

Sistema de identificación de perfiles falsos en las redes sociales

Boris Hurtado, Carlos Jiménez
Maestría en Seguridad de la Información Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes.
Bogotá, Colombia noviembre 2022

Abstract— Resumen del Proyecto, alcance y resultados

I. INTRODUCCIÓN

En la actualidad, hay un gran número de redes sociales y plataformas en las cuales la mayoría de las personas pueden registrarse (crear una cuenta) sin mayor necesidad que proveer un correo electrónico y una contraseña. Esto presenta un problema, debido a que no se llevan revisiones exhaustivas a la hora de registrar un usuario en una plataforma, existen personas que utilizan dichas plataformas o redes sociales para hacerse pasar por otras personas con fines maliciosos. Entre estos fines maliciosos se encuentran, fraude, desinformación o simplemente dañar o contaminar la reputación de la persona que están suplantando.

Aunque existen algunas redes sociales que verifican a sus usuarios como es el caso de Twitter o Instagram, estas plataformas no se encargan activamente de detectar perfiles falsos o incluso bots que existen dentro de su base de usuarios.

Es cierto que existen mecanismos para denunciar en cada plataforma una cuenta, pero estos procesos están bajo la normatividad de las plataformas y se encargan únicamente de cerrar las cuentas denunciadas una vez han llevado a cabo su investigación. Sin embargo, una vez cerrada la cuenta, la persona que está llevando la suplantación de identidad puede simplemente crear una nueva cuenta y seguir con las actividades de suplantación. Adicionalmente, existe el problema de los bots, que son programas automatizados que participan y se comunican activamente en redes sociales, un ejemplo claro se trata de Twitter que, aunque en la actualidad ha declarado “que menos del 5% de sus usuarios son ‘bots’, el multimillonario Elon Musk asegura que son hasta cuatro veces más.” (Pesantes, 2022). La actividad de estos bots o perfiles falsos puede variar, pero, como se explicó anteriormente, se suelen usar para tratar de cometer actividades de suplantación o en el caso de redes sociales incrementar el número de seguidores que no se tratan de cuentas que pertenecen a personas reales o a quienes dicen ser.

Teniendo en cuenta el problema presentado, el siguiente proyecto busca, a través de una solución tecnológica, tratar de mitigar estos casos de suplantación de identidad, identificando cuando una cuenta se trata de un perfil falso o no y, de esta

forma, evitar que se cometan fraudes o posibles crímenes. A continuación, se presentará la definición del problema, la propuesta de solución y su implementación detallada, así como las reglas y procesos que se han implementado para tratar de determinar si una cuenta se trata de un perfil falso o no. Por último, se presentarán las secciones de gestión del proyecto y las conclusiones de este.

II. DISEÑO DE LA SOLUCIÓN

Con el objetivo de poder identificar perfiles falsos o cuentas que traten de suplantar a otras personas, la solución propuesta se trata de una aplicación web que, a partir de un nombre de usuario, sea capaz de determinar si se trata de un perfil falso o no. Para construir esta solución, se hará uso de distintas tecnologías que serán descritas en el apartado de Diseño e implementación de la solución. A continuación, las funcionalidades principales de la solución propuesta

- Permitir a un usuario de la solución crear una cuenta en el sistema
- Permitir a un usuario de la solución consultar por el nombre de una cuenta la información de esta en distintas plataformas
- Permitir a un usuario de la solución revisar el histórico de las cuentas que ha consultado
- A partir de un nombre de usuario, determinar si se trata de un perfil falso o que intenta suplantar a una persona
- Mostrar las distintas plataformas en las que una cuenta existe con el nombre de usuario consultado
- Proveer links para que un usuario de la aplicación pueda revisar la cuenta consultada en las distintas plataformas encontradas

El diseño de la solución, en primer lugar, se va a presentar la matriz de requerimientos funcionales y requerimientos no funcionales. En segundo lugar, se presentará las herramientas y la metodología utilizada para llevar a cabo el proyecto, así como la recopilación de información sobre un perfil. Por último, se explicará qué reglas se han implementado una vez se haya recolectado la información para determinar si el perfil consultado por el usuario es falso o no.

