



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

**UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA
ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES**

Jurgen Andoni Ramirez Ramírez

Asesorado por el Ing. Mario José Bautista Fuentes

Guatemala, noviembre de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA
ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JURGEN ANDONI RAMIREZ RAMÍREZ
ASESORADO POR EL ING. MARIO JOSÉ BAUTISTA FUENTES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

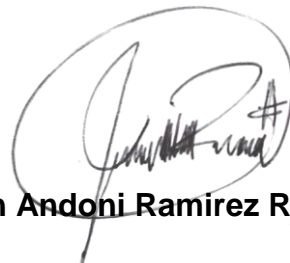
DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Cesar Augusto Fernández Cáceres
EXAMINADOR	Ing. Herman Igor Véliz Linares
EXAMINADOR	Ing. Miguel Ángel Cancinos Rendón
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 20 de noviembre de 2021.

A handwritten signature in black ink, enclosed in a light grey oval. The signature is stylized and appears to read 'Jurgén Andoni Ramírez Ramírez'.

Jurgén Andoni Ramírez Ramírez

Ciudad de Guatemala, 02 de noviembre de 2022




Ing. Carlos Azurdia
Coordinador Trabajos de Tesis
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería

Estimado Ing. Azurdia

Por este medio informo que en mi papel de asesor he revisado el trabajo de Tesis titulado: **“UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES”** elaborado por el estudiante **Jurgen Andoni Ramirez Ramirez** quién se identifica con DPI **2557346111221** y registro academico **201404179**.

Con base a la evaluación realizada hago constar que el trabajo de graduación cuenta con mi aprobación.

Atentamente,


Mario Jose Bautista Fuentes
Ingeniero en C.C Y Sistemas
Colegiado. 10017
Ing. Mario Jose Bautista Fuentes
Asesor de Tesis



Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 16 de noviembre de 2022

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **JURGEN ANDONI RAMÍREZ RAMÍREZ** con carné **201404179** y CUI **2557 34611 1221** titulado “**UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES**” y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,



Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA

LNG.DIRECTOR.240.EICCSS.2022

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador de área y la aprobación del área de lingüística del trabajo de graduación titulado: **UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES**, presentado por: **Jurgen Andoni Ramirez Ramírez**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería.

“ID Y ENSEÑAD A TODOS”



Msc. Ing. Carlos Gustavo Alonzo
Director

Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, noviembre de 2022



LNG.DECANATO.OI.800.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **UTILIZACIÓN DE LA PLATAFORMA DE PRIVACIDAD -DIGI.ME- PARA LA ADMINISTRACIÓN DE LA INFORMACIÓN PERSONAL EN APLICACIONES MÓVILES**, presentado por: **Jurgen Andoni Ramirez Ramirez**, después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:



Inga. Aurelia Anabela Cordova Estrada

Decana

Guatemala, noviembre de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios

Por ser mi fuente de inspiración, darme sabiduría y permitirme culminar esta etapa tan importante en mi vida.

Mis padres

Víctor Ramírez y Anabela Ramírez (q. e. p. d.), por ser ejemplo de fortaleza, esfuerzo y dedicación. Por su apoyo incondicional en cada etapa de mi vida.

Mis hermanos

Por brindarme su apoyo en todo momento y siempre ayudarme cuando lo he necesitado.

AGRADECIMIENTOS A:

**Universidad de San
Carlos de Guatemala**

Por ser mí alma máter, y brindarme los medios y recursos necesarios para formarme como profesional.

Facultad de Ingeniería

Por ser mi segunda casa y permitirme recibir el conocimiento en sus aulas, donde pude formarme profesionalmente con las enseñanzas de mis docentes y consejos de compañeros de estudio.

Ing. Anabela Córdova

Por su apoyo y orientación durante mi carrera.

Ing. Mario Bautista

Por darme su apoyo, compartir su experiencia y consejos en el asesoramiento de este trabajo de graduación.

**Mis catedráticos de la
Facultad de Ingeniería**

Por ayudarme en mi crecimiento personal y profesional mediante sus enseñanzas en el aula.

**Mis profesores de
primaria y secundaria**

Por forjar mi espíritu desde muy pequeño, sin su dedicación y conocimiento transmitido este acto no fuera posible. Especialmente a los maestros Glenda Paz, Jorge Cuevas, Cindy Alvarado en la Escuela Privada Ovidio Pivaral Herrarte.

Mis familiares

Por siempre darme palabras de apoyo y aliento cuando más lo necesitaba.

Mi novia

Por su paciencia, apoyo y palabras de aliento.

Mis amigos

Por las experiencias compartidas y por siempre encontrar en ellos un apoyo a lo largo de esta etapa.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES.....	V
LISTA DE SÍMBOLOS	VII
GLOSARIO	IX
RESUMEN	XIII
OBJETIVOS.....	XV
INTRODUCCIÓN	XVII
1. INICIOS DE LA WORLD WIDE WEB.....	1
1.1. Inicios de la World Wide Web.....	1
1.2. Datos personales.....	2
1.3. Filtraciones de datos en plataformas de gigantes tecnológicos.....	3
1.4. Botón Azul EE.UU.	5
1.5. Reglamento general de protección de datos (GDPR EUROPA)	5
1.5.1. Alcance del GRDP	7
2. GESTIÓN DE INFORMACIÓN PERSONAL	9
2.1. Definición de gestión de información personal	9
2.2. Herramientas de gestión de la información	10
2.3. Almacenamiento de datos personales.....	10
2.4. Identidad única	11
2.5. Nube de datos personales.....	12
2.6. Plataformas de Identidad.....	13

2.7.	Diferencias entre nube de datos personales y plataformas de identidad.....	14
3.	¿QUE ES -DIGI.ME-?	17
3.1.	Características de -Digi.me-	18
3.2.	Funciones de -Digi.me-	19
3.2.1.	-Digi.me- Connect	19
3.2.2.	Acceso a datos con consentimiento de usuario	19
3.2.3.	Contrato de consentimiento.....	20
3.2.4.	Plataforma -Digi.me- en dispositivos móviles	23
3.2.4.1.	-Digi.me- Data Viewer	23
3.2.4.2.	PostCleaner.....	23
3.2.5.	Playground -Digi.me-.....	24
3.3.	Política de privacidad -Digi.me-.....	24
3.3.1.	Como recopilan la información	25
3.3.2.	Tipos de datos recopilados y conservados.....	25
3.3.3.	Como se utilizarán sus datos	26
3.3.4.	Conservación de datos.....	27
3.4.	Protocolos de Seguridad -Digi.me-	28
3.4.1.	Alcance de seguridad.....	28
3.4.2.	Diseño de seguridad	30
3.5.	Acreditaciones y certificaciones	32
3.5.1.	ISO 27001:2013 e ISO 27017:2015	32
3.5.2.	NEN 7510.....	33
3.5.3.	Medmij.....	33
3.5.4.	Cyber Essentials	33
3.5.5.	Estado de los operadores de MyData 2020	34
3.6.	Beneficios para los usuarios	34
3.7.	Beneficios para las organizaciones o empresas.	35

4.	UTILIZACIÓN DE -DIGI.ME-	37
4.1.	Definición del problema	37
4.2.	Uso de playground -Digi.me-	37
4.3.	Implementación en Android	45
4.3.1.	Descripción de la aplicación	45
4.4.	Diseño de APP	47
4.4.1.	Configuración de ID e instalación SDK Android.....	48
4.4.2.	Implementación en proyecto Android	50
4.4.3.	Escritura de archivos -Digi.me-	51
4.4.4.	Lectura de archivos -Digi.me-	52
4.4.5.	Aplicación Feeling App	54
	CONCLUSIONES	61
	RECOMENDACIONES	63
	BIBLIOGRAFÍA.....	65

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Detalle de ¿por qué?.....	20
2.	¿Cómo lo hará?	21
3.	Dar consentimiento	22
4.	Agregar playground -Digi.me-	38
5.	Dashboard.....	39
6.	Configuraciones	40
7.	Solicitar información al usuario	41
8.	-Digi.me- playground autorización.....	42
9.	Autorizar a -Digi.me- a acceder a la cuenta	43
10.	Dashboard -Digi.me- al recibir información del usuario.....	44
11.	Diagrama Flujo de funcionalidad Feeling App.....	46
12.	Diseño de la aplicación Feeling APP.....	47
13.	Diagrama base de datos Feeling APP	48
14.	Pantalla de inicio Feeling APP	54
15.	Registro Feeling App.....	55
16.	Inicio de Sesión Feeling APP	55
17.	Menú	56
18.	Inicio.....	56
19.	Registrar sentimiento	57
20.	Historial de sentimientos	57
21.	Menú -Digi.me-.....	58
22.	Escribiendo -Digi.me-	58
23.	Leyendo archivo escrito en formato JSON.....	59

LISTA DE SÍMBOLOS

Símbolo	Significado
ZB	10^{21} bytes

GLOSARIO

API	Application Programming Interface.
CCTV	Circuito cerrado de cámaras de vigilancia.
Datos personales	Es cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.
-Digi.me-	Plataforma de uso compartido privado para conectarse a diferentes fuentes de datos solicitando consentimiento de usuario.
eIDAS	Identificación Electrónica, Autenticación y Servicios de Confianza.
GRDP	Reglamento General de Protección de Datos, es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

Hipertexto	Sistema de organización y presentación de datos que se basa en la vinculación de fragmentos textuales o gráficos a otros fragmentos, lo cual permite al usuario acceder a la información no necesariamente de forma secuencial sino desde cualquiera de los distintos ítems relacionados.
HTML	Es el código que se utiliza para estructurar y desplegar una página web y sus contenidos. Por ejemplo, sus contenidos podrían ser párrafos, una lista con viñetas, o imágenes y tablas de datos.
POD	Personal Online Data.
PODS	Personal Online Data Store.
SDK	Es generalmente un conjunto de herramientas de desarrollo de software que permite a un desarrollador de software crear una aplicación informática para un sistema.
UE	Unión Europea.
World Wide Web	Es un sistema que funciona por medio de Internet, por el cual se pueden transmitir diversos tipos de datos a través del Protocolo de Transferencia de Hipertextos o HTTP, que son los enlaces de la página web.

Zettabyte

Es una unidad de almacenamiento de información cuyo símbolo es el ZB, equivale a 10^{21} bytes.

RESUMEN

Han pasado más de tres décadas desde que inicio la *web* (Word Wide Web), se inició intercambiando documentos entre instituciones de educación y otras organizaciones, para luego a pasar a intercambiar los datos personales a cambio de servicios gratuitos, en todo este tiempo se han generado miles de datos personales de cada usuario que interactúa con diferentes plataformas informáticas en toda la red, las grandes empresas nunca explican de forma clara los procedimientos para procesar los datos, el tiempo que los tendrán almacenados.

No existen reglamentos en la mayoría de países que protejan los datos personales o que establezcan normas claras de cómo se debe garantizar la protección de los datos personales, ni de como las empresas deben de tratarlos.

Los datos personales que se generan en los sistemas de información que interactúa el usuario son comerciados por empresas y no se les notifica a los usuarios, incluso en muchas ocasiones los usuarios no conocen con exactitud qué datos está recolectando las aplicaciones con las que interactúa porque esta no le informa de forma clara.

Es por esto que surgen plataformas que buscan informar con flujos preestablecidos de forma clara como se estará procesando su información y también apegada a reglamentos de protección de datos que garantiza que los usuarios son los que concederán permiso para que las organizaciones o

empresas puedan hacer uso de los mismos a cambio de servicios de valor personalizados para los usuarios.

OBJETIVOS

General

Utilizar la plataforma de uso compartido privado -Digi.me- para facilitar el acceso de información personal con el consentimiento del usuario.

Específicos

1. Enumerar los beneficios que obtienen los usuarios al tener su biblioteca privada de datos personales, y poder decidir cuándo compartirlos con una aplicación.
2. Identificar los beneficios que obtienen las organizaciones o empresas al acceder; a los datos personales con el consentimiento del usuario.
3. Describir el alcance y diseño de seguridad que utiliza la plataforma de gestión de privacidad -Digi.me- para proteger la información personal.
4. Evaluar la funcionalidad del SDK de la plataforma de gestión de privacidad -Digi.me- para acceder a los datos personales.

INTRODUCCIÓN

Las principales características de la investigación se basan en la plataforma de uso compartido privado -Digi.me-, como una solución para solicitar datos personales con el consentimiento del usuario, los datos personales que genera cada usuario en la red están en diferentes sistemas de información, la plataforma de uso compartido permite tener una única conexión para extraer la información de diferentes fuentes, se abordan temas como reglamento general de protección de datos aplicado en países de Europa, como otras iniciativas que se han impulsado en Estados Unidos orientadas a la protección de datos personales, se explica la diferencia entre la nube de datos personales y plataformas de identidad.

