Verificación en dos pasos en el proceso enseñanza/aprendizaje
Two-step verification in the teaching / learning process

Angélica González Arrieta, Daniel López Sánchez, Ángel Luis Sánchez Lázaro, María Belén Pérez Lancho, José Rafael García-Bermejo-Ginner, Juan Andrés Hernández Simón, Pastora Isabel Vega Cruz
email angelica@usal.es, email lope@usal.es, email alsl@usal.es, email lancho@usal.es, email coti@usal.es, email jahsimon@usal.es, email pvega@usal.es

Informática y Automática
Universidad de Salamanca
Salamanca, España

Resumen- Al igual que en otros sectores, en el proceso de enseñanza/aprendizaje existe la necesidad de mantener protegida las cuentas de usuario y el acceso a diferentes servicios de la comunidad universitaria: correo electrónico, repositorios en la nube como Drive o Dropbox dónde el profesor almacena el material de trabajo y exámenes y los alumnos sus trabajos, listado de todos los alumnos, las plataforma de formación, servicio de grabar el resultado de las evaluaciones, datos personales del trabajador y estudiante en el centro educativo, etc. La forma de conseguir esa seguridad en los servicios on-line es identificando o validando la identidad del usuario a través de diferentes métodos. Actualmente no es suficiente un único método y se recurre al uso de un segundo factor de autenticación, bien sea en formato software o hardware. Presentamos el estudio realizado en la Universidad de Salamanca y planteamos diferentes propuestas de segundo factor de autenticación, analizando ventajas e inconvenientes de cada una de ellas.

Palabras clave: Universal SecondFactorAuthentication (U2F), llaves Fast IDentify Online (FIDO), servicio on-line

Abstract- As in other sectors, in the teaching / learning process there is a need to keep user accounts protected and access to different services of the university community: email, cloud repositories such as Drive or Dropbox where the teacher stores the work material and exams and the students their work, the list of all the students, the training platforms, the service of recording the results of the evaluations, the personal data of the worker and student in the educational center , etc. Security in online services is achieved identifying o validating the user's identity through several methods. Nowadays, a single method is not enough and the use of a second authentication factor, either in software or hardware format. We present the study carried out at the University of Salamanca and propose different proposals for a second authentication factor, analyzing the advantages and disadvantages of each of them.

Keywords: Universal Second Factor Authentication (U2F), Fast IDentify Online (FIDO) keys, on-line service

1. INTRODUCCIÓN

Existen dos tipos de tecnología de autenticación. La de factores universales de autenticación (Universal Authentication Factors o UAF) que utiliza únicamente uno de los tres métodos universales: datos biométricos, dispositivos físicos (mochila) y contraseñas. La segunda se conoce como Universal Second Factor Authentication (U2F) o autenticación en dos pasos. Dado que todos los métodos de autenticación tienen desventajas: las contraseñas se pueden adivinar, las tarjetas inteligentes se pueden robar y la biométrica se puede fingir en determinadas condiciones, si se combinan, como se hace en la U2F, el nivel de seguridad es mayor (Megouache, 2020).

El segundo factor de autenticación es pues un método de validación adicional de datos que, sumado a los métodos habituales (Ding Wang, 2020), permite intensificar los niveles de seguridad; por poner un ejemplo, a nivel bancario es muy frecuente utilizar una tarjeta plástica que tiene en el dorso una matriz de filas y columnas; cada celda contiene pares de datos (números), que le serán solicitados al usuario en el momento de la firma de cualquier operación monetaria. Otro ejemplo es el uso de una clave de un solo uso que es enviada al usuario a través de un canal alternativo como puede ser su teléfono móvil cuyo número formará parte de los datos personales del usuario., que es una aplicación que puede ser instalada en cualquier dispositivo smartphone y que funciona como método de validación de datos, intensificando los niveles de seguridad y evitando el fraude electrónico, permitiendo generar claves de autenticación dinámica para la firma de operaciones.