A continuación, se presenta la matriz de requerimientos de la solución

Código	Descripción	Componente
RF1	Implementar login para un usuario	BackEnd
RF2	Implementar registro para un usuario	BackEnd
RF3	Implementar el cifrado de la contraseña de los usuarios registrados	BackEnd
RF4	Persistir la información del usuario registrado	BackEnd
RF5	Consultar, por nombre de cuenta, la información de un perfil en distintas redes sociales y plataformas	BackEnd
RF6	Persistir la información obtenida tras consultar el nombre de la cuenta en las diferentes plataformas	BackEnd
RF7	Retornar la información obtenida para la cuenta consultada	BackEnd
RF8	Generar histórico para un usuario y las cuentas que ha consultado	BackEnd
RF9	Determinar si la cuenta consultada se trata de un perfil falso o no	BackEnd
RF10	Configurar las reglas para la detección de perfiles falsos	BackEnd
RF11	Crear los controladores para la consulta de información a partir de un nombre de usuario	BackEnd
RF12	Crear los controladores para el registro de un usuario	BackEnd
RF13	Crear los controladores para el login de un usuario	BackEnd
RF14	Crear las entidades para realizar el mapeo de la base de datos	BackEnd
RF15	Crear las interfaces para la comunicación con el API de Twitter	BackEnd
RF16	Crear las interfaces para hacer uso del proyecto Sherlock	BackEnd
RF17	Crear las clases de lógica que se encargaran de procesar las solicitudes de consulta y verificación	BackEnd
RF18	Crear la base de datos de la aplicación	Base de Datos
RF19	Crear las tablas en la base de datos de la aplicación	Base de Datos
RF20	Crear la aplicación web	Front End
RF21	Desarrollar la interfaz de usuario	Front End
RF22	Desarrollar interfaz de registro e inicio de sesión	Front End
RF23	Desarrollar la interfaz de consultas	Front End
RF24	Desarrollar la interfaz de resultados	Front End
RNF1	La aplicación debe funcionar en los navegadores Chrome, Safari y Mozilla	BackEnd y Front End
RNF2	La aplicación debe estar disponible todo el tiempo	BackEnd y Front End
RNF3	El tiempo de consulta no debe exceder un minuto por perfil consultado	BackEnd y Front End

Tabla 1. Matriz de requerimientos

Para el desarrollo de la solución se implementó la metodología de desarrollo SCRUM, que se trata de un conjunto de buenas prácticas para trabajar en equipo y obtener el mejor resultado posible en un proyecto. En primer lugar, se realizó la investigación de posibles soluciones existentes al problema anteriormente expuesto. Teniendo en cuenta esto, se realizó un levantamiento de requerimientos para conocer qué funcionalidades debía tener la aplicación para cumplir la meta definida en el apartado de la propuesta de la solución. En segundo lugar, y teniendo en cuenta los requerimientos que se listaron en la matriz de requerimientos, se decidió qué tecnologías serían utilizadas. Por último, una vez realizada la implementación, se realizaron pruebas para demostrar las diferentes funcionalidades y características de la aplicación.

Herramientas Utilizadas: Para llevar a cabo el desarrollo de la solución propuesta, se hará de uso de las siguientes herramientas:

- API de Twitter: Se hizo uso de este API para consultar y recopilar la información de una cuenta a partir de los datos ingresados por el usuario de la aplicación desarrollada
- Proyecto Sherlock: Este proyecto se trata de una herramienta que permite, a partir de un nombre de usuario, encontrar que plataformas tiene una cuenta registrada con este nombre de usuario
- Proceso OSINT: OSINT consta de una serie de fases que permiten estructurar el trabajo de manera que se agilice la investigación. A continuación, damos una breve descripción de estas fases:



Figura 1. Osint

- Requisitos: ¿Qué problema queremos resolver? ¿Qué información necesitamos?
- Identificación fuentes de información: ¿Que fuentes nos pueden aportar información valiosa y veraz?
- Adquisición: Etapa de obtención de la información
- Procesamiento: Dar formato a toda la información “en bruto” obtenida en la anterior fase
- Análisis: Generar inteligencia a partir de todos los datos obtenidos, encontrando relaciones entre estos que nos permitan llegar a conclusiones.
- Presentación: Darle a la información un formato en el que se pueda comprender de manera eficaz y sencilla.