El trabajo de investigación será una guía para; solicitar información con el consentimiento del usuario, los beneficios obtenidos al compartir información, describir el alcance y diseño de seguridad que maneja esta plataforma de gestión de privacidad, y de cómo utilizar el SDK en aplicaciones móviles para poder solicitar información del usuario de algunas fuentes de datos populares como lo pueden ser redes sociales, ya sea compartir información o consumir información, los beneficios que obtienen las empresas al ser transparentes en el procesamiento de datos personales con el consentimiento de cada usuario como también se aborda los beneficios que obtienen los usuarios al dar consentimiento de su información personal.

1. INICIOS DE LA WORLD WIDE WEB

1.1. Inicios de la World Wide Web

El World-Wide Web (WWW) es un sistema hipermedia distribuido, accesible a través de Internet, que permite navegar con facilidad por una enorme cantidad de información. El WWW fue iniciado en el CERN por Tim Berners-Lee (Berners-Lee, 1993a; Berners-Lee, Caillau, Groff y Pollerman, 1992a y 1992b) con el objeto de integrar información accesible a través de una única red de ordenadores, pero mediante sistemas diversos. El WWW se sustenta en cuatro elementos fundamentales: un nuevo protocolo de comunicación (HTTP o HyperText Transfer Protocol); Un lenguaje para escribir documentos hipermedia (HTML o Hypertext Markup Language); un sistema notacional para designar objetos en la Internet y las operaciones a realizar sobre ellos (URL o Uniform Resource Locator); y, finalmente, un conjunto de aplicaciones (los clientes o browsers WWW y los servidores httpd) que se dividen el trabajo de servir y presentar la información multimedia al usuario.¹

La historia y desarrollo del lenguaje de marcado, Hypertext Mark Up Language (de aquí en adelante HTML), es una historia llena de necesidades y desarrollos realizados en un entorno de innovación totalmente dinámico y colaborativo, en el cual se mezclan intereses de empresas privadas, con deseos de estandarización de consorcios, intereses de usuarios generalistas y hasta impulsos personales.²

El lenguaje HTML no es otra cosa, que un lenguaje estandarizado con el que los navegadores interpretan la información que contienen la multitud de páginas que componen la World Wide Web (de aquí en adelante WWW). Es un lenguaje de marcación de texto que permite al navegador conectado interpretar la página que solicita al servidor. No es un lenguaje de programación y no tiene compiladores, por lo tanto si hay algún error en los documentos que interpreta, lo visualiza de la manera en que no lo ha entendido. El lenguaje HTML se basa principalmente en un sistema de etiquetas que indica al navegador dónde está el cuerpo de un documento.³

¹ Unidad de Innovación, Universidad de Murcia. *Diseño y evaluación de materiales didácticos. La navegación hipertextual en el World-Wide Web.* https://www.um.es/innova/OCW/diseño_y_evaluación_materiales_didacticos/mpaz/utilidades/pdf/18.pdf. Consulta: 11 de septiembre de 2022.

² ABBATE, Janet. *Inventing the Internet, The MIT Press.* https://gredos.usal.es/bitstream/handle/10366/132322/El_inicio_de_la_Web_historia_y_cronologia.pdf?sequence=1. Consulta: 20 de septiembre de 2022.

³ RODRÍGUEZ, Elisabet. *El HTML, una idea en evolución.* <http://www.maestrosdelWeb.com/editorial/htmlhis/>. Consulta: 22 de septiembre de 2022.

Este lenguaje estándar ha evolucionado notablemente desde la primera versión que conceptualizó Tim Berners-Lee en 1991 (Zakon, 1993-2011) y ha llevado una evolución constante hacia un mayor dinamismo y ejecución de acciones (a través de otras tecnologías y complementos) y cada vez menos estatismo, de la mano de tecnologías auxiliares al lenguaje principal, que han sido incorporadas con el propósito de su estandarización. La historia del lenguaje HTML, comienza en el European Laboratory for Particle Physics (de aquí en adelante CERN), en Ginebra, Suiza. El CERN es un centro en el que se dan cita algunas de las mentes más brillantes y abstractas del mundo de la física.⁴

La World Wide Web surge como una necesidad de intercambio de información principalmente académica, también de intereses privados y personales, y ha estado cambiando y siendo más adaptada a la demanda de información global, ha permitido superar obstáculos de comunicación entre continentes, y en la actualidad es algo esencial para los avances en todos los campos del conocimiento.

1.2. Datos personales

Según el proyecto Hub of All Things (HAT), datos personales son todo lo que hay en Internet que es personal, palabras, fotos, música, ubicaciones, transacciones, financieras. Todo lo generado cuando se completa un formulario, se crea una cuenta de usuario en aplicaciones y sitios web, cuando se interactúa en cualquier sistema, utilizando redes sociales o sitios web de comercio electrónico, serán fragmentos de información personal que quedarán en internet.

El GRDP en el Art.4 del Reglamento expresa que «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización,

⁴ TABARÉS GUTIÉRREZ, Raúl. *Inicio de la web*. https://gredos.usal.es/bitstream/handle/10366/132322/EI_inicio_de_la_Web_historia_y_cronologia.pdf?sequence=1&isAllowed=y. Consulta: 5 de septiembre de 2022.

un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.⁵

Los datos personales que genera cada persona son cada vez mayores, solo en los dispositivos móvil actualmente se albergan muchos archivos con información personal y muy sensible, la interacción humana con los dispositivos digitales va en incremento, se van integrando a cada una de las actividades cotidianas, comerciales, sociales entre otras.

Según el informe de Data Never Sleeps 9.0 cada minuto a nivel mundial para julio de 2021 se comparten 240,000 fotos en Facebook, se hacen 575,000 Tweets, 5.7 millones de búsquedas en Google, en ese año la cantidad de datos consumidos globalmente fue de 79 *zettabytes* y se proyecta un crecimiento a 180 *zettabits* para el 2025.

1.3. Filtraciones de datos en plataformas de gigantes tecnológicos

En el año 2021 Facebook declaro que hubo una filtración de datos según la empresa no obtuvieron estos datos pirateando sus sistemas, sino extrayéndolos de la plataforma antes de septiembre de 2019 informó Clark.

En esta filtración de datos fue expuesta información personal de un poco más de 533 millones de usuarios de más de 106 países en los que incluían números de teléfonos, Id de Facebook, nombres completos, ubicaciones, fechas de nacimiento, biografías y en algunos casos correos electrónicos, esto publicado en un foro de piratería de bajo nivel.

⁵ Domo. *Data Never Sleeps 9.0*. <https://www.domo.com/learn/infographic/data-never-sleeps-9>. Consulta: 2 de agosto de 2022.

En el mismo año 2021 LinkedIn fue víctima de una filtración de datos, este afecto a 700 millones de usuarios de esta plataforma, la información fue principalmente publicada, pero los datos que se publicaron en la Dark Web en junio de 2021, incluían direcciones de correo electrónico, número de teléfono, registro de geolocalización, géneros y otros detalles de redes sociales, la empresa se negó aceptar su culpabilidad.

En noviembre de 2019, también sufrió un ataque el sitio de compras chino Alibaba's y este afecto a más de 1,100 millones de datos de usuarios, según el reporte el ataque duro ocho meses, el software extraía información de los usuarios como identificaciones, números de teléfonos móviles y comentarios de clientes, en este no se comprometió información encriptada como contraseñas.

Otras filtraciones que han ocurrido en años anteriores en diversas plataformas han revelado estos problemas no son los que se sufren por tener la información personal de forma centralizada en servidores de cada una de estas empresas, pero existe un informe realizado en el año 2017 por Cracked Labs en que se revela como las empresas comparten y agrupan los datos personales de sus usuarios recopilados de forma directa o indirecta.

A lo largo de la historia de la era informática los datos personales se han vistos afectados porque los datos personales están almacenados en único sistema, significa que la información no se encuentra en nodos separados sino que están concentrados en un solo lugar y siempre surgen vulnerabilidades que dejan a la información expuesta en dichos sistemas y hay personas con capacidad de explotar estas vulnerabilidades, los más afectados son los usuarios pues en muchos casos la información llega a ser muy sensible.

1.4. Botón Azul EE.UU.

Este concepto surge en el año 2010, y su objetivo es permitir un acceso directo al consumidor de su propia información de salud en un formato que puedan usar, esto significa que el consumidor puede descargar un único archivo electrónico que contiene sus datos de salud disponibles, esta iniciativa se ha extendido más allá de agencias gubernamentales, sino que también al sector privado.

Se han desarrollado eventos de gobierno abierto en los cuales se promueve la regulación y publicación de datos de gobierno, existe un movimiento sobre el botón azul donde se informa sobre el acceso a la información de salud como utiliza la información, y también como proteger la privacidad e información esto proporcionado por The Office of the National Coordinator for Health Information Technology (ONC)[La Oficina del Coordinador Nacional de Tecnología de la Información de la Salud de EE.UU].

Esta iniciativa ha beneficiado a los usuarios pues han podido acceder y conocer, descargar su información médica, es necesario empoderar a las personas pues son ellas quienes son dueñas de su información y tienen derechos de conocer y administrar su información que reside en los sistemas que interactúa.

1.5. Reglamento general de protección de datos (GDPR EUROPA)

El Reglamento General de Protección de Datos (GRDP por sus siglas en inglés) es un marco legal que establece pautas para la recopilación y el procesamiento de información personal de personas que viven en la Unión Europea (UE). Dado que el Reglamento se aplica independientemente de dónde se encuentren los sitios web, todos los sitios que atraigan a visitantes europeos deben respetarlo, incluso si no comercializan bienes o servicios específicamente para los residentes de la UE.

El GRDP exige que los visitantes de la UE reciban una serie de divulgaciones de datos. El sitio también debe tomar medidas para facilitar tales derechos de los consumidores de la UE como una notificación oportuna en caso de que se produzca una violación de los datos personales. Adoptado en abril de 2016, el Reglamento entró en pleno vigor en mayo de 2018, después de un período de transición de dos años.⁶

El propósito del GRDP es proteger a las personas y los datos que las describen y garantizar que las organizaciones que recopilan esos datos lo hagan de manera responsable. El GRDP también exige que los datos personales deben estar protegidos contra el "procesamiento no autorizado o ilegal, y contra la pérdida, destrucción o daño accidental". El reglamento también sugiere límites sobre la cantidad de datos que se recopilan, diciendo que la recopilación de datos debe limitarse a lo que sea necesario en relación con los fines para los que se procesan.⁷

La reglamentación toma en cuenta el tratamiento de los datos, basándose en estos cuatro puntos:

- Identificar y estructurar los datos personales en archivos según su finalidad.
- Categorizar cada archivo de acuerdo a su tipo de dato Básicos, Especiales o Penales.
- Asociar cada archivo a un responsable o encargado de tratamiento
- Identificar si algún archivo pertenece a alguna de las categorías especiales (alto riesgo, transferencias internacionales, elaboración de perfiles, entre otros).

El autor de la investigación considera como objetivo que este reglamento da un conjunto de reglas de protección y privacidad de datos para que la Unión

⁶ (DRURY Frankenfeld; COSTAGLIOLA. *Investopedia*.: www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp. Consulta: 7 de agosto de 2022.

⁷ CASTAGNA, R., & Lavery, T. *TechTarget*. techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR. Consulta: 8 de julio de 2022.

Europea es decir los países que la integran, tenga un marco de interpretación homogéneo estableciendo reglas claras para todas las empresas de tecnología de cómo deben operar los datos en esa región.

Establece normas más estrictas, como el autocontrol o control individual, o cómo las compañías pueden usar la información que está directa y personalmente relacionada con los ciudadanos. Estas normas rigen además lo que sucede si se viola el acceso a los datos personales de un individuo y las secuelas (penalidades) que las organizaciones pueden padecer en tal caso. Con esta norma aplicada en la Unión Europea algunas compañías grandes como Google tuvieron que realizar algunos ajustes al tratamiento de la información de sus usuarios.⁸

1.5.1. Alcance del GRDP

El alcance de esta norma que aplica la Unión Europea es ceder el control de los datos personales y como se va a dar tratamiento a los mismos desde un entorno jurídico de protección. Esta se extiende a:

- Organizaciones o empresas que tienen presencia física en cualquier país miembro de la UE.
- Organizaciones o empresas que procesan o almacenan datos sobre individuos que residen en la UE.
- Organizaciones o empresas que utilizan servicios de terceros que procesan o almacenan información de los individuos que residan en la UE.

⁸ XXIV Congreso Argentino de Ciencias de la Computación. *Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica.* http://sedici.unlp.edu.ar/bitstream/handle/10915/73652/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y. Consulta: 9 de julio de 2022.