Para hacer que el proceso de compra/venta por internet sea más seguro se aprobó la directiva Europa PSD2 (Payment Services Directive) (EUR-Lex, 2015) que persigue reforzar la seguridad en las compras online y dificultar los fraudes; normativa que fue aprobada en 2015 y que entró en vigor, en el caso de España, el 1 de enero de 2021. Sin duda, esta seguridad la debemos de incorporar en otros sectores, como la Enseñanza, para mejorar los que hasta ahora mayoritariamente todo el mundo utiliza en exclusiva que son el par usuario-contraseña.

En el proceso de enseñanza-aprendizaje sea presencial u on-line, tanto alumnos como profesores vamos a usar servicios on-line en los que nos tenemos que identificar. Algunos de esos servicios que usa el profesor son: correo electrónico, almacenamiento en la nube, plataformas de formación on-line

DOI: 10.26754/CINAIC.2021.0108

para el apoyo a la enseñanza presencial o para formación on-line, acceso a bibliotecas virtuales, acceso a servidores para almacenar resultados de calificación. En el caso del estudiante: consulta de materiales, expediente, calificaciones, etc. Para el correcto funcionamiento de esos servicios conocer la identidad del actor es clave.

2. CONTEXTO

Para el estudio que presentamos nos hemos centrado en la Universidad de Salamanca. Para la identificación tanto de profesores como estudiantes la universidad tiene el portal de autenticación que le da acceso a los diferentes servicios como el acceso al correo electrónico (Figura 1) o a la plataforma de formación Moodle (Figura 2).

Figura 1 Portal identificación en la Universidad de Salamanca para acceder al correo electrónico.

Figura 2 Portal identificación en la Universidad de Salamanca para acceder a la plataforma Moodle (studium.usal.es).

Como se aprecia en las anteriores figuras, hay dosmétodos de identificación alternativos.

Además, la universidad ofrece a la comunidad universitaria el uso de un Latch o cerrojo: una app para móviles que permite un segundo factor de autenticación basado en un PIN temporal como función de seguridad opcional u obligatoria (*Figura 3*).

Figura 3 Latch de seguridad.

Con esta aplicación añadimos un nivel adicional de protección en el acceso a los servicios digitales. Latch protegerá en el caso de que a un usuario le hayan robado su contraseña. Un ejemplo del beneficio de usar Latch: "Si alguien conociese mi contraseña y tratase de entrar en mis aplicaciones cuando estén bloqueadas, sucederán dos cosas, primero no tendría acceso (no vería mi información, ni accedería a mis recursos, etc.) y segundo me llegará una alerta al móvil, para que pueda tomar las medidas oportunas».

El objetivo principal es concienciar de la necesidad de utilizar otros métodos de autenticación más seguros por considerar que el uso de un identificador y una contraseña no proporciona un nivel de seguridad adecuado. Otro objetivo es hacer un estudio de la utilización de la app que proporciona la Universidad como segundo factor de autenticación. Y por último analizar como alternativa de segundo factor de autenticación las llaves de seguridad y estudiar si el segundo factor de autenticación en la gestión universitaria on-line es viable.

3. DESCRIPCIÓN

En el proceso de enseñanza/aprendizaje accedemos a multitud de servicios on-line que incluyen mucha información personal y de nuestros alumnos. Por eso es muy importante tener la información protegida y en el caso de plataformas de formación on-line solo puede restringirse el acceso a usuarios autorizados si tenemos identificada a la persona que accede. En la actualidad, por los ataques tecnológicos que estamos sufriendo, no basta con contraseña segura y complicada pues hemos visto hackear a servicios y exponer públicamente las contraseñas de sus usuarios. Y afecta aún más cuando utilizamos la misma contraseña para acceder a diferentes servicios.

Una primera barrera, antes de acceder a los servicios on-line es proteger el acceso a nuestros equipos. A modo de ejemplo Windows dispone de diferentes opciones de inicio de sesión (Figura 4). Se aprecia que además del inicio de sesión por reconocimiento de rostro, huella pin y contraseña ofrece la posibilidad de uso de clave de seguridad.

