Type: application/x-www-form-urlencoded

[4] *POST* es un método que utiliza HTTP para enviar datos: los transmite en el cuerpo de la petición.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 101 - 103

Cuerpo:

grant_type:authorization_code

code:MSEzR6ErbpglHhZJuTE25fNk6ho

redirect_uri:http://localhost:5000/callback

Lo anterior debería devolver como resultado un objeto json[5] como se muestra en la figura 5, con la información del token de acceso, los permisos (*scopes*) del *token*, el tipo de *token* y el tiempo de validez del *token* (*expires_in*).

Figura 5

Respuesta recibida al solicitar el token de acceso (access token)


```
{
    "access_token": "jq_bzfsyE8iVnlyq7DyB6ajHz7c",
    "scope": "openid profile email",
    "id_token": "eyJ0eXAiOiJKV1QiLCJraWQiOiJ3VTNpZklJYUxPVUFSZVJC
        eyJhdF9oYXNoIjoiYTliNXZmTXRXRVVja18yZEpXMGxvdyIsInN1YiI6I
        ZmZGZiOWRhYjkzLTc2NDU4Iiwic3VibmFtZSI6IjY4YzRkNWVhLTM5NjY
        c2lkIjoieEJwZWdUZW5ZZDVpMnVPR3FMYkRUZTAwNHFxcTJLNmI4dFNOT
        JvY2sub3BlbmlkY29ubmVjdC5vcHMiOiJFT0hLMmQ4UWZMSDEtMml5SFZ
        NDEsInRva2VuVHlwZSI6IkpXVFRva2VuIiwiaWF0IjoxNjY3NTg5NDQxf
        SqUXBqBlizatn_UZWtYFrPFBuFLx1rO0ljIkiya0yklL9-LLBxrFh9bSR
        VRWiUFzjsJPdHHMCrgSttR5VjHzzRSX3kDxxcXO4aUkwla0Hf0pz4Tnsm
    "token_type": "Bearer",
    "expires_in": 3599
}
```


Al llegar a este punto se puede considerar que la autorización ha sido completada.

Una vez que se cuenta con la autorización, se pueden solicitar los recursos al servidor, en este caso el recurso será la información del usuario. Para este caso, se realiza una petición *GET* a la dirección https://idu.unam.mx/sso/oauth2/unam/userinfo, para lo que se agrega la siguiente cabecera:

Authorization: Bearer jq_bzfsyE8iVnlyq7DyB6ajHz7c

A esta cabecera de autorización se le agrega el *token* que devolvió el servidor *IDU*, antecediendo la cadena "*Bearer*", lo que devuelve como respuesta la información del usuario en formato json, como se muestra en la figura 6. Se pueden realizar tantas consultas como se necesiten mientras el token esté activo.

[5] *JSON* es una notación de objetos *JavaScript* por sus siglas en inglés, formato que sirve para el intercambio de datos basándose en la sintaxis de los objetos de *JavaScript*.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 102 - 103

Figura 6

Respuesta que se recibe con los datos de la persona

Para terminar la sesión e invalidar el token se tendrán que realizar las siguientes peticiones:

Una petición *POST* a la siguiente dirección:

https://idu.unam.mx/sso/oauth2/unam/token/revoke?token=jq_bzfsyE8iVnlyq7D yB6ajHz7c

Se enviará como parámetro el *token* de acceso (*access_token*) que se recibió cuando fue solicitado (figura 4) y se agrega la cabecera *Autorization* compuesta de la palabra "*Basic*" seguido de una cadena *base64* donde se incluye el identificador del cliente, dos puntos y la contraseña del cliente "*id_client:client_secret*"; esta petición no regresará alguna respuesta. Una vez realizada esta petición se invalidará el *token* y como último paso para terminar la sesión se envía una petición *GET* a la siguiente *URL*:

https://idu.unam.mx/sso/oauth2/unam/connect/endSession?id_token_hint=eyJ0eXAiOiJKV1Qi...&client_id=sistema-firma documentos&post_logout_redirect_uri=http://localhost:5000/end

Siendo *id_token_hint:* el identificador del *token* de acceso (*id_token*) que se recibió al inicio (figura 4), el *client_id* que corresponde al *id* del cliente y el *post_logout_redirect* la ruta a la cual se redireccionará después de terminar la sesión.