“Todas las empresas u organizaciones que realicen este tipo de servicios y que almacenan información deben de apegarse a las normas de la UE.”⁹

El GRDP abarca una amplia gama de actividades de seguimiento, incluida la publicidad conductual, las actividades de geolocalización, en particular con fines de marketing, el seguimiento en línea mediante el uso de cookies u otras técnicas de seguimiento, como la toma de huellas dactilares, la dieta personalizada y los servicios de análisis de salud en línea, CCTV, mercado encuestas, así como otros estudios de comportamiento basados en perfiles individuales y seguimiento o informes regulares sobre el estado de salud de un individuo.¹⁰

La finalidad del reglamento es proteger el derecho individual, así también ampliar la definición de lo que es información personal y privada, que sobre lo que incluye, como, registros financieros, oficiales, médicos, información genética, cultural y social. El usuario es quien debe dar el consentimiento a las empresas para obtener y utilizar sus datos, debiendo respetar su derecho a que se eliminen todos los datos que tenga la empresa, cuando sea solicitado por él.

⁹ XXIV Congreso Argentino de Ciencias de la Computación. *Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica*. http://sedici.unlp.edu.ar/bitstream/handle/10915/73652/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y. Consulta: 9 de mayo de 2022.

¹⁰ Zacco. *We can't find the page you're looking for*. <https://www.zacco.de/articles/the-territorial-scope-of-the-gdpr>. Consulta: 12 de septiembre de 2022.

2. GESTIÓN DE INFORMACIÓN PERSONAL

2.1. Definición de gestión de información personal

La gestión de información personal (PIM por sus siglas en inglés), se refiere tanto a la práctica como a el estudio de las actividades que realiza una persona para adquirir o crear, almacenar, organizar, mantener, recuperar, usar y distribuir la información necesaria para cumplir con los muchos objetivos de la vida (cotidianos y a largo plazo, relacionados con el trabajo y no), y para cumplir con los muchos roles y responsabilidades de la vida (como padre, cónyuge, amigo, empleado, miembro de la comunidad, entre otros).

PIM por sus siglas en inglés (Personal Information Management), pone especial énfasis en la organización y mantenimiento de colecciones de información personal en las que elementos de información, como documentos en papel, documentos electrónicos, correo electrónico, mensajes, referencias web, notas escritas a mano, se almacenan para su uso posterior y reutilización repetida.

Anteriormente existían los archivos físicos como una forma de guardar y organizar la información en la actualidad la forma de almacenar la información cambio y esto se encuentra en ordenadores o en la nube, gestionar la información personal debe considerarse como una actividad importante, conocer que información se tiene en la red, como poder gestionarla de forma fácil, actualmente se genera mucha información al utilizar diversos servicios electrónicos.

2.2. Herramientas de gestión de la información

En la actualidad existen a disposición muchas herramientas para gestionar la información personal, se debe de seleccionar una herramienta adecuada a la necesidad dependiendo de las actividades que se necesiten realizar, por ejemplo, algunas pueden ser como EsencialPIM que le permite organizar correo, notas, documento y conectarse a diversas nubes.

Puede utilizar otras un poco menos sofisticadas como Google Keep para mantener sus apuntes, Microsoft to Do para gestionar sus actividades diarias, un simple editor de texto, pero si necesita herramientas para buscar o almacenar la información puede utilizar el sistema de ficheros de los diversos sistemas operativos actuales que le permite guardar su información en ficheros, también puede exportar su información en formatos como JSON para posteriormente darle un tratamiento mucho más técnico en el capítulo 3 y 4 de la presente investigación muestra cómo se puede extraer información personal de las plataformas de redes sociales.

2.3. Almacenamiento de datos personales

El almacenamiento de datos consiste en la conservación de información empleando una tecnología específicamente desarrollada para mantener los datos y que se encuentren accesibles siempre que sean necesarios.

El almacenamiento de datos se refiere al uso de medios de grabación para conservar los datos utilizando PC y otros dispositivos. “Las formas más frecuentes de almacenamiento de datos son el almacenamiento de archivos, el

almacenamiento en bloque y el almacenamiento de objetos, cada uno de los cuales resulta adecuado para un fin diferente.”¹¹

Existen formas de guardar la información personal como lo puede ser los ordenadores donde se puede almacenar la información en ficheros, teléfonos móviles que contienen gran cantidad de información personal, se puede también llevar almacenamiento a otras herramientas en línea como son los almacenamientos de la nube, Google Drive, One Drive, Dropbox entre otros que ofrecen almacenamiento, existen herramientas de nube de datos personales como el proyecto “HAT” (Hub of All Things), u otras herramientas de nube de datos personales que permite almacenar la información personal.

2.4. Identidad única

“La Identidad Digital certifica que una persona es quien dice ser. Que la persona o el dispositivo que pide acceso a un servicio, o lo proporciona, es la persona autorizada para hacerlo.”¹²

Actualmente en la Unión Europea ha estado investigando como implementar una identidad digital única certifique y de confianza de las partes que están realizando cualquier tipo de transacción.

En el año 2014 inicia Electronic Identification, Authentication and trust services eIDAS por sus siglas en inglés, eIDAS significa Identificación Electrónica, Autenticación y Servicios de Confianza. El Reglamento eIDAS estableció el marco para garantizar que las interacciones electrónicas entre

¹¹ Hpe. *Almacenamiento*. <https://www.hpe.com/es/es/what-is/data-storage.html#:~:text=El%20almacenamiento%20de%20datos%20consiste,accesibles%20siempre%20que%20sean%20necesarios>. Consulta: 8 de agosto de 2021.

¹² Igaleno. *Identidad digital única*. <https://www.igaleno.com/blog/identidad-digital-unica/>. Consulta: 8 de agosto de 2021.

empresas sean más seguras, rápidas y eficientes, sin importar el país europeo en el que se lleven a cabo. Es un Reglamento europeo que creó un marco único para la identificación electrónica (eID), y los servicios de confianza, lo que facilita la prestación de servicios en toda la Unión Europea.

2.5. Nube de datos personales

Hay muchas soluciones de nube personal existentes que se incluyen en esta categoría. Dentro de los cuales se puede mencionar -Digi.me-, Nextcloud, CozyCloud entre otros, también hay programas de gobiernos de diferentes países como lo puede ser MesInfos.fings.org, My Data.

Todas estas herramientas ofrecen a sus usuarios la capacidad de almacenar sus datos personales en un servidor central gestionado por el proveedor. Los usuarios pueden acceder a sus datos a través de internet.

Las características más importantes de estos softwares son:

Recolección de Datos. Las soluciones citadas anteriormente ofrecen la posibilidad de recopilar automáticamente los datos personales de los usuarios de las empresas y administraciones que los albergan. Esta es posible gracias a las iniciativas de divulgación inteligente (por ejemplo, el botón azul y verde, MyStudentData, entre otros en los EE. UU.), y nuevas regulaciones como el GRDP en Europa.

Los recopiladores de datos utilizan las credenciales de los usuarios para conectarse a los servicios en línea y obtener las últimas actualizaciones para el propietario de la nube personal.

Almacenamiento confiable. Dentro de la infraestructura del proveedor de la nube, los datos de los usuarios están compartidos, y los usuarios solo pueden acceder y realizar cálculos con sus propios datos. Esta separación lógica garantiza un almacenamiento confiable. Algunas soluciones permiten el almacenamiento de los datos cifrados de los usuarios en diferentes ubicaciones en lugar de en el servidor del proveedor queda un mayor nivel de protección.¹³

2.6. Plataformas de Identidad

Las plataformas de identidad permiten establecer una identidad única y dan la posibilidad a las aplicaciones lean y escriban varios datos en un nodo, esto le garantiza al usuario administrar y controlar el flujo de la información.

Entre los proyectos más importantes de plataformas de Identidad están:

Solid (Social Linker Data por sus siglas en inglés), es una especificación que permite a las personas almacenar sus datos de forma segura en almacenes de datos descentralizados llamados Pods.

Los pods son como servidores web personales seguros para datos. Cuando los datos se almacenan en el Pod de alguien, controlan qué personas y aplicaciones pueden acceder a ellos, cualquier cosa se puede almacenar en un Pod desde datos estructurados hasta archivos normales que se pueden almacenar en carpetas de Google Drive o Dropbox, en cualquier momento la personas pueden revocar el acceso.

El Proyecto Solid está liderado por el Profesor Tim Berners-Lee que es el inventor de la World Wide Web, y continuamente se hacen reuniones con la comunidad para avanzar en este proyecto puede ver más de las reuniones y eventos en el siguiente enlace: <https://solidproject.org/events>.

¹³ Secure Distributed Computations for the Personal Cloud (inria.fr) Secure Distributed Computations for the Personal Cloud. *Almacenamiento confiable*. Online Personal Clouds. <https://hal.inria.fr/tel-03220376v1/document>. Consulta: 15 de agosto de 2021.

Hub-of-All-Things(HAT por sus siglas en inglés) El microservidor HAT es una tecnología avanzada nativa de la nube que confiere plenos derechos legales de datos personales a las personas a través de su propiedad de un servidor de datos personales.

El microservidor HAT está alojado en la nube, pero es totalmente portátil entre sistemas en la nube. Las personas pueden conectarse con aplicaciones para traer sus datos desde cualquier otro lugar de Internet, realizar transacciones con sus datos con aplicaciones e instalar herramientas para tener análisis y algoritmos privados para obtener información sobre sus datos, su salud, su historial y sus recuerdos.

El código técnico HAT es totalmente de código abierto, pero su implementación en la nube es parte de la infraestructura de transacciones y cuentas de datos personales pendientes de patente de Dataswift.

Este es uno de los proyectos más avanzados de la Universidad de Cambridge, este ecosistema se basa en único servidor que tiene muchos microservicios internos.

2.7. Diferencias entre nube de datos personales y plataformas de identidad

Las principales diferencias entre la nube de datos personales y plataformas de identidad es que las primeras están un poco más maduras y existen muchas opciones como se vio en la presente investigación en el inciso 2.5, las nubes personales han evolucionado actualmente y permiten archivos con o sin formatos y dan la facilidad para intercambiar información, pero una de las deficiencias que no solucionan es que la información se encuentra

segregada en diferentes plataformas por ejemplo si se registra en una red social nueva se tendrá que volver a registrar todos los datos personales nuevamente, y esto aplica a cualquier otro sistema nuevo que se quiera utilizar y se necesite estar registrado.

Es allí donde radica la diferencia con las plataformas de Identidad que estas lo que prometen es que los datos se concentren en un nodo y puede ser descentralizado como indica el proyecto solid donde las aplicaciones puedan consultar la información así estará informado de que aplicaciones están accediendo o escribiendo la información personal lo cual es un proyecto muy prometedor en cuanto a la privacidad de datos personales.

3. ¿QUE ES -DIGI.ME-?

-Digi.me- es un ecosistema global de datos personales. “Esto permite a las personas conectarse con organizaciones para compartir sus datos o permitir el acceso a sus datos a cambio de un servicio de valor. Se enfoca en dos cosas principales: enrutamiento de datos y servicios de consentimiento.”¹⁴

Es una plataforma uso compartido privado, que le permite a los usuarios tomar el control de su información personal y a los desarrolladores conectarse a miles de fuentes de una forma en cual se respeta la privacidad del usuario y esta se ajusta al GRDP, a los usuarios les permite tomar una decisión informada sobre si otorgar el consentimiento o no para darles acceso a su información personal a cambio de algún servicio de valor.

Recientemente -Digi.me- fue adquirido por WORLD DATA Exchange, la misión principal es ayudar a hacer un mejor uso de los datos personales, en lo cual promueven formas para que el usuario pueda tomar el control de sus datos.

Provee herramientas y una fácil implementación en lenguajes de programación como Android, IOS, y node js, para que sea más fácil a las organizaciones o empresas añadirlos en sus plataformas de tecnología actuales fácilmente.

¹⁴ insider-trends. *How is digi-me pioneering a new approach to personal privacy.* <https://www.insider-trends.com/how-is-digi-me-pioneering-a-new-approach-to-personal-privacy/>. Consulta: 10 de julio de 2020.

3.1. Características de -Digi.me-

La plataforma -Digi.me- provee un conjunto de servicios para que se pueda integrar fácilmente a los proyectos y ayudar a crear excelentes experiencias utilizando datos personales y uso compartido privado, sus principales características son:

Conexión: se incorpora fácilmente a sus aplicaciones los datos personales que sus usuarios han generado en otros lugares, se puede encontrar más información sobre las fuentes disponibles en el este enlace: <https://-Digi.me-/comprehensive-data-sources>.

Consentimiento: se debe dar a conocer al usuario a que información se va acceder y obtener su consentimiento explícito e informado, existe un flujo de consentimiento y se puede encontrar más información en: <https://-Digi.me-/feature-consent>.

Almacenamiento: es una forma segura para almacenar datos personales que se generen para los usuarios, se puede solicitar un consentimiento adicional para utilizar estos datos de otras formas.