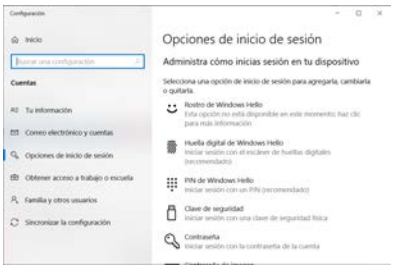


Figura 4 Opciones de inicio de sesión de Windows.

Una *clave de seguridad* es un dispositivo de hardware (Figura 5) que puedes usar en lugar de tu nombre de usuario y contraseña para iniciar sesión en la web. Dado que se usa con una huella digital o un PIN, aunque alguien tenga la clave de seguridad, éste no podrá iniciar sesión sin el PIN o la huella digital que hayas creado.

Figura 5 Llave de seguridad FIDO.

Nunca fue más fácil realizar la verificación en dos pasos que con el método de las llaves físicas de seguridad. De esta manera, se acabó el mirar el móvil o el correo electrónico para pulsar un botón de verificaciones; conectas un USB al ordenador y éste es el que lleva a cabo la verificación. Se asemeja al dispositivo del documento de identidad portable en forma de USB que se puede conectar al ordenador.

La llave de seguridad es una verificación en dos pasos estándar, son dispositivos hardware que funcionan a través de U2F. La principal diferencia de la verificación tradicional es que, en ésta, es necesario un dispositivo hardware que desempeñará la función de llave, en vez de recibir un código. Sin este dispositivo, no podríamos acceder a una cuenta de usuario.

La forma en la que están hechas estas llaves es igual a la forma tradicional de cualquier memoria USB. Fundamentalmente no dejan de ser dispositivos USB, que llevan en su interior un chip con un firmware especial que aporta un extra de seguridad que verifica la cuenta y la URL. Al realizarlo de este modo, se evitan técnicas como el phishing, y, por ende, se evita la suplantación de cuentas.

A la hora de comprar estas llaves de seguridad, podemos observar que existen distintos tipos. Estas diferencias se basan en los métodos de conexión que ofrecen, que se pueden resumir en las siguientes clases:

- USB, disponen de un conector USB tipo A o C se conecta al conector USB de tu dispositivo para poder acceder a la cuenta.
- USB/NFC, además de la conexión USB ofrecen NFC para realizar la verificación con sólo acercarla al lector NFC del dispositivo.
- USB/NFC/Bluetooth, aquí se añade la conexión Bluetooth. De ese modo si no cuentas con lector NFC podrás usar la conexión Bluetooth que está mucho más extendida entre una gran variedad de dispositivos móviles.

La manera en la que estos dispositivos funcionan es totalmente segura. En el momento en el que un usuario lleva acabo un registro de manera "online" que emplea el estándar FIDO, el sistema genera una pareja de claves criptográficas. La clave privada se conserva en el "hardware" del dispositivo que el cliente debe mostrar al servicio online que dispone de la clave privada realizando una verificación matemática. La clave privada solo se puede desbloquear una vez que el usuario lo haya autorizado de forma local en el dispositivo. Este desbloqueo se puede realizar mediante una acción fácil y segura como, por ejemplo, utilizando la voz, huella dactilar, o introduciendo un PIN. En internet se pueden encontrar múltiples presentaciones que apoyan este método como segundo factor de autenticación (FIDO, slideshare, 2021).

La Alianza FIDO es una asociación industrial abierta con una misión enfocada: estándares de autenticación para ayudar a reducir la dependencia excesiva de las contraseñas en el mundo. La Alianza FIDO promueve el desarrollo, el uso y el cumplimiento de los estándares de autenticación y certificación de dispositivos (FIDO, Autenticación más simple y sólida, 2009). Al formar parte de FIDO empresas como Microsoft, Google, Samsung, Apple, PayPal, Visa, American Express, Lenovo, Intel, Yahoo y Nok Nok, entre otros, es seguro que lo apoyarán de una forma u otra en sus productos.