Reglas de validación:

Con el fin de consolidar un proceso de validación de los perfiles se procede a desarrollar todos los lineamientos y reglas que el Sistema debe ejecutar para poder determinar si la cuenta que se está validando en su momento es un perfil real o es falso.

- Revisar si la cuenta asociada al nombre de usuario está verificada en Twitter. Esto permite tener un punto de partida a la hora de decidir si la cuenta es falsa o no (sobre todo para perfiles de celebridades o personas influyentes en redes sociales). Vale la pena mencionar que, para este punto en particular, no se tiene en cuenta la nueva funcionalidad de Twitter que permite a un usuario pagar para obtener la verificación de su cuenta. La medida anteriormente mencionada, fue implementada por la compañía después de que se planteara este proyecto.
- Verificar el número de seguidores de la cuenta en Instagram y Twitter (como mínimo). Esta validación incluiría la cantidad de seguidores, la cantidad de cuentas seguidas y el número de posts y tweets, respectivamente. Si la cuenta no tiene seguidores se determinará como posible cuenta falsa ya que las

cuentas que no tienen seguidores a pesar de tener contenido son generalmente falsas (Romero, 2020)

- Determinar qué cuentas tienen un nombre de usuario similar en la misma plataforma (remover caracteres no alfabéticos) para comparar los datos de las cuentas encontradas
- Para un nombre de usuario específico, una vez obtenida la información, remover caracteres no alfabéticos y realizar una nueva consulta con el nombre de usuario modificado. Una vez se haya realizado la consulta, comparar los datos de las cuentas (número de seguidores, post y cuentas seguidas) si se trata de un nombre de usuario lo bastante similar, tendrá prelación la cuenta que cuente con mayor cantidad de seguidores, cuentas seguidas y antigüedad de creación.
- Comparar las fechas de creación de las cuentas en la plataforma Twitter (siempre y cuando exista información de la cuenta consultada).
- A partir de una lista de celebridades o personas influyentes, cruzar información de la cuenta consultada para determinar si corresponde a la cuenta de alguna celebridad real o si trata de suplantar la cuenta de dicha celebridad. El siguiente es un ejemplo claro:



Figura 2. Perfil Falso



Figura 3. Perfil Real

III. IMPLEMENTACIÓN DE LA SOLUCIÓN

En esta sección se explicará detalladamente la manera en la que se implementó la solución propuesta. En primer lugar, se explicará la arquitectura de la solución sus components y las tecnologías empleadas. En Segundo lugar se explicará cómo se comunican los distintos components. Por ultimo se mostrará las diferentes funcionalidades de la aplicación

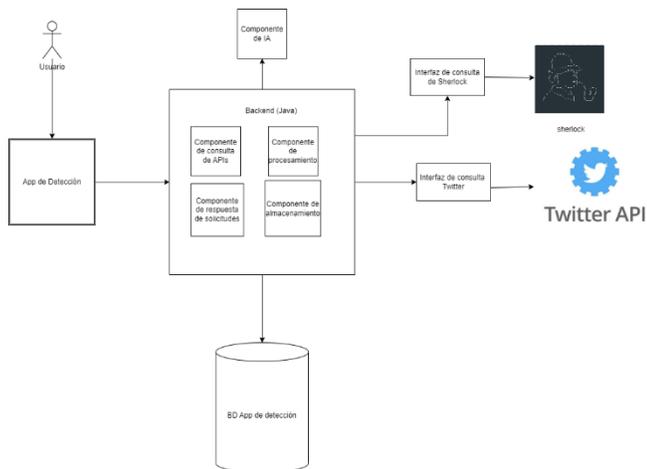


Figura 4. Arquitectura de la solución

Componentes de la solución:

- Aplicación web: Se encarga de la interacción con el usuario (Registro, login, consulta de nombres de usuario) Tecnología usada: React v. 18.1.0 Estructura de la aplicación web