4. RESULTADOS

Se realizó la integración del servicio *IDU* con el Sistema de seguimiento de titulación universitaria por medio de dos librerías. La primera, llamada "*Guzzle*", se recomienda para proyectos que no tengan algún marco de trabajo, ya que facilita el uso de las peticiones HTTP hacia *IDU*.

La segunda librería se llama "*Socialite*" y se integra con el marco de trabajo *Laravel*, lo que facilita el manejo de sesiones y de usuarios, propios de dicho marco de trabajo.

Se generó un manual de interoperabilidad revisado junto con la Coordinación de Servicios de Identidad y de Firma Electrónica Universitaria de la DGTIC, donde se detalla la implementación.

Adicionalmente, dado que el sistema de seguimiento ya tenía un módulo para registro de usuarios, asignación de permisos y autenticación, éste fue adaptado para recibir los datos de *IDU*, para ello se eliminaron datos como el nombre de usuario y contraseña, y se agregó el campo RFC que sirve como punto de conexión entre ambos sistemas.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.18 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 103 - 103

Para el caso de los alumnos, al no contar con su información académica se implementó otra conexión al servicio web de la Dirección General de Administración Escolar para traer su trayectoria académica y verificar el cumplimiento de los requisitos para iniciar su trámite

5. CONCLUSIONES

El servicio *IDU* permite que un usuario proporcione su información con otras aplicaciones sin revelar toda su identidad, lo que mejora la privacidad y la seguridad de los usuarios al no tener que compartir sus credenciales con las aplicaciones, y se permite el acceso delegado y restringido a sus recursos, para controlar qué acciones puede realizar la aplicación en su nombre y poder revocar el acceso en cualquier momento.

IDU facilita la integración y la interoperabilidad entre las aplicaciones y servicios reduciendo la complejidad y el mantenimiento del sistema, y se encarga de la gestión de la información de los usuarios, la emisión de los tokens de acceso y la comunicación entre los componentes.

- Algunas de las áreas de oportunidad a considerar son:
- La implementación cuidadosa y un seguimiento de las buenas prácticas para evitar vulnerabilidades o ataques de seguridad, como el robo o la suplantación de tokens, la suplantación de identidad (*phishing*) o la falsificación de solicitud entre sitios *CSRF* (*cross-site request forgery*).
- La evaluación del nivel de dependencia de los servidores de autorización y recursos, que pueden tener fallos, retrasos o cambios en sus políticas o especificaciones lo que puede provocar que no puedan ingresar a los sistemas.
- El diseño de la interfaz de usuario para evitar que se genere confusión o desconfianza al mostrarle la información que se compartirá con la aplicación.

Al elaborar esta memoria técnica se busca dejar un antecedente para que las áreas universitarias que requieran información para obtener la autenticación y obtención de datos de *IDU* lo puedan desarrollar de manera sencilla.

6. AGRADECIMIENTOS

Se reconoce y agradece la colaboración recibida del personal de la Coordinación de Servicios de Identidad y de la Firma Electrónica Universitaria y del equipo de aseguramiento de la calidad de la Dirección de Colaboración y Vinculación, ambas áreas pertenecientes a la DGTIC.

REFERENCIAS BIBLIOGRÁFICAS

Guzzle. (2021). *Guzzle Documentation*. Recuperado el 22 de septiembre de 2023, de https://docs.guzzlephp.org/en/stable/index.html

OAuth 2.0 — OAuth. (2012). *Oauth.net*. Recuperado el 12 de septiembre de 2023, de https://oauth.net/2/