Grandes servicios como Google (Ayuda de cuenta Google, 2021) y Facebook (Servicio de ayuda Facebook, 2021) entre otros ofrecen en la web apoyo para activar las llaves de seguridad y otros como Dropbox (Dropbox, 2021) proporcionan información de cómo habilitar la verificación en dos pasos.

La configuración de estas llaves es muy sencilla. Básicamente, en las opciones de seguridad de los diferentes servicios deberás ver la opción de **Añadir llave de seguridad.** Cuando se accede a dicha opción se ve que hay distintas posibilidades, desde llaves USB físicas o incluso usar tu dispositivo móvil como llave. Esto último es una opción más reciente y consiste en hacer que cuando inicies sesión en un servicio tengas que confirmar que eres tú desde tu smartphone.

Google explica cómo utilizar la verificación en dos pasos para proteger la cuenta de los hackers, incluso si han robado información como tu contraseña y presenta cómo configurar la llave de seguridad integrada de tu teléfono para iniciar sesión de forma segura en dispositivos Chrome OS, iOS, macOS y Windows 10 (Google, Usar la llave de seguridad integrada de tu teléfono, 2021).

Hemos referenciado el método de acceso a la cuenta de Google por ser de interés institucional al tener la Universidad de Salamanca externalizado el correo electrónico a Gmail. Las cuentas de Google pueden ser personales o cuenta de Google Workspace y ambas pueden utilizar diferentes métodos para verificar la identidad (Google, Seguridad, 2021). En el caso de estas última el administrador debe permitir que actives la verificación en dos pasos al ser una cuenta institucional y ésta sería nuestra situación.

Para poder llevar a cabo el estudio del uso de las llaves físicas FIDO hemos necesitado contar con los siguientes recursos materiales y software específico:

- **Llaves FIDO usb con NFC y NFC y JavaCard**. Llave de seguridad USB + NFC y JavaCard (FIDO U2F Security Key) para PC, Mac y dispositivos móviles Android con NFC. Proponemos estas llaves FIDO porque al incorporar tecnología JavaCard permite ejecutar de forma segura pequeñas aplicaciones java (applets) en dicha llave.
- **Software servidor control llaves FIDO**. Se trata del software de activación de las llaves FIDO, que ahora para el estudio hemos utilizado una demo (Cloudentify, 2021) pero que si se llegara a implantar como acceso a diferentes servicios web en la Universidad habría que hacer el desarrollo web.

Hemos buscado en la red para ver si alguna universidad española ha puesto en marcha el uso de las llaves FIDO como segundo factor de autenticación y no hemos encontrado ninguna. Por ello, planteamos a la Universidad de Salamanca ser la pionera en la implantación del sistema FIDO para el inicio de sesión del campus de formación on-line y en la identificación en la intranet para el proceso de gestión académica.

4. RESULTADOS

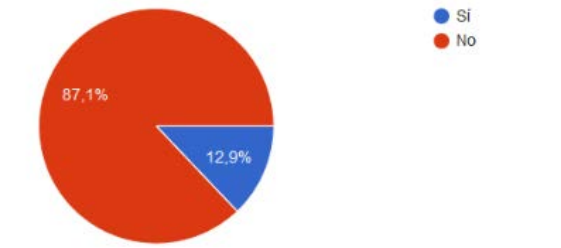
En el estudio que presentamos han participado 54 alumnos del Grado en Informática de la Facultad de Ciencias y 62 miembros de la Junta de Facultad de Ciencias y fue realizado antes de la pandemia. Nos centramos en el método que utilizan los usuarios para el acceso a los servicios digitales de la Universidad de Salamanca e hicimos un análisis de quienes utilizan un segundo factor de autenticación, el Latch.

En este estudio los estudiantes ponen de manifiesto que siempre utilizan el usuario y contraseña para el acceso (Tabla 1).