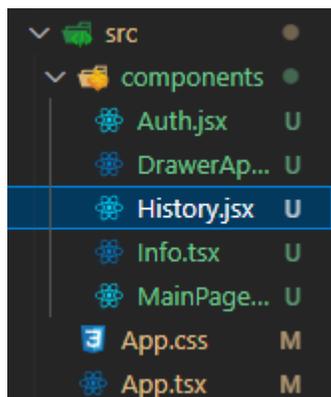


Figura 5. Estructura App Web

Auth: componente que se encarga del registro y del Login de un usuario
Drawer: Componente que se encarga de las opciones

del usuario
Info: Componente que se encarga de mostrar la información recopilada de un usuario
MainPage: Componente que permite al usuario realizar consultas sobre un perfil
History: Componente que permite al usuario revisar los perfiles anteriormente consultados
- Componente de Backend: Se encarga de procesar las solicitudes hechas a través de la aplicación web, aplicar la lógica de las reglas, persistir la información de los perfiles consultados y de los usuarios registrados. Así como la comunicación con el API de Twitter y la comunicación con el proyecto Sherlock.
Tecnologías usadas: Java 11, SpringBoot
Estructura del componente BackEnd:

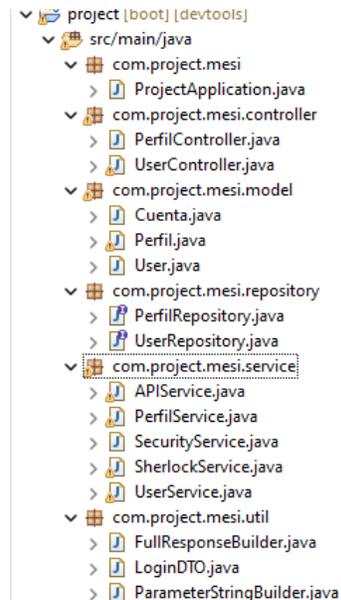


Figura 6. Estructura BackEnd

- Paquete com.project.mesi: Contiene la clase que inicializa y despliega la aplicación
- Paquete com.project.mesi.controller: Contiene los archivos de los controladores para recibir y procesar solicitudes de la aplicación
- Paquete com.project.mesi.model: Contiene los archivos que se encargan de realizar el mapeo de las tablas de la base de datos a las entidades
- Paquete com.project.mesi.repository: Contiene los archivos que se encargan de obtener la información persistida en la base de datos
- Paquete com.project.mesi.service: Contiene los archivos que se encargan de procesar toda la lógica de la aplicación así como

comunicarse con las diferentes fuentes de información utilizadas en el proyecto

- Paquete com.project.mesi.util: Contiene los archivos utilitarios del componente de backend como la transformación de la información obtenida, el cifrado de las contraseñas para almacenamiento seguro y el almacenamiento en archivos de texto de la información obtenida cuando se utiliza el proyecto Sherlock

Diagrama de la base de datos.

Tecnologías usadas: PostgreSQL v.10.0.1

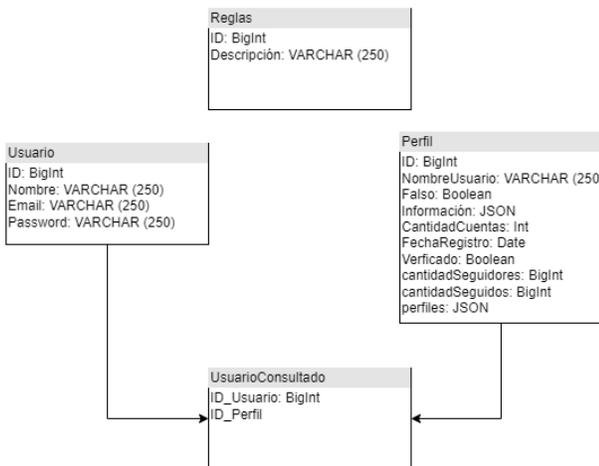
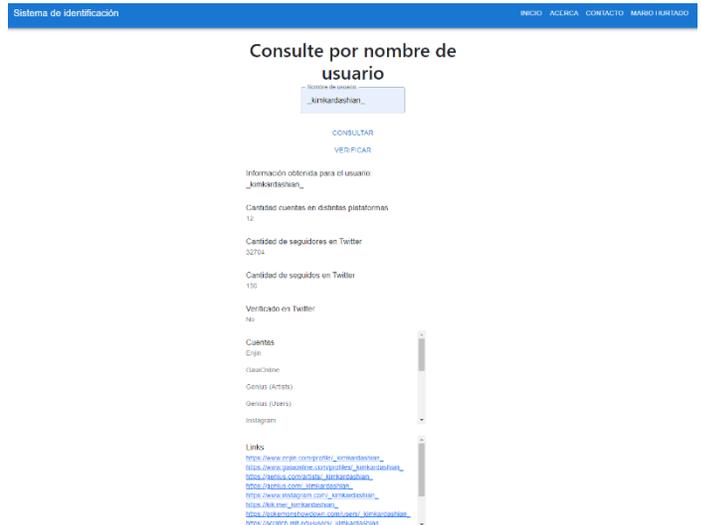