Combinación: se pueden obtener los datos que se recopilan de cada API de servicio en su formato original o normalizarlos a un esquema usando estándares comunes, lo que garantiza que siempre se almacene en un formato coherente, puede encontrar más información en el enlace:

<https://developers.-Digi.me-/docs/references/service-groups>.

Sin Código: una solución para recibir datos de los usuarios de forma fácil sin la necesidad de implementarlo en un sistema es decir sin escribir una línea de código se puede utilizar playground que es una herramienta que provee -Digi.me- que permite solicitar información de las principales redes sociales.

3.2. Funciones de -Digi.me-

El ecosistema global de datos personales -Digi.me- presenta a continuación, sus funciones.

3.2.1. -Digi.me- Connect

Una de las principales funciones es -Digi.me- Connect donde se puede solicitar acceso a gran parte de la información de sus clientes, hay una gran cantidad de fuentes de datos y si como organización se quiere compartir información con -Digi.me- connect se puede poner en contacto con el equipo de desarrollo para que puedan configurar y estandarizar la información que se compartirá.

3.2.2. Acceso a datos con consentimiento de usuario

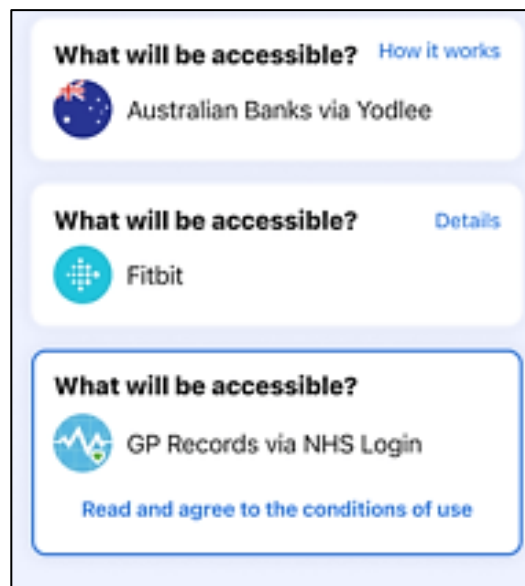
Puede tener acceso a muchas fuentes de datos con el consentimiento del usuario, esto le ayuda a crear una confianza entre la organización o empresa con el usuario, ya que le solicitará la información con consentimiento explícito e informado de sus clientes al establecer claramente que información se necesita y qué sucederá con ella, todo esto mediante una misma API.

3.2.3. Contrato de consentimiento

La pantalla que provee -Digi.me- es una de las más informativas y flexibles disponibles en la actualidad, la clave del consentimiento es informar claramente al usuario por qué desea su información y también debe especificar cómo la utilizará, los puntos importantes que debe mostrar al usuario es:

¿Por qué? aquí debe comunicar de manera clara la conexión y el intercambio de los datos de una fuente, dependiendo de cómo lo decida la fuente el usuario, deberá tomar medidas adicionales, puede solicitar el contrato de consentimiento en el enlace: <https://-Digi.me-/request-contract>.

Figura 1. Detalle de ¿por qué?



Fuente: -Digi.me-. *What will be accessible?* <https://-Digi.me-/feature-consent>.

Consulta: 22 de agosto de 2022.

¿Cómo lo hará? Debe definir como tratará los datos de sus clientes utilizando, en todo momento el cliente puede leer más acerca de cada una de las declaraciones.

Figura 2. ¿Cómo lo hará?



Fuente: -Digi.me-. *what will happen to it?* <https://-Digi.me-/feature-consent>.

Consulta: 22 de agosto de 2022.

Consentimiento: -Digi.me- ha diseñado el botón de consentimiento con deslizamiento esto para garantizar que el cliente está dando su consentimiento y no quepa duda que lo haya hecho de forma accidental.

Figura 3. **Dar consentimiento**



Fuente: -Digi.me-. *Give consent*. <https://-Digi.me-/feature-consent>.

Consulta: 22 de agosto de 2022.

Es importante informar que el usuario tiene derecho a retirar su consentimiento si por alguna razón cambia de opinión.

Cuando haya dado el consentimiento para la recopilación, el procesamiento y la transferencia de los datos personales para un propósito específico (por ejemplo, en relación con el marketing directo que ha indicado que le gustaría recibir), tiene derecho a retirar el consentimiento.

Para ese procesamiento específico en cualquier momento. Para retirar el consentimiento, envíe un correo electrónico a DPO (@) -Digi.me-.

3.2.4. Plataforma -Digi.me- en dispositivos móviles

-Digi.me- ofrece dos plataformas en dispositivos Android y IOS en las cuales se explica más a detalle en el enlace a continuación: <https://-Digi.me-/demo>.

3.2.4.1. -Digi.me- Data Viewer

Esta aplicación se puede encontrar en las tiendas de Google Play y App Store con el nombre de -Digi.me-, recientemente tuvo una actualización importante ya que no necesita registrarse ni tampoco acceder con clave y contraseña para crear su biblioteca de datos personales.

Otra característica que cambió es que ya no se almacena en almacenamiento de tercero como Google drive, Dropbox u otro almacenamiento de tercero, sino que se almacena en la propia plataforma de -Digi.me- garantizando más seguridad y accesibilidad a dicha información, para utilizarla lo que debe hacer es descargar la aplicación y luego puede conectar a las fuentes de datos, como es Facebook, Twitter y muchas fuentes más, luego puede visualizar la información hacer búsquedas o exportar su información en formato JSON.

3.2.4.2. PostCleaner

Esta es otra de las aplicaciones que puede encontrar en las tiendas de Google Play y App Store con el nombre de PostCleaner esta aplicación le solicita que se conecte con una fuente de datos de aplicaciones de redes sociales como Facebook, Twitter, Instagram, lo que hace esta aplicación es escanear todas sus publicaciones y las compara con más de 3000 palabras o

frases que pueden ser ofensivas, identifica los post y es el usuario quien decide si debe mantenerlos eliminarlos.

3.2.5. Playground -Digi.me-

Otra funcionalidad que ofrece -Digi.me- es su playground esto le permite que las personas comportan rápidamente sus datos personales con organizaciones u empresas, puede descargar los datos compartidos para analizarlos utilizando sus propias herramientas de análisis o simplemente con Microsoft Excel, esta herramienta la puede utilizar sin la necesidad de escribir una línea de código esto se amplía más en el capítulo 4.

3.3. Política de privacidad -Digi.me-

En -Digi.me-, se entiende que se tiene la responsabilidad de cuidar los datos, proteger y respetar la privacidad. “La aplicación -Digi.me- no requiere que el usuario se registre para usar la aplicación y, por lo tanto, de forma predeterminada, la empresa no conoce la información de identificación personal del usuario (nombre, dirección de correo electrónico, etc.)”¹⁵

-Digi.me- se toma muy en serio la política de privacidad de datos de sus usuarios, sus principales funciones están en informar a los usuarios que está sucediendo con su información, es por eso que a continuación se detallan partes importantes del contrato de privacidad de -Digi.me- y también puede servir de ejemplo de cómo se puede definir los contratos de privacidad de los sistemas o servicios de información.

¹⁵ -Digi.me-. *Recopilación de información*. <https://-Digi.me-/privacy-policy>. Consulta: 9 de septiembre de 2022.

3.3.1. Como recopilan la información

Se obtienen datos personales de los usuarios cuando, por ejemplo, se realizan las siguientes actividades:

- Suscríbase a nuestros boletines de usuarios, empresas o socios;
- Regístrese como usuario beta, probador, únase a nuestro programa interno o use Apple Testflight;
- Envíenos un informe de error a través de Instabug u otro sistema de informes o envíe un ticket de soporte a través de Freshdesk u otro sistema de soporte;
- Completar formularios en nuestro sitio web;
- Participar en un concurso, promoción o encuesta;
- Asistir a un hackathon u otro evento;
- Solicitar más información de nosotros con respecto a los servicios que brindamos;
- Contáctenos por correo electrónico, correo postal, teléfono o redes sociales;
- Tener una relación comercial con nosotros como cliente, proveedor, asesor comercial, consultor u otro proveedor de servicios;
- Al hacer una solicitud de empleo.¹⁶

En cualquier plataforma de tecnología que se desarrolle y se tenga la necesidad de recopilar información del usuario, es importante que se le dé a conocer como se está recopilando la información, en este caso particular - Digi.me- detalle de forma clara que información está recopilando.

3.3.2. Tipos de datos recopilados y conservados

Los datos que se recopilaron y se conservan pueden incluir:

- Sus datos personales, como su nombre, dirección, dirección de correo electrónico, números de teléfono, información de pago, dirección IP, etc.;
- Su historial profesional u otros datos si está realizando una solicitud de empleo;
- Información sobre su uso de la aplicación -Digi.me-, datos de sesión, etc.;
- Cualquier comunicación que haya tenido lugar entre nosotros;

¹⁶ -Digi.me-. *Recopilación de información*. <https://-Digi.me-/privacy-policy>. Consulta: 9 de septiembre de 2022.

- Detalles de contacto que hemos tenido con usted con respecto a la prestación real o propuesta de servicios para usted o de usted;
- Detalles de cualquier servicio que haya recibido de nosotros o que nos haya brindado;
- Información sobre cualquier queja y consulta que nos haya hecho o que nosotros le hayamos hecho.¹⁷

Es importante dejar claro al usuario que tipos de datos son los que estarán guardando, debe quedar de forma explícita para que cualquier usuario sepa con exactitud los datos que están quedando almacenados, esto genera mayor confianza en la interacción que se tenga con los sistemas.

3.3.3. Como se utilizarán sus datos

Se usa información de las siguientes maneras:

- Para procesar consultas, confidencialidad u otros acuerdos o pedidos que nos haya enviado o que nosotros le hayamos enviado o para la ejecución de cualquier contrato que tengamos con usted o usted con nosotros;
- Para cumplir con nuestras obligaciones legales y cualquier obligación contractual que tengamos con usted;
- Para proporcionarle productos y servicios;
- Para permitirnos revisar y mejorar nuestro sitio web, aplicaciones y servicios;
- Para proporcionar atención al cliente, incluida la respuesta a sus solicitudes de soporte;
- Para administrar cuentas de acreedores o deudores y procesar y rastrear pagos;
- Para llevar a cabo análisis estadísticos y de marketing o donde busquemos sus pensamientos y opiniones sobre los servicios que brindamos;
- Para notificarle sobre cambios en nuestro sitio web, términos y condiciones, servicios o precios;
- Para procesar solicitudes de empleo;
- Para proporcionarle información sobre nuestros productos y servicios que nos solicita o que creemos que pueden ser de su interés, siempre que haya dado su consentimiento para ser contactado para tales fines.¹⁸

¹⁷ -Digi.me-. *Recopilación de información*. <https://-Digi.me-/privacy-policy>. Consulta: 9 de septiembre de 2022.

¹⁸ -Digi.me-. *Recopilación de información*. <https://-Digi.me-/privacy-policy>. Consulta: 9 de septiembre de 2022.

Al aclarar de qué forma utilizará sus datos, el usuario tendrá certeza de cómo se procesará su información en los sistemas de -Digi.me-, se debe dejar claro para que los usuarios tengan conocimiento de cómo se está utilizando su información.

3.3.4. Conservación de datos

Solo se conservarán los datos personales durante el tiempo que sea necesario para cumplir con los fines para los que se recopilan.

Al evaluar qué período de retención es apropiado para los datos personales, se toma en consideración:

- Los requisitos de nuestro negocio y los servicios que le brindamos y los servicios que nos brinda;
- cualquier obligación estatutaria o legal;
- los fines para los que recopilamos originalmente los datos personales;
- los motivos legales en los que basamos nuestro procesamiento;
- los tipos de datos personales que hemos recopilado;
- la cantidad y categorías de sus datos personales; y
- si el propósito del procesamiento podría cumplirse razonablemente por otros medios.

Es posible que necesitemos conservar sus datos hasta 7 años después de que finalice cualquier acuerdo comercial para cumplir con nuestras obligaciones legales, fiscales o contables.¹⁹

El tiempo que se conservara la información debe ser del conocimiento del usuario para que, de su consentimiento, pero sobre todo que este informado porque está conservando su información debe tener una razón, como las definidas anteriormente.

¹⁹ -Digi.me-. *Recopilación de información*. <https://-Digi.me-/privacy-policy>. Consulta: 9 de septiembre de 2022.

3.4. Protocolos de Seguridad -Digi.me-

-Digi.me- Utiliza estándares de cifrados líderes en la industria conocidos como AES-256, que significa para el Estándar de cifrado avanzado del Instituto Nacional de Estándares y Tecnología de EE. UU., y “utiliza claves de 256 bits, que determina la complejidad matemática (por lo tanto, tiempo, costo y esfuerzo) de romper el cifrado archivo.”²⁰

En los sistemas información se debe conocer los diversos métodos de encriptación de datos esto para prevenir futuras eventualidades o ataques que sufran los mismos, al estar encriptados garantiza que, aunque el atacante tenga acceso a los mismos no pueda descifrarlos.