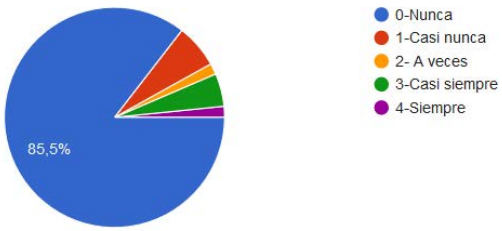
Tabla 1 Método de autenticación utilizado por los alumnos.

	Método para autenticación/validación de identidad			
	[Usuario y contraseña]	[DNIe con lector de tarjeta]	[Certificado digital de la FNMT]	[Otro]
0-Nunca	0,0%	81,0%	85,7%	87,3%
1-Casi nunca	1,6%	7,9%	3,2%	0,0%
2- A veces	3,2%	1,6%	0,0%	1,6%
3-Casi siempre	14,3%	1,6%	1,6%	0,0%
4-Siempre	81,0%	0,0%	0,0%	1,6%
Sin contestar	0,0%	7,9%	9,5%	9,5%

Pocos alumnos tienen instalada la app (Figura 6 (a)) y aunque así sea casi nunca la utilizan (Figura 6 (b)**¡Error! No se encuentra el origen de la referencia.**).



(a)



(b)

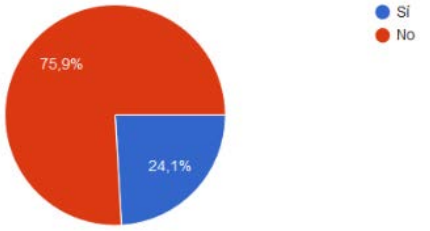
Figura 6 (a) Alumnos que tienen instalada la app de Latch. (b) Frecuencia de uso.

Los miembros de la Junta de Facultad también manifiestan que prácticamente siempre utilizan el usuario y contraseña para el acceso a los servicios on-line en la Universidad, que alguna vez utilizan el certificado digital de la FNMT y raramente el DNIe (Tabla 1 Método de autenticación utilizado por los alumnos.Tabla 2). En este caso, el profesorado mayoritariamente sí tiene formación previa por los cursos que se han impartido en la universidad y porque para otras gestiones externas como los sexenios o acreditaciones es obligatorio el uso del certificado digital.

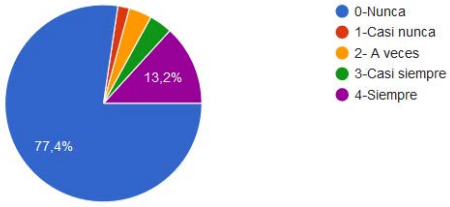
Tabla 2 Método de autenticación utilizado por miembros junta de facultad.

	Método para autenticación/validación de identidad			
	[Usuario y contraseña]	[DNIe con lector de tarjeta]	[Certificado digital de la FNMT]	[Otro]
0-Nunca	0,0%	63,0%	53,7%	63,0%
1-Casi nunca	0,0%	3,7%	7,4%	0,0%
2- A veces	1,9%	3,7%	9,3%	0,0%
3-Casi siempre	9,3%	0,0%	1,9%	0,0%
4-Siempre	87,0%	0,0%	1,9%	0,0%
Sin contestar	1,9%	29,6%	25,9%	37,0%

Del estudio se deduce que menos de la cuarta parte de los que respondieron la encuesta tienen instalada la app (Figura 7 (a)) y de estos, sólo la mitad la utilizan (Figura 7 (b)). El porcentaje ha aumentado levemente respecto del de alumnos y posiblemente sea por miedo a posible falsificación de las actas.



(a)



(b)

Figura 7 (a) Miembros Junta de Facultad que tienen instalada la app Latch. (b) Frecuencia de uso de la app.

También les preguntamos a los alumnos por la necesidad de aumentar la seguridad en los servicios on-line de la Universidad y apreciamos que 58,7% consideran que se debería aumentar. La misma encuesta fue respondida por miembros de la Junta de Facultad, formada por personal docente e investigador, personal de administración y servicios, estudiantes de grado y de postgrado; de todos los estamentos hubo participación; en el caso de estudio con un porcentaje respectivamente de 75,9%, 11,1%, 7,4% y 5,6%. A la pregunta de si ven necesitad de aumentar la seguridad en los servicios on-line de la Universidad se aprecia un porcentaje inferior que en el caso de los alumnos y posiblemente sea por sentir seguridad los que utilizan la app de seguridad (Tabla 3).