Figura 7. Diagrama Base de datos

IV. FUNCIONALIDADES DE LA APLICACIÓN

Funcionalidad de consulta por nombre de usuario:

- Cumple la tarea de permitir al usuario consultar por un nombre de perfil las diferentes plataformas en las que ese nombre de perfil tiene una cuenta



Funcionalidad de verificación:

- Cumple la tarea de, una vez consultado el nombre de usuario, verificar el perfil haciendo uso de las reglas de validación anteriormente descritas.

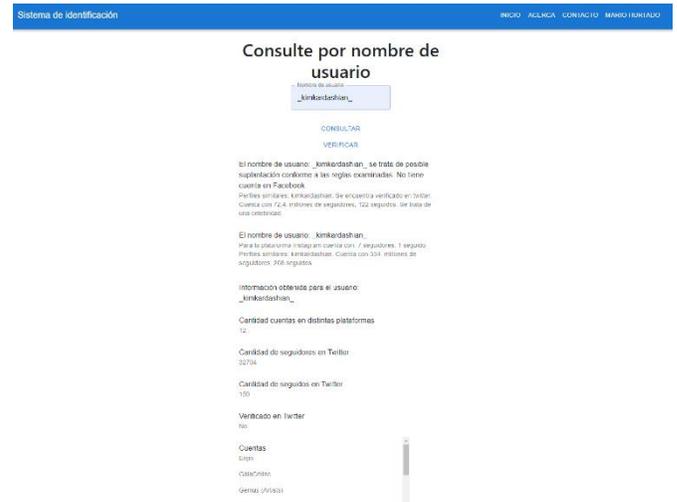


Figura 8. Funcionalidad Verificación

Funcionalidad de historial de consulta:

- Cumple la función de permitir al usuario revisar qué cuentas ha consultado y si se trata de un perfil falso.

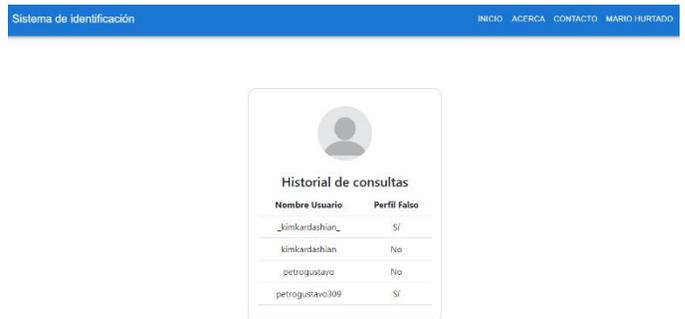


Figura 9. Funcionalidad historial de consulta

V. GESTIÓN DEL PROYECTO

Una vez explicadas las funcionalidades de la aplicación, esta sección explicará los pasos necesarios para llevar a cabo el proyecto en cuanto a su gestión. Así, se describe la estructura organizacional para la solución, haciendo énfasis en los roles que debe tener el equipo de recursos humanos para llevar a cabo cada una de las actividades en el cronograma propuesto.