3.4.1. Alcance de seguridad

Para definir el alcance de la seguridad para la revisión del cumplimiento en entornos de datos personales, se establece siete principios básicos que se deben cumplir durante todo el diseño y se deben probar en la práctica por medio de análisis intrusivos y validación física agresiva.

Se debe demostrar que un sistema seguro cumple y supera los requisitos principales:

- Protección de almacenamiento: todos los archivos de datos del usuario están cifrados, al menos, con los estándares bancarios y el algoritmo AES-256. Esto debe usar individual cifrado de archivos además de cualquier cifrado proporcionado por la propia tecnología de almacenamiento (es decir, almacenamiento en la nube). Para prevenir una sola clave de descifrado para desbloquear todos los datos, debe haber claves separadas para cada archivo.

²⁰ Dr. GAVIN, Ray. *Documento Securing Personal Data*. <https://-Digi.me->. Consulta: 27 de agosto de 2021.

- Autenticación y autorización: todos los componentes de software que manejan datos de usuario (aplicaciones, sistemas y servicios integrados) deben poder demostrar su procedencia, generalmente con un certificado criptográfico emitido por una parte de confianza e imposible de falsificar. Estas las credenciales deben estar completamente protegidas cuando no estén activas y deben indicar el alcance de la autorización del software para actuar según los instrumentos comerciales, legales o reglamentarios acordados.
- Protección de datos en tránsito: todos los datos del usuario deben estar protegidos en tránsito mediante conexiones cifradas con autenticación del remitente y el receptor, no hay opción para la interlocución por parte de malos actores capaces de falsificar credenciales o explotar las debilidades en los estándares públicos de Internet o software publicado.
- Anti invasión: el sistema debe estar protegido contra la fuerza bruta, la invasión encubierta y la explotación de cualquier vulnerabilidad conocida. En componentes de software públicos utilizados en la construcción de cualquiera de las aplicaciones o sistemas de procesamiento en la nube.
- Anti falsificación: todos los datos y credenciales del sistema deben ser verificables para evitar su falsificación.
- Cadena de confianza: todos los datos que ingresan al sistema deben poder demostrarse como inalterados desde el primer punto de entrada, moviéndose entre intermedios almacenamiento, servicios de tránsito y eventuales destinatarios.
- Integridad: todos los códigos, sistemas y funciones deben poder demostrarse como originales y estar contruidos a partir de fuentes verificables para garantizar la infiltración del sistema y la corrupción por parte de malos actores no pueden ocurrir.²¹

Los 7 principios anteriormente descritos establecen de forma clara como protege -Digi.me-.

La información, también da un panorama de cómo se debe manejar la información en los sistemas de información para garantizar la seguridad de la misma.

²¹ Dr. GAVIN, Ray. *Documento Securing Personal Data*. <https://-Digi.me->. Consulta: 27 de agosto de 2021.

3.4.2. Diseño de seguridad

La plataforma de gestión de privacidad -Digi.me- se basa en modelos de diseño derivados de la experiencia de los arquitectos de seguridad. Asesorar y validar sistemas financieros, de grandes empresas y gubernamentales.

La entrega del sistema es continuamente monitoreada por ataques deliberados diseñados para emular a los del mundo real y para garantizar la seguridad establecida se mantienen los niveles.

Para probar que un sistema es seguro, hay un conjunto de principios básicos y elementos críticos que deben aparecer en todos los sistemas activos. La lista a continuación muestra cómo todo el flujo de datos y todos los componentes dentro del el flujo debe estar asegurado y validado. Vale la pena verlos resumidos para comprender el alcance completo de un sistema. Validación y cómo -Digi.me- alcanza los estándares requeridos:

- Almacenamiento: los datos, cuando se almacenan, deben cifrarse con un algoritmo sólido y probado en el que, por lo general, el costo del ataque es mayor. que el valor de los datos. AES-256 es el estándar actual y líder del sector bancario y de la salud.
- Almacenamiento: cuando los datos se almacenan en un servicio en la nube (como Microsoft Azure, AWS, etc.) aunque puedan ser cifrados por el proveedor, debe tener doble cifrado para garantizar que el compromiso del proveedor no comprometa los datos del usuario.
- Almacenamiento: todos los archivos de datos se cifran individualmente para garantizar que descifrar el cifrado una vez, para un archivo, no abra todos los archivos de datos al acceso inmediato.
- Autenticación: dondequiera que se almacenen las credenciales de usuario para acceder a sus datos remotos, deben estar encriptadas al máximo estándar para evitar la ingeniería inversa.
- Autenticación: dondequiera que el sistema se conecte a aplicaciones de terceros, debe autenticar que el tercero es la entidad.

- Autorización: siempre que un usuario o una aplicación de terceros se conecte al sistema, solo debe realizar solicitudes autorizadas que puedan ser irrefutablemente validado y no falsificado.
- Datos en tránsito: todos los datos, cuando se transmiten, deben estar cifrados y las claves de cifrado protegidas y validadas.
- Autenticación de datos en tránsito: cuando se transmiten datos, debe probarse que cada parte se ha identificado de manera única.
- Validación de datos en tránsito: cuando se transmiten datos, no debe ser posible que un "intermediario" se haga pasar por un destinatario autorizado. o entidad de tránsito de los datos del usuario.
- Invasión: en cada punto de un sistema no debe haber ningún medio para que un tercero no autorizado acceda a los datos del usuario o falsifique credenciales para obtener acceso, lo que se conoce como interdicción. Esto significa proteger los sistemas operativos, su memoria, su procesamiento, sus funciones de transmisión y su almacenamiento.
- Falsificación: cuando se almacenan o comparten datos del usuario, un interlocutor no debe poder modificar los datos en ningún lugar de las aplicaciones móviles / de escritorio, a través de las redes o dentro de cualquiera de los servicios de procesamiento, uso compartido o almacenamiento en la nube.
- Cadena de confianza: cuando los datos han entrado en el "sistema", debe poder demostrarse que los datos no se han modificado durante el almacenamiento o tránsito desde el primer punto de entrada.
- Integridad de la fuente: cuando el software está escrito para ejecutar las funciones del sistema, debe poder demostrarse que el código proviene de fuentes "confiables" y no comprometido.
- Integridad de la versión: donde el software está escrito para ejecutar las funciones del sistema, debe poder demostrarse que la versión implementada es la versión escrita según lo previsto y no modificado por malos actores.
- Prueba: donde el sistema promulga comandos y mueve datos, debe haber una prueba de actividad para fines de auditoría.
- Privacidad: donde el sistema ejecuta comandos y mueve datos, debe haber certeza de que no hay datos de usuario o artefactos de privacidad. permanecer dentro del sistema.²²

²² Dr. GAVIN, Ray. *Documento Securing Personal Data*. <https://-Digi.me->. Consulta: 27 de agosto de 2021.

En los 17 puntos determina como -Digi.me- asegura todo el flujo de datos y los elementos que lo componen, también da significado de que elementos debe tener un software sólido para dar confianza en su diseño de seguridad de la información.

Esta plataforma debe asegurar los datos ya que son datos sensibles por ejemplo los contratos electrónicos y eventos de registro que muestran cuando se crea un contrato, cuando el usuario acepta y se promulga, los contratos deben estar protegidos para que no se puedan falsificar o modificar, hay que considerar la profundidad de protección que ofrece.

Debe tomarse en cuenta que un sistema debe ser seguro como servicio y -Digi.me- ha estado trabajando durante años en sistemas de ingeniería de privacidad más avanzados y mejorando sus prácticas.

3.5. Acreditaciones y certificaciones

-Digi.me- cuenta con varias acreditaciones en las cuales se describirán continuación, es importante aclarar que las acreditaciones significan que los sistemas cumplen con los procesos y estándares rigurosos avalado y auditados por diferentes organismos encargados en otorgar cada uno de las certificaciones, esto permite dar confianza en los diferentes países, gobiernos, organismos de la industria y de cómo realizan las regulaciones y uso de datos.

3.5.1. ISO 27001:2013 e ISO 27017:2015

Acreditado para cumplir con estos estándares ISO relacionados con: “el desarrollo y la provisión de una plataforma de gestión de datos personales y el

soporte continuo que permite a los consumidores de todo el mundo compartir datos personales de forma privada y segura.”²³

3.5.2. NEN 7510

“Este estándar de atención médica holandés para la seguridad de la información se basa en ISO 27001: 2013 y el NEN 7510 cumple con tres nuevos criterios adicionales específicos de datos de salud.”²⁴

3.5.3. Medmij

“El estándar MedMij permite a los ciudadanos holandeses obtener control sobre sus datos de atención médica, a través de sistemas de atención médica personal. Los proveedores de servicios certificados también deben tener una acreditación NEN 7510.”²⁵

3.5.4. Cyber Essentials

El Centro Nacional de Seguridad Cibernética brinda certificaciones respaldadas por el gobierno a organizaciones que han demostrado los niveles de protección requeridos contra amenazas comunes en línea.

²³ ISO 27001:2013 - 27017:2015. *Plataforma de gestión de datos personales*. <https://-Digi.me-/accreditations>. Consulta: 21 de septiembre de 2021.

²⁴ NEN 7510. *Estándar de atención médica holandés para la seguridad*. <https://-Digi.me-/accreditations>. Consulta: 21 de septiembre de 2021.

²⁵ MedMij. *Estándar MedMij*. <https://-Digi.me-/accreditations>. Consulta: 25 de septiembre de 2021.

3.5.5. Estado de los operadores de MyData 2020

-Digi.me- se enorgullece de recibir el estatus de MyData Operators 2020 en reconocimiento a la operación de infraestructura centrada en el ser humano para la gestión y el intercambio de datos personales.

Es importante destacar que todas las acreditaciones que posee -Digi.me- han sido auditadas y ha obtenido sus respectivas certificaciones por los diferentes organismos anteriormente descritos, lo que da mayor valor y seguridad de lo que realmente protege la plataforma privacidad como su principal oferta.

3.6. Beneficios para los usuarios

Cuando se utiliza -Digi.me- como una biblioteca privada de datos garantiza beneficios para el usuario, y es que no solo se vuelve algo transparente la forma en que el usuario se empodera con la información, los beneficios son:

- **Compartir datos a cambio de servicios de valor:** al compartir los datos a través de la plataforma de privacidad -Digi.me- permite a los usuarios que la organización o empresa que desea acceder a los mismos le dé un servicio a un menor costo, o su servicio sea más personalizada por proveer la información con su consentimiento.
- **Control de datos y transparencia:** con los flujos previamente establecidos por parte -Digi.me- provee mayor control de los datos puesto que están destinados a cuidar la privacidad de los usuarios, incluso con las funciones descritas en el capítulo 3.3 detallan las herramientas que puede emplear el usuario provee días por -Digi.me-, también le da control

a que en cualquier momento solicitar al equipo de -Digi.me- que pueda eliminar algún contrato, cuando sienta que sus derechos fueron vulnerados, es importante señalar que se apega al reglamento de GRDP.

- Seguridad en el resguardo de su información: -Digi.me- cuenta con una trayectoria en la protección de datos como se amplió en el capítulo 3.5 y también con diversas acreditaciones por lo que el usuario puede sentirse seguro de cómo será tratada su información, y el equipo de -Digi.me- autoriza a las empresas u organizaciones que cumplan con ciertos criterios para autorizar el acceso a la información del usuario, como la forma en que deben elaborar dichos contratos.

3.7. Beneficios para las organizaciones o empresas

Las empresas pueden obtener grandes beneficios al utilizar -Digi.me- porque les permite obtener datos personales directamente del usuario con su autorización, además de todas las características y herramientas que le provee -Digi.me- para implementarlos en sus sistemas de información, incluso sin escribir código utilizando playground.

Algunas características del uso compartido para obtener datos son:

- Es una de las formas seguras y éticas para el acceso a datos valiosos de usuarios consentidos con su aplicación o empresa.
- Utilizar una única API para conectarse a miles de fuentes: les permite acceso a datos enriquecidos armonizados de los usuarios, con -Digi.me- fácilmente se puede integrar y normalizar las fuentes de datos mientras la empresa se concentra en como innovar su aplicación.

- Consentimiento del usuario: al solicitar la información directamente del usuario le ayudará aumentar la confianza y obtener el consentimiento informado de sucederá con sus datos.
- Fácil de implementar: con las herramientas que ofrece -Digi.me- al utilizar el SDK no tendrá problemas, porque le ofrece optimizar y estandarizar la información si desea obtener información de fuentes de datos distintas.

4. UTILIZACIÓN DE -DIGI.ME-

4.1. Definición del problema

cuando se desarrollan nuevas plataformas de tecnología en ocasiones es necesario acceder a la información personal del usuario que esta almacenada en otras plataformas estas pueden ser redes sociales, plataformas médicas entre otras.