Tabla 3 Respuesta ante la necesidad de aumentar el nivel de seguridad.

	Miembros de la Junta de Facultad	Alumnos
Sí	46,3%	39,7%
No	50,0%	58,7%
NC	3,7%	1,6%

Del estudio se concluye que, aunque tengamos a nuestra disposición un segundo factor de autenticación no lo usamos.

Puede que no lo usemos por desconocimiento o por necesitar un móvil para usarlo o incluso ser un segundo factor poco cómodo de utilizar. Por ello vamos a analizar otras alternativas como segundo factor de autenticación y con mayor seguridad.

Cada autor, participante de este estudio hemos ido probando diferentes segundos factores de autenticación. Cada uno nos hemos encontrado con una serie de dificultades. En particular, hemos comprobado que las llaves sólo son compatibles oficialmente con Google Chrome; en Mozilla Firefox sólo es compatible mediante un plugin, aunque están trabajando para implementar el Universal 2 Factor en Firefox de forma nativa. Otra de las dificultades es que para acceder a servicios como Google Drive para activar las llaves tenemos que hacer uso de un teléfono móvil. En este caso, como la Universidad de Salamanca cuenta con telefonía móvil sobre protocolo IP (VoIP) cada profesor dispone de un número de móvil, aunque en algunos casos es compartido; el problema es que los alumnos tendrían que hacer uso de tu teléfono personal.

Todos los participantes en este estudio hemos registrado las llaves de seguridad USB/NFC/Bluetooth en la web de prueba (Cloudentify, 2021) y hemos probado el acceso a la web con dicha llave sin ningún problema.

5. Conclusiones

Realizado el estudio llegamos a unas conclusiones que se resumen en los siguientes ítems:

- La mayoría de los usuarios desconocen el segundo factor de autenticación que ofrece la universidad, en concreto la existencia de Latch. Además de entre quienes lo conocen, muchos no lo tienen activado y muchos de los que lo tienen activado lo dejan abierto.
- Es una necesitad trabajar con un segundo factor de autenticación para acceder al campus virtual y a servicios como acceso a grabar las actas y otros que tienen información confidencial. Actualmente se puede acceder con certificado digital pero también con usuario y contraseña.
- El manejo de las llaves FIDO es muy sencillo como hemos podido probar en diferentes servicios.
- El segundo factor de autenticación mediante el uso de un dispositivo hardware aumenta el nivel de seguridad frente a otros métodos de autenticación.
- Hay que hacer un estudio de qué procesos de la gestión on-line del proceso de enseñanza/aprendizaje se deben considerar de nivel máximo de seguridad y plantear la viabilidad de hacer obligatorio el uso de las llaves FIDO.
- La inversión para aumentar la seguridad es asequible; en concreto hay que proporcionar una llave FIDO a cada profesor, hacer el desarrollo web de acceso a los diferentes servicios y desarrollar el software de control de las llaves.

Sin duda aumentar la seguridad en la verificación de la identidad on-line repercutirá sobre la docencia. En la actualidad la mayoría de la formación Oficial en la USAL es presencial entendiendo que la mayor dificultad en la formación on-line es la acreditación del estudiante sobre todo en el momento de realizar la evaluación on-line. En la enseñanza presencial para la evaluación continua nos da miedo dar más peso a los cuestionarios o tareas realizadas por la plataforma de formación on-line por la inseguridad de quien lo ha realizado. Por ello, si aumentamos el grado de certeza de quién es quién se está formando podremos apostar más por la formación virtual, por la semipresencial o presencial con mayor formación complementaria on-line.