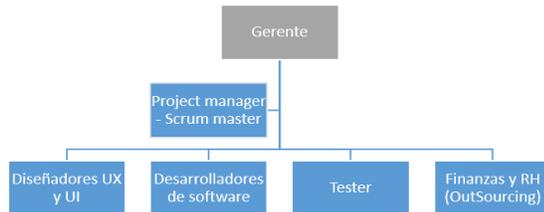


Figura 8. Organigrama del proyecto

Scrum Master: es quien debe asegurarse de que el equipo siga metodologías y estructuras ágiles. Estas metodologías son un concepto que puede describirse como una mentalidad de gestión de proyectos que se enfoca en la colaboración y la creación de valor. Según el Manifiesto Ágil, sus valores principales incluyen:

- Individuos e interacciones por sobre procesos y herramientas
- Software funcional por sobre documentación comprensible
- Colaboración con el cliente por sobre negociación de contratos
- Responder a los cambios por sobre seguir un plan

En la gestión de proyectos, el scrum permite un desarrollo rápido mientras el trabajo se lleva a cabo en partes más pequeñas llamadas sprints. El scrum master es el responsable de cómo se siguen las estructuras en el equipo. Su rol incluye eliminar obstáculos, crear un ambiente productivo y ayudar al equipo a trabajar bien en conjunto. Aunque técnicamente es un líder, no tienen autoridad por sobre otros miembros del equipo.

UX (experiencia de usuario), así que la responsabilidad principal del diseñador UX es asegurar un resultado suave y enfocado en el usuario. Su rol es imaginarse como el usuario final interactuando con el producto, y hacen que este sea fácil de utilizar y se enfocan en todos los aspectos de la experiencia: usabilidad, funcionalidad y rendimiento.

UI (Interfaz de usuario), por lo que el rol del diseñador UI se enfoca principalmente en el software y en cómo se ve y se siente para el usuario. Necesitan que sea intuitivo y directo.

Los diseñadores UX y UI toman la idea del cliente y el producto y utilizan prototipos para desarrollar la idea. Son una parte fundamental del equipo de desarrollo de software ya que son los que defienden las necesidades del usuario. Los roles de estos dos actores se superponen mucho, y dependiendo del tamaño del proyecto, se pueden condensar en uno solo.

El desarrollador de software: es quien implementa las ideas del arquitecto, y discute las posibilidades o imposibilidades de la implementación con el mismo. A menudo, este miembro del equipo de desarrollo de software es responsable de hacer

seguimiento a su propio progreso, e informar al jefe de proyecto sobre los problemas que encuentra en el camino. Aunque es capaz de realizar todas las tareas de desarrollo, puede delegar funciones como la de programación, testeo, supervisión o mantenimiento, a otros miembros del equipo, para ceñirse a la implementación. Es responsable de que todos los aspectos de la implementación del proyecto funcionen correctamente.

Tester: Este importante miembro del equipo de desarrollo de software, se encarga de asegurar que los requisitos definidos por el arquitecto de software son cumplidos en la implementación del producto o servicio llevada a cabo por los desarrolladores y/o programadores. Junto a estos últimos, aplicará diferentes métodos de testeo e informará sobre todos los errores encontrados durante la fase de prueba.

Finanzas y RH (OutSourcing): Es la forma en la que se subcontrata los servicios de gestión financiera y gestión humana. En empresas que se dediquen netamente a llevar las cuentas de las empresas emergentes en el mercado de las TICs.

VI. COSTOS Y RIESGOS DEL PROYECTO

A continuación, se presentarán los riesgos técnicos con los que cuenta la solución a implementar. Estos están organizados en un orden descendente, de acuerdo a la importancia del riesgo, el flujo de las actividades conforme el cronograma de ejecución y las acciones que se deben desarrollar para minimizarlos:

Nivel 1 de la RBS	Nivel 2 de la RBS	Riesgo
Riesgo técnico	Análisis	Falta de medición general del proceso.
Riesgo técnico	Análisis	Métodos de análisis in escalables y demasiado formales
Riesgo técnico	Procesos técnicos	Demasiadas sorpresas en el proyecto (Incertidumbre)
Riesgo técnico	Desarrollo	Falta de énfasis en las pruebas
Riesgo técnico	Estimaciones, supuestos y restricciones	Costos ocultos sustanciales del paquete de software
Riesgo técnico	Paquetes de software	Falta de soporte del proveedor en la ubicación del cliente
Riesgo técnico	Implementación	Pruebas inadecuadas del usuario

Tabla 2: Matriz para riesgos identificados.