Una forma de solucionar es utilizando el SDK de -Digi.me- que ofrece herramientas para que el usuario de su consentimiento y tenga presente quien está accediendo a su información de forma clara y de qué forma se utilizará la misma.

Para esta investigación se aborda el uso de playground para extraer información del usuario con su consentimiento en algunas plataformas de redes sociales populares y también la implementación del SDK en una aplicación en Android donde puede escribir y leer información.

4.2. Uso de playground -Digi.me-

Para utilizar el playground en -Digi.me- se deben seguir los pasos.

- Registrarse en este proceso solicita de la información:
 - nombre
 - correo electrónico

- contraseña

Figura 4. **Agregar playground -Digi.me-**

Playground Home

Welcome to digi.me Playground!

Use Playground to get people to quickly share personal data with you. **Sign up** below, share your unique link, and then download data that has been shared with you so you can analyze it using your own analytics tool(s), or Microsoft Excel.

Sign up Log in Demo

Full name
Enter your full name

Work email
Enter your work email address
We will NOT share your email with anyone else.

Password
Choose a password

Confirm password
Confirm your password

Sign Up

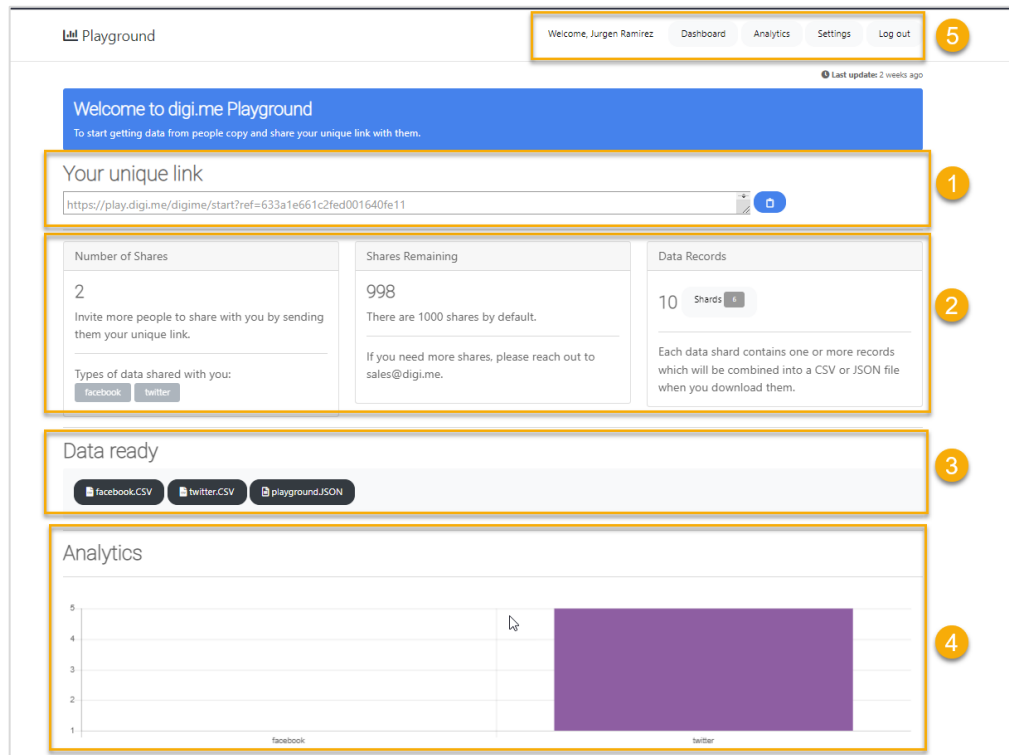
© 2022 Digi.me Ltd - All Rights Reserved

Fuente: play.-Digi.me-. *Playground en -Digi.me-*. <https://play.-Digi.me/>.

Consulta: 22 de septiembre de 2022.

- Ingresar a la plataforma: posterior a registrarse se procede a ingresar a la plataforma <https://play.-Digi.me/>
- Dashboard: una vez que se ha ingresado exitosamente a la plataforma se puede visualizar lo que aparece a continuación en la figura 5.

Figura 5. Dashboard



Fuente: play.-Digi.me-. *Dashboard*. <https://play.-Digi.me/>.

Consulta: el 22 de septiembre de 2022.

- En el apartado 1 se provee un link, en él se puede compartir y solicitará información de redes sociales.
- En el apartado 2 se puede ver la cantidad de personas que han dado su consentimiento para acceder a su información en alguna red social.
- En el apartado 3 se puede descargar la data de los usuarios que han concedido permiso para acceder al análisis de su información en formatos .csv o JSON.

- En el apartado 4 muestra una analítica de la información que han compartido los usuarios.
- El apartado 5 es un menú el cual se puede seleccionar Dashboard, Analíticas, configuraciones y cerrar sesión.

Figura 6. **Configuraciones**

The screenshot displays the 'Configuraciones' (Settings) page in the 'Playground' application. The page header includes the application name 'Playground', the user name 'Welcome, Jurgen Ramirez', and navigation links for 'Dashboard', 'Analytics', 'Settings', and 'Log out'. The main content area is titled 'Company Information' and contains a text input field with the value 'Facultad de Ingeniería Escuela de Ciencias y Sistemas, Universidad de San Carlos de Guatemala.' Below this is a text area with the prompt 'Describe why they should share with you and what you will do with the data they share.' and the text 'Es para uso exclusivo de proyecto de tesis Jurgen Ramirez.' A blue 'Update information' button is located at the bottom of the form. On the left side, there are three numbered callouts: 1. Company Profile, 2. Company Logo, and 3. Clear Data. The footer of the page reads '© 2022 Digi.me Ltd - All Rights Reserved'.

Fuente: play.-Digi.me-. *Configuraciones*. <https://play.-Digi.me-/>. Consulta: 22 de septiembre de 2022.

- En el apartado 1 de configuraciones se permite colocar información de la organización u compañía que quiere solicitar información al usuario, también se debe añadir una descripción que se le mostrara al usuario al momento de compartir su información.
- El apartado 2 permite colocar un logo, este se mostrará al momento de solicitar información al usuario.

- En el apartado 3 permite eliminar la información que los usuarios han compartido.
- Solicitar información al Usuario.

Quando se solicita información al usuario se comparte el link único para este ejemplo: <https://play.-Digi.me/-/Digi.me-/start?ref=633a1e661c2fed001640fe11>

Figura 7. Solicitar información al usuario

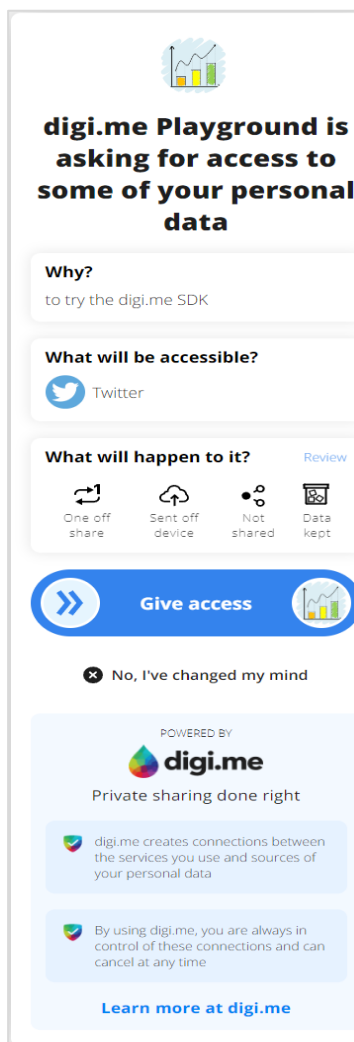


Fuente: play.-Digi.me-. *Solicitar información al usuario*. <https://play.-Digi.me/-/>. Consulta: 22 de septiembre de 2022.

Mostrará una pantalla donde se visualiza el logo y la descripción de la organización previamente configurada en el paso 4.

Se puede seleccionar el servicio de cuales están Facebook, Twitter, Flickr, Instagram. En este caso se seleccionó Twitter, este habilita el botón compartir datos de Twitter utilizando -Digi.me- al dar *click* sobre el botón llevará a la pantalla que se muestra en la figura 8.

Figura 8. -Digi.me- playground autorización



Fuente: play.-Digi.me-. *Playground autorización*. <https://api.-Digi.me-/apps/saas/authorize>.

Consulta: 22 de septiembre de 2022.

En esta pantalla se da el consentimiento del usuario para que -Digi.me- se conecte y extraiga su información de una fuente de datos, se muestra un botón que se puede deslizar, el cual al hacerlo el usuario acepta el contrato para conceder su información.

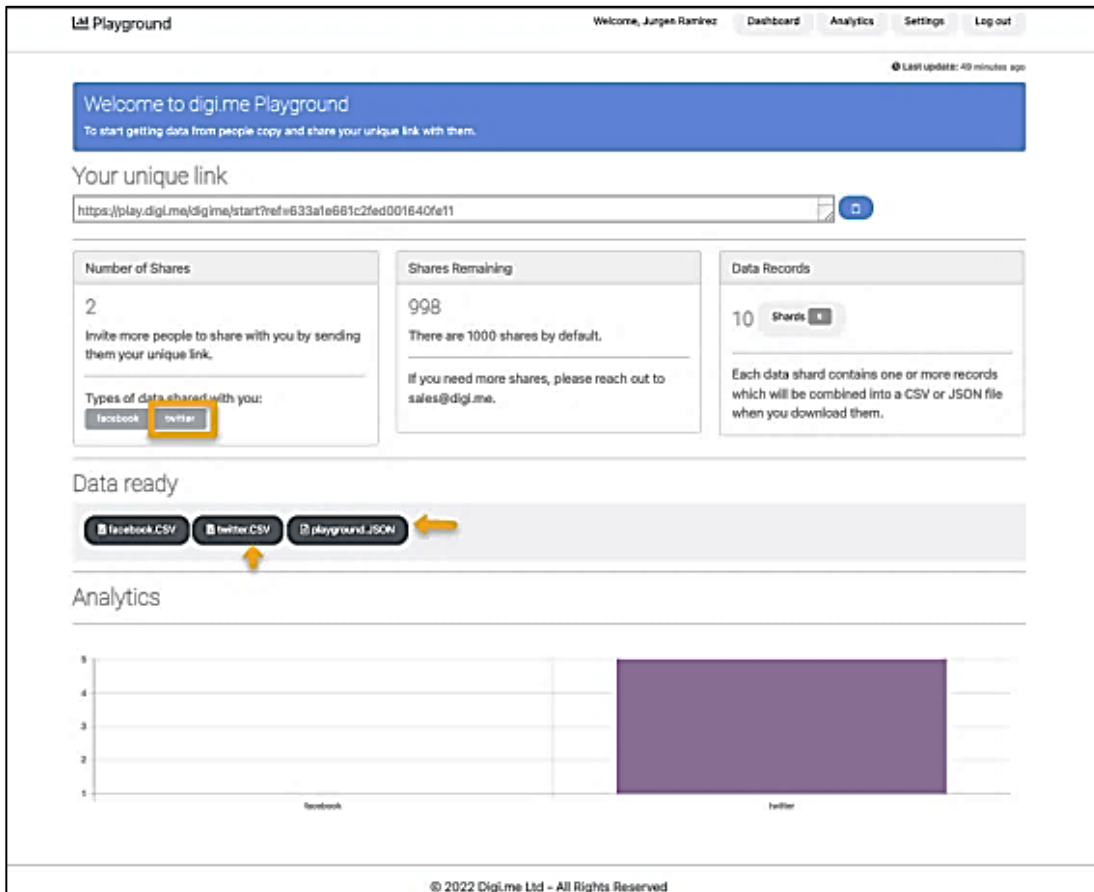
Figura 9. **Autorizar a -Digi.me- a acceder a la cuenta**



Fuente: play.-Digi.me-. *Autorizar a -Digi.me- a acceder a tu cuenta.*
<https://api.twitter.com/oauth/authorize>. Consulta: 22 de septiembre de 2022.

En la ventana que se muestra a continuación pide que se registre a la cuenta de Twitter para darle acceso a -Digi.me- que extraiga la información de la cuenta, al darle en autorizar iniciará el proceso extracción de información, el cual puede durar unos minutos dependiendo de cuanta información tenga la cuenta.

Figura 10. Dashboard -Digi.me- al recibir información del usuario



Fuente: play.-Digi.me-. Welcome to -Digi.me- Playground. <https://play.-Digi.me/>.

Consulta: 22 de septiembre de 2022.

Una vez terminado este proceso aparece en el *dashboard* la información que el usuario dio acceso en formato JSON o CSV, para proceder a descargarlo y procesar la información en otras plataformas.