Evitaremos que los mensajes que nos enviamos por correo electrónico, por ejemplo, exámenes que estamos preparando entre profesores, o los mismos exámenes que tengamos en Dropbox, caigan en manos de los estudiantes que se vayan a evaluar si alguien consigue nuestro usuario y contraseña ya que le faltaría la llave.

Una llave FIDO nos sirve para acompañar a nuestro usuario y contraseña de cuenta de acceso con un segundo factor de autentificación, siendo una llave de este tipo más segura que un SMS o incluso un código de autenticador móvil, por el sencillo hecho de no estar conectado ni ser alterable.

La llave FIDO U2F (Universal 2 Factor Authentication) lleva grabada una clave privada que no es modificable y será cotejada con la clave pública en nuestros servicios online, cada vez que iniciemos sesión en nuestra cuenta. Por ejemplo, si nos identifiquemos en el id_USAL para acceder a la plataforma de formación studium.usal.es, a la calificación de actas, en la cuenta Google, Dropbox, etc.

Con esta propuesta aproximamos la tecnología de las Universidades a las que utilizan otros grandes mundiales como como Google, Apple, Dropbox, etc. que ya la tienen experimentada.

Agradecimientos

A la Universidad de Salamanca por la convocatoria de ayudas a proyectos de innovación y mejora docente por la concesión de las propuestas “Análisis y propuesta de diferentes métodos de autenticación para el acceso a las plataformas de formación on-line y al servicio de calificación de actas. (Código del Proyecto: ID2016/0106)” y “Llaves FIDO (Fast IDentify Online) como segundo factor de autenticación en la gestión on-line de los procesos de enseñanza y aprendizaje (Código del Proyecto: ID2017/030)” que nos ha permitido desarrollar este estudio.

Agradecer a los estudiantes del Grado en informática de la Universidad de Salamanca y a los miembros de la Junta de Facultad de Ciencias por su colaboración plasmada en las respuestas de los cuestionarios.

Referencias

Ayuda de cuenta Google. (2021). Obtenido de Utilizar una llave de seguridad para la verificación en dos pasos: https://support.google.com/accounts/answer/6103523?co=GENIE.Platform%3DAndroid&hl=es

Cloudentify. (2021). *Prueba usao la clave de seguridad FIDO U2F*. Obtenido de https://u2f.cloudentify.com/u2fdemo/

Ding Wang, X. Z. (January de 2020). *Understanding security failures of multi-factor authentication schemes for multi-*

server environments. Obtenido de https://id.elsevier.com/as/hx96h/resume/as/authorization.ping?client_id=SDFE-v3&state=retryCounter%3D0%26csrfToken%3Dff70cb41-4a18-4532-8a60-e3bc32b95420%26idpPolicy%3Durn%253Acom%253Aelsevier%253Aidp%253Apolicy%253Aproduct%253Ainst_assoc%26returnUrl%3D%2

Dropbox. (2021). *Cómo habilitar la verificación en dos pasos*. Obtenido de https://www.dropbox.com/es_ES/help/security/enable-two-step-verification#2falsecurity-keys

EUR-Lex, A. t. (25 de noviembre de 2015). *Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015*. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015L2366

FIDO, A. (2009). *Autenticación más simple y sólida*. Obtenido de https://fidoalliance.org/

FIDO, A. (2021). *slideshare*. Obtenido de Alianza FIDO: https://www.slideshare.net/FIDOAlliance/presentations

Google. (2021). *Seguridad*. Obtenido de https://myaccount.google.com/security

Google. (2021). *Usar la llave de seguridad integrada de tu teléfono*. Obtenido de https://support.google.com/accounts/answer/9289445?co=GENIE.Platform%3DAndroid&oco=0

Megouache, L. Z. (2020). *Hum. Cent. Comput. Inf. Sci. 10, 15 (2020)*. Obtenido de Ensuring user authentication and data integrity in multi-cloud environment: https://link.springer.com/article/10.1186%2Fs13673-020-00224-y

Servicio de ayuda Facebook. (2021). *¿Qué es una clave de seguridad y cómo funciona?* Obtenido de https://es-la.facebook.com/help/401566786855239