- Falta de medición general del proceso: Limitar las actividades en cuanto a tiempos y alcance de cada una de estas para trazar una línea de ruta en donde se prioricen los resultados en pro de alcanzar las metas inicialmente propuestas en la planeación del proyecto.
- Métodos de análisis in escalables y demasiado formales: Fijar e implementar métodos de análisis en donde se permitan tener en cuenta los diversos requerimientos del sistema y adicionar un extra al momento de fijar metas específicas, lo cual nos permitiría ampliar la solución hasta en el 40 % adicional de lo que usualmente estaría presupuestado.
- Demasiadas sorpresas en el proyecto (Incertidumbre): Limitar los escenarios que pueden presentarse y minimizar al máximo la incertidumbre que se puedan presentar.
- Falta de énfasis en las pruebas: Ejecutar un plan de acción y/o cronograma de pruebas en donde cada una

de ella contribuya a la validación y certificación de la solución que brinda el aplicativo.

- Costos ocultos sustanciales del paquete de software: Dimensionar desde el comienzo todos los posibles escenarios para poder abarcar la mayor cantidad de requerimientos en cuanto a procesamiento y desempeño del software a utilizar.
- Falta de soporte del proveedor en la ubicación del cliente: Tener personal técnico de respaldo en donde entraría a ser un backup para todas las actividades a implementar.
- Pruebas inadecuadas del usuario: Seleccionar la data con la que se va a hacer las pruebas por parte de usuario final.

En la actualidad hay un sin número de perfiles de los nativos digitales que vienen siendo los menos de edad con una alta exposición ampliando así la superficie de ataque para muchos delincuentes en las redes sociales con el fin de tener unos objetivos específicos de trata y explotación infantil. (Hansford, 2021) La proporción detectada de menores víctimas de trata se ha triplicado, mientras que la proporción de niños se ha multiplicado por cinco en los últimos 15 años. Las niñas son víctimas de trata principalmente con fines de explotación sexual, mientras que los niños son explotados con fines de trabajos forzosos, según el Informe Mundial sobre la Trata de Personas, presentado hoy por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés). Por lo anterior, una forma de hacer frente a todas estas cifras es la implementación de una herramienta que permita otorgar un grado de confianza a los perfiles que tienen agregados a sus contactos todos estos menores de edad en las redes sociales. Haciendo un listado de clientes potenciales podemos identificar a los siguientes:

- Red PaPaz
- Red Viva de Colombia
- UNICEF
- Agencia PANDI
- Children International
- Fundación ANTONIO RESTREPO BARCO
- Red PAI (Protección a la Infancia)

La finalidad con la que se pensó la funcionalidad del software es para contrarrestar todos los casos de suplantación de identidad que sufren algunos de los viajeros frecuentes que van al extranjero. Posteriormente sus familiares son contactados para luego solicitarle activos financieros. Como una solución opcional a este tipo de comportamiento se pensó una estrategia que abarca a las agencias de viajes y se puede ofertar servicio adicional, en el que los usuarios que compren los paquetes de viajes se les anexe una funcionalidad que les permita tener un

usuario en el software, que les permita consultar el grado de confianza que tengan los perfiles que deseen consultar.