4.3. Implementación en Android

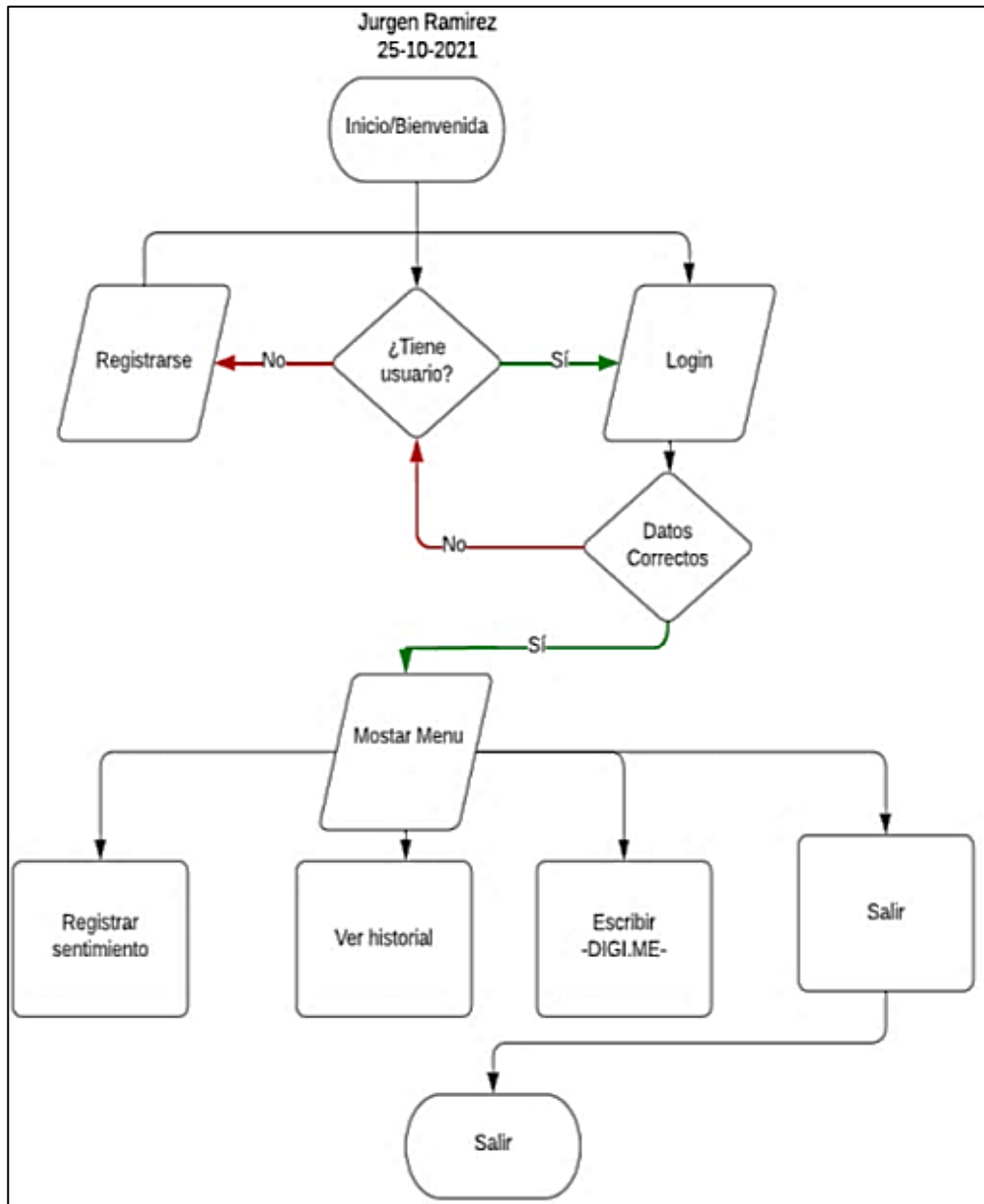
A continuación, se detallan los pasos para implementar el SDK de - Digi.me- en una aplicación desarrollada en Android.

4.3.1. Descripción de la aplicación

Es una aplicación creada en Android versión 12, con dimensiones de pantalla de un teléfono Pixel 6, API 31, la aplicación Feeling App es una aplicación que guarda los sentimientos del usuario (sus estados de ánimo), para posteriormente escribir los datos en -Digi.me-.

- Funcionalidad la aplicación
 - La aplicación cuenta con un interfaz de bienvenida la cual muestra información y un mensaje de bienvenida para el usuario.
 - Dentro del flujo de inicio de sesión pregunta si ya está registrado en la plataforma, si no tiene usuario lo lleva a la página de registro, si ya cuenta con un usuario lo lleva a la página de inicio de sesión o *login*, si los datos son correctos puede registrar sus sentimientos del día, ver su historial, guardar la información en -Digi.me-, cerrar sesión.

Figura 11. Diagrama Flujo de funcionalidad Feeling App



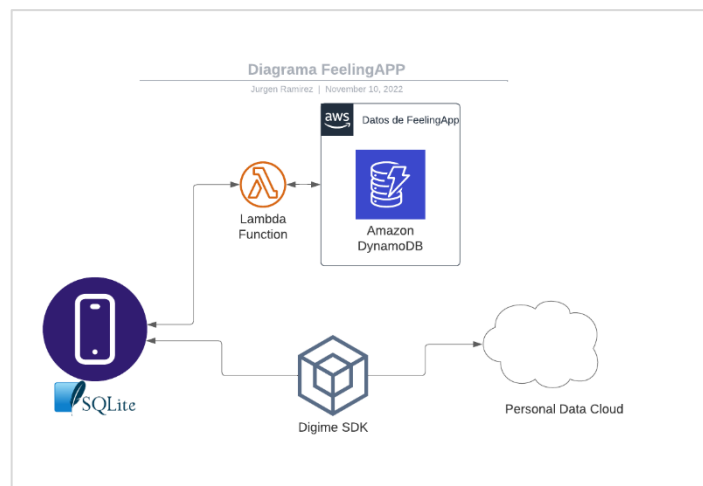
Fuente elaboración propia, empleando Lucidchart.

4.4. Diseño de APP

El diseño de la aplicación integra componentes de la nube de Amazon AWS, los cuales son funciones lambda que interactúan con la base de datos no relacional de Dynamodb.

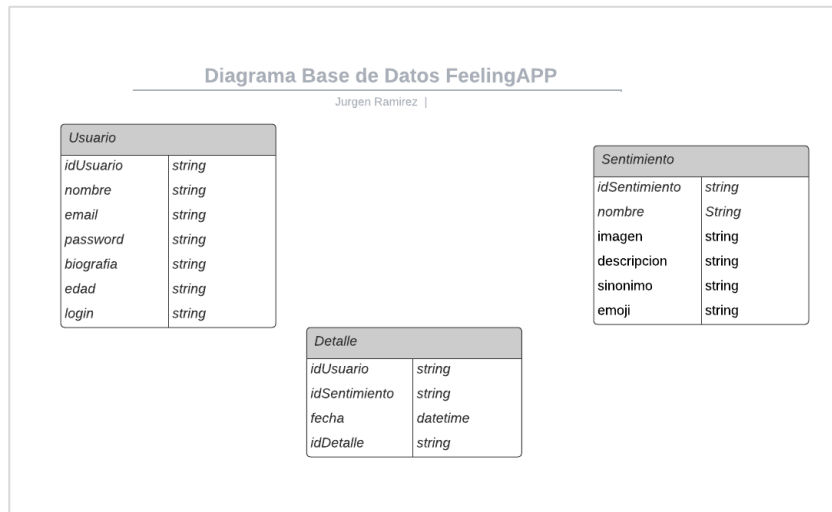
Cuando se realiza el inicio de sesión la información que está en la nube del usuario se almacena una base de datos local de SQLite en el dispositivo Android esto para facilitar el acceso a la información sea más rápido y no depender de las conexiones de red, también tiene la conexión a -Digi.me- utilizando el SDK.

Figura 12. **Diseño de la aplicación Feeling APP**



Fuente elaboración propia, empleando Lucidchart.

Figura 13. Diagrama base de datos Feeling APP



Fuente elaboración propia, empleando Lucidchart.

4.4.1. Configuración de ID e instalación SDK Android

Para configurar el SDK en un proyecto de android se deben seguir los pasos:

- En la página oficial de -Digi.me- se debe llenar un formulario(<https://developers.-Digi.me-/get-app-id>), para obtener las credenciales como lo es AppId y las llaves privadas, si presenta algún problema puede comunicarse por diferentes canales que se proveen (<https://developers.-Digi.me-/support>), alguien del equipo de soporte se pondrá en contacto.

Le proporcionaran un contrato, para acceder a la plataforma -Digi.me-, debe obtener una identificación de la aplicación, así como una identificación de

contrato valida. Estos contratos lo que representan son los datos que se solicitan al usuario, así como detalles sobre los términos de uso.

- En el paso anterior le llegara vía correo electrónico o por otro canal oficial un archivo que contiene AppID, Private Key, Contract ID.

AppID: es código único que identifica a la aplicación dentro de -Digi.me-.
Private Key RSA: es una clave de 256 bits para seguridad de autenticación de la aplicación con la plataforma -Digi.me-.

Contract ID: contiene un código único que identifica el contrato para que la aplicación pueda escribir en la biblioteca privada o leer de alguna otra fuente, estos pueden ser varios dependiendo de las acciones solicitadas, por ejemplo, solicitar las publicaciones en las redes sociales del usuario.

Los proyectos en Android a los cuales se les quiera añadir el SDK de -Digi.me- deben tener algunos requisitos, se puede consultar lo más actualizado en el enlace: <https://developers.-Digi.me-/docs/android-sdk/quickstart>.

- Desarrollo
- -Android Studio 4.2.2 o más reciente
- -Gradle 6.7.1 o posterior
- -Kotlin 1.5.1 o posterior*
- *El SDK está escrito completamente en Kotlin, pero es compatible con proyectos Java.
- Despliegue.
- -Android 5.1 o posterior (nivel de API 21).

Después de realizar los pasos anteriores y cumplir con los requisitos se debe añadir la dependencia de -Digi.me- en el repositorio de su proyecto Android, para verificar la versión más actualizada se puede consultar el enlace <https://developers.-Digi.me-/docs/android-sdk/quickstart>.

- dependencies {
- implementation "me.digi:sdk:4.0.10"
- }

Esto les permitirá a los desarrolladores hacer uso de los datos de usuarios de miles de fuentes de una manera que respeta la privacidad del usuario.

4.4.2. Implementación en proyecto Android

Una vez que se hayan realizado las configuraciones y la instalación del SDK, se debe realizar la implementación siguiendo los siguientes pasos.

- Inicializar el SDK: se debe sobrescribir el método `onActivityResult` en la actividad en la cual se utilizarán las funciones del SDK.
- `override fun onActivityResult(requestCode: Int, resultCode: Int, data: Intent?) {`
- `super.onActivityResult(requestCode, resultCode, data).`
- `AppCommunicator.getInstance().onActivityResult(requestCode, resultCode, data).`
- `}`

Se debe configurar el objeto con el que puede interactuar principalmente para usar el SDK. Se debe instanciar con el contexto principal de la aplicación, el objeto solicita el appID, Contract ID y la Private Key.


```

1. val writeClient: -Digi.me- by lazy {
2.
3.     val configuration = -Digi.me-Configuration(
4.         "your_app_id",
5.         "your_contract_id",
6.         "your_private_key",
7.         "https://api.-Digi.me-/"
8.     )
9.
10.     Init(requireContext().applicationContext, configuration)
11. }

```

4.4.3. Escritura de archivos -Digi.me-

Una vez que se han realizado las configuraciones anteriores se puede escribir datos para el usuario en la nube de -Digi.me-, para esto se debe pasar por el flujo de autorización y obtener un *token* de acceso de usuario, en la respuesta de la autorización se obtienen las credenciales de usuario, también se obtiene el *postboxId*, *publicKey*, con esta información se puede realizar la escritura del archivo en la nube de -Digi.me-, en este caso de ejemplo se escribe un archivo JSON.

```

private fun writeFile() {
    writeClient.authorizeAccess(
        this,
        null,
        null,
        null
    ) { response, authorizeError ->
        if (authorizeError == null) {
            credentials = response?.credentials!!
            val nombreArchivo =
Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_DOW
NLOADS).toString() + "/" + "file.json"
            val stream
=this.applicationContext.openFileInput("file.json")
            val size = stream.available()
            val buffer = ByteArray(size)
            stream.read(buffer)
            stream.close()

```

```

        val fileContent: ByteArray =buffer
        val metadata: ByteArray = getFileContent(this,
"metadataajson.json")
        val postbox: Data = Data().copy(
            key = response.session?.key,
            postboxId = response.authResponse?.postboxId,
            publicKey = response.authResponse?.publicKey
        )

        val payloadWriteImage =
            WriteDataPayload(postbox, metadata, fileContent,
MimeType.IMAGE_PNG)

        writeClient.write(
            payloadWriteImage,
            response.credentials?.accessToken?.value!!
        ) { _, error ->
            progressBar.isVisible = false
            if (error == null)
                readFile.isEnabled = true
            else
                Log.d("MainActivity", "Failed to write data")
        }
    } else {
        progressBar.isVisible = false
        Log.d("MainActivity", "Failed to authorize")
    }
}
}
}

```

4.4.4. Lectura de archivos -Digi.me-

La lectura de archivos debe contar con contract ID que le permita realizar lectura de la nube de datos -Digi.me-, debe pasar por el flujo de autorización, posteriormente puede leer los archivos del usuario incluidos en las credenciales y obtener la información para manejarla desde Android.

```

private fun readFile() {
    readClient.authorizeAccess(
        this,
        null,
        credentials,
        null
    )
}

```

```

    ) { response, authorizeError ->
        if (authorizeError == null) {

readClient.readFileList(response?.credentials?.accessToken?.value!!) {
readFileResponse, error ->
    progressBar.isVisible = false
    if (error == null) {
        val data = readFileResponse?.fileList
        val adapter =
binding.appBarMenuSidePrincipal.contetLayout.readList.adapter as
ReadAdapter

        adapter.listaArchivos.clear()
        adapter.listaArchivos.addAll(data)
        adapter.notifyDataSetChanged()
        Log.wtf("File ", "enviamos data ")
        adapter.setOnFileItemClickListener {
            obtainStoragePermissionIfRequired()

.observeOn(AndroidSchedulers.mainThread())
            .subscribeBy(
                onComplete = {
                    fileId = it.fileId
                    readClient.readFile(

response.credentials?.accessToken?.value!!, fileId
                    ) { readFileResponse, error ->
                        val fileContentBytes =

readFileResponse?.fileContent

openFile(fileContentBytes!!)

                    }
                })
            }

        } else
            Log.d("MainActivity", "Failed to read files")
        }
    } else {
        Log.d("MainActivity", "Failed to authorize")
        progressBar.isVisible = false
    }
}
}
}

```

4.4.5. Aplicación Feeling App

A continuación, se muestra el flujo de la aplicación Feelen APP la cual permite guardar los sentimientos, y escribirlos en -Digi.me-

Figura 14. Pantalla de inicio Feeling APP



Fuente elaboración propia, empleando emulación de aplicación.

Figura 15. **Registro Feeling App**



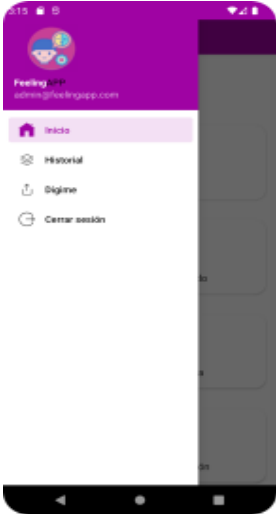
Fuente elaboración propia, empleando emulación de aplicación.

Figura 16. **Inicio de Sesión Feeling APP**



Fuente elaboración propia, empleando emulación de aplicación.

Figura 17. Menú



Fuente elaboración propia, empleando emulación de aplicación.

Figura 18. Inicio



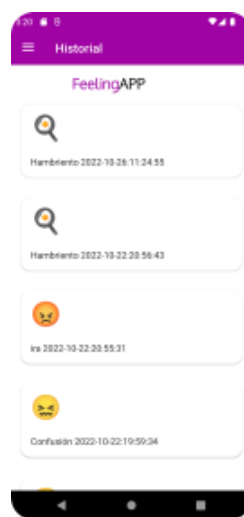
Fuente elaboración propia, empleando emulación de aplicación.

Figura 19. Registrar sentimiento



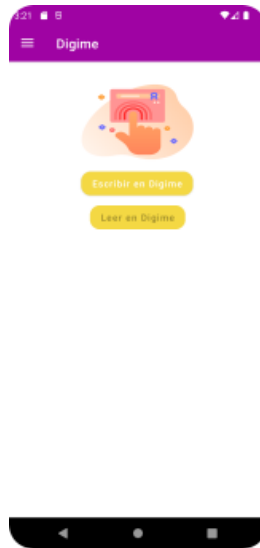
Fuente elaboración propia, empleando emulación de aplicación.

Figura 20. Historial de sentimientos



Fuente elaboración propia, empleando emulación de aplicación.

Figura 21. **Menú -Digi.me-**



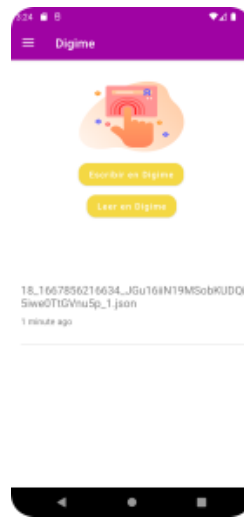
Fuente elaboración propia, empleando emulación de aplicación.

Figura 22. **Escribiendo -Digi.me-**



Fuente elaboración propia, empleando emulación de aplicación.

Figura 23. **Leyendo archivo escrito en formato JSON**



Fuente elaboración propia, empleando emulación de aplicación.

CONCLUSIONES

1. Los usuarios obtienen beneficios al dar consentimiento a organizaciones o empresas para que accedan a su información personal, los más importantes son: conocer quien consulta y por cuanto tiempo lo hará a cambio el usuario obtiene servicios de valor, decidir si quiere seguir compartiendo ya que puede revocar el acceso en cualquier momento, se tiene la seguridad de que ha pasado por un proceso de verificación por parte del equipo de -Digi.me- el cual cuenta con el respaldo de una empresa que protege la privacidad de los datos del usuario y es utilizado por diversas organizaciones y empresas en varios países.
2. Las organizaciones o empresas al solicitar el consentimiento explícito del usuario dan una mayor credibilidad y afianzan la confianza de sus clientes, porque definen de forma clara durante qué tiempo y para que utilizarán la información como también los beneficios que el cliente recibirá por dar el acceso a su información personal, pueden hacer uso de los flujos de contrato de consentimientos definidos en -Digi.me-.
3. El alcance de diseño y arquitectura de seguridad de -Digi.me- está desarrollado y probado, además de contar con certificaciones que respaldan sus procesos, recientemente en el año 2022 realizaron una actualización donde ya no trabajan con fuentes de almacenamientos de terceros, esto para mejorar la seguridad y el acceso a la información con mayor rapidez, los datos se encuentran encriptados.

4. Implementar el SDK en aplicaciones Android es sencillo, y le permite escribir y leer información de una forma sencilla, como crear su contrato o solicitar información personal pues cuenta con flujos ya preestablecidos, sin embargo hace falta más documentación que debe proveer -Digi.me- en su página web debido a que los proyectos de ejemplo se encuentran desactualizados, puede utilizar los canales de comunicación con el equipo de -Digi.me- y ellos lo pueden orientar de cómo realizar la implementación en su aplicación.

RECOMENDACIONES

1. Contar en Guatemala con un marco legal como el Reglamento General de Protección de Datos que tiene Europa, porque con esto se logra establecer los derechos de las personas sobre sus datos personales, y a las organizaciones o empresas se les define claramente cómo deben de dar tratamiento a los mismos desde un entorno jurídico. A las organizaciones o empresas que presten cualquier servicio electrónico donde recolecten información personal, se les debe dar a conocer la importancia de informar a sus usuarios de cómo están tratando sus datos personales, y sobre los beneficios que obtendrán por hacerlo.
2. Promover el uso de servicios electrónicos que respeten y cumplan con estándares donde su prioridad sean los derechos del usuario en lugar de la comercialización de su información sin su consentimiento.
3. Realizar un análisis de otros proyectos de protección de datos personales, como el proyecto SOLID que actualmente continua en investigación por diferentes organizaciones que promueven el almacenamiento de datos personales descentralizados, y la no comercialización de datos personales sin consentimiento.

BIBLIOGRAFÍA

1. ABBATE, Janet: *Inventing the Internet*, The MIT Press. [en línea]. <https://gredos.usal.es/bitstream/handle/10366/132322/El_inicio_de_la_Web_historia_y_cronologi.pdf?sequence=1>. [Consulta: 11 de agosto de 2022].
2. Castagna, R., & Lavery, T. *TechTarget*. [en línea]. <www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR>. [Consulta: 8 de 7 de 2022].
3. -Digi.me-. *Recopilación de información*. [en línea]. <<https://-Digi.me-/privacy-policy>>. [Consulta: 9 de septiembre de 2022].
4. digital-strategy. *Discover eidas*. [en línea]. <<https://digital-strategy.ec.europa.eu/en/policies/discover-eidas>>. [Consulta: 11 de agosto de 2021].
5. Domo. *Data Never Sleeps 9.0*. [en línea]. <<https://www.domo.com/learn/infographic/data-never-sleeps-9Insider>. Business. <https://www.insider.com/>>. [Consulta: 13 de agosto de 2022].
6. Frankenfeld, J., Drury, A. & Costagliola, D. *Investopedia*. [en línea]. <www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp>. [Consulta: 11 de noviembre de 2020].

7. Hat. *Hub of All Things*. [en línea]. <<https://www.hubofallthings.com/main/what-is-the-hat>>. [Consulta: 20 de agosto de 2021].
8. HealthIT.gov. *Official Website of The Office of the National Coordinator for Health Information Technology (ONC)*. [en línea]. <<https://www.healthit.gov/how-do-i/individuals>>. [Consulta: 8 de agosto de 2022].
9. Hpe. *Almacenamiento*. [en línea]. <<https://www.hpe.com/es/es/what-is/data-storage.html#:~:text=El%20almacenamiento%20de%20datos%20consiste,accesibles%20siempre%20que%20sean%20necesarios>>. [Consulta: 8 de agosto de 2021].
10. Igaleno. *Identidad digital única*. [en línea]. <<https://www.igaleno.com/blog/identidad-digital-unica/>>. [Consulta: 8 de agosto de 2021].
11. Insider-Trends. *How is digi-me pioneering a new approach to personal privacy*. [en línea]. <<https://www.insider-trends.com/how-is-digi-me-pioneering-a-new-approach-to-personal-privacy/>>. [Consulta: 10 de julio de 2020].
12. ISO 27001:2013 - 27017:2015. *Plataforma de gestión de datos personales*. [en línea]. <<https://-Digi.me-/accreditations>>. [Consulta: 21 de septiembre de 2021].

13. MedMij. *Estándar MedMij*. [en línea]. <<https://-Digi.me-/accreditations>>. [Consulta: 25 de septiembre de 2021].
14. NEN 7510. *Estándar de atención médica holandés para la seguridad*. [en línea]. <<https://-Digi.me-/accreditations>>. [Consulta: 21 de septiembre de 2021].
15. play.-Digi.me-. *Playground en -Digi.me-*. [en línea]. <<https://play.-Digi.me-/>>. [Consulta: 22 de septiembre de 2022].
16. RODRÍGUEZ, Elisabet. *El HTML, una idea en evolución*. [en línea]. <<http://www.maestros delWeb.com/editorial/htmlhis/>>. [Consulta: 22 de septiembre de 2012].
17. Solid. *Your data, your choice*. [en línea]. <<https://solidproject.org/>>. [Consulta: 20 de agosto de 2021].
18. TABARÉS GUTIÉRREZ, Raúl. *Inicio de la web*. [en línea]. <https://gredos.usal.es/bitstream/handle/10366/132322/El_inicio_de_la_Web_historia_y_cronologi.pdf?sequence=1&isAllowed=y>. [Consulta: 11 de octubre de 2022].
19. The hub of all things. *Own Your Own Personal Data Server*. [en línea]. <<https://www.hubofallthings.com/main/what-is-the-hat>>. [Consulta: 5 de agosto de 2022].
20. U. S. *Department of veterans Affairs*. *Blue Button*. [en línea]. <<https://www.va.gov/bluebutton/>>. [Consulta: 17 de octubre de 2021].

21. Unidad de Innovación, Universidad de Murcia. *Diseño y evaluación de materiales didácticos. La navegación hipertextual en el World-Wide Web.* [en línea]. <https://www.um.es/innova/OCW/disenio_y_evaluacion_materiales_didacticos/mpaz/utilidades/pdf/18.pdf>. [Consulta: 11 de septiembre de 2022].
22. WOLFIE, Christl. *7 Most Infamous Cloud Security Breaches.* [en línea]. <<https://www.arcserve.com/blog/7-most-infamous-cloud-security-breaches>>. [Consulta: 19 de mayo de 2022].
23. XXIV Congreso Argentino de Ciencias de la Computación. *Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica.* [en línea]. <http://sedici.unlp.edu.ar/bitstream/handle/10915/73652/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y>. [Consulta: 4 de abril de 2022].
24. Zacco. *We can't find the page you're looking for.* [en línea]. <<https://www.zacco.de/articles/the-territorial-scope-of-the-gdpr>>. [Consulta: 7 de septiembre de 2022].