ITEM	HORAS	FECHA INICIO	FECHA FIN	2022	HORAS	2023	HORAS	2024	HORAS
Planificación del Proyecto	1.300	8/08/2022	9/08/2024	\$ 48.750.000,00	200	\$ 1.325.000,00	\$ 360,00	\$ 11.250.000,00	500
Gestión del Proyecto	2.300	8/08/2022	9/08/2024	\$ 80.000.000,00	800	\$ 66.250.000,00	\$ 1.500,00		
Diseño de la Solución	200	16/08/2022	10/08/2022	\$ 7.500.000,00	200				
Adquisición Infraestructura	1.300	20/08/2022	9/08/2023	\$ 19.125.000,00	510	\$ 29.625.000,00	\$ 790,00		
Requerimiento de Procesos	1.200	28/08/2022	10/12/2024	\$ 22.500.000,00	600	\$ 11.250.000,00	\$ 300,00	\$ 11.250.000,00	300
Desarrollo de Software	1.800	28/08/2022	16/08/2023	\$ 24.750.000,00	660	\$ 43.750.000,00	\$ 1.180,00		
Instalación y Configuración Infraestructura	600	10/09/2022	20/01/2023	\$ 15.750.000,00	420	\$ 6.750.000,00	\$ 180,00		
Testing de la Solución	130	8/08/2022	10/12/2022	\$ 12.000.000,00	230				
Implementación	1.300	10/11/2022	10/11/2023	\$ 11.250.000,00	300	\$ 17.500.000,00	\$ 1.000,00		
TOTAL				\$ 186.625.000,00	4.530	\$ 187.250.000,00	4.960	\$ 42.500.000,00	800
Total Proyecto				\$ 416.375.000,00	10.270				

Costos por Hora conforma al perfil	
Gerente de Proyecto	\$ 62.500,00
Desarrollador	\$ 37.500,00
Arquitecto de software	\$ 37.500,00
Arquitecto de Seguridad	\$ 37.500,00
Ingeniero TI	\$ 37.500,00
QA	\$ 37.500,00
Ingeniero Industrial	\$ 37.500,00

Figura 3. Estructura de costos y presupuesto

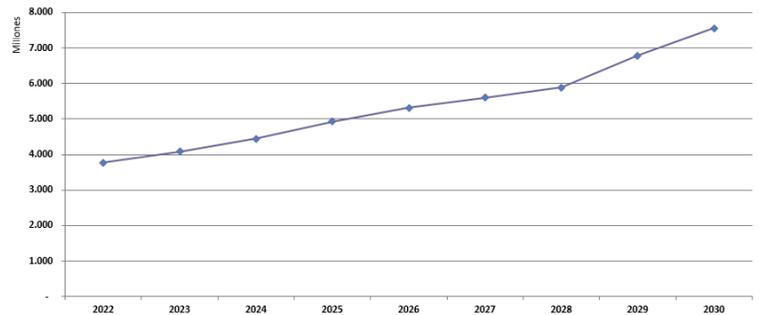


Figura 9.. Flujo de caja

En la estructura de costos y presupuesto se puede detallar cada uno de los roles y su respectivo valor por hora, como también se puede observar las diferentes actividades que se deben ejecutar y cuanto tiempo se debe emplear en dichas actividades para llevar a buen termino el desarrollo del proyecto. Los valores del las horas para cada uno de los perfiles requeridos fueron tomados del promedio actual de compensación mensual y estos valores fueron divididos entre los 30 días del mes.

Los valores asignados para cada una de las actividades corresponden a la valoración de cuanto tiempo debería tomarnos desarrollar cada uno de estas actividades haciendo hincapié en la complejidad de cada uno de los procesos; teniendo las cantidades totales de tiempos en horas se procede a multiplicar por el valor por hora que corresponde a cada uno de los roles.

Valor actividad: cantidad horas de desarrollo actividad * Valor hora por rol

Gerente de proyecto:

$$15.000.000 \text{ COP} / 30 \text{ días} / 8 \text{ horas} = 65.000 \text{ COP} \times \text{Hora}$$

Dependiendo de la complejidad de las actividades y el requerimiento que debe tener este rol se multiplica las cantidades de horas requerida para que el rol pueda desarrollar dicha actividad.

$$700 \text{ Horas} * 65.00 \text{ COP} = 43.750.000,00$$

Desarrollador:

$$660 \text{ Horas} * 37.500 \text{ COP} = 12.000.000,00 \text{ COP}$$

VII. CONCLUSIÓN Y TRABAJO FUTURO

La suplantación de identidad es un problema que cada vez se presenta más a menudo, las plataformas o redes sociales no realizan verificaciones exhaustivas a la hora de registrar un nuevo usuario. Debido a lo anterior, es fácil que una persona trate y logre suplantar la identidad de alguien más a través de estas plataformas.

El Sistema de identificación, se desarrolló entonces para tratar de mitigar estos casos de suplantación en redes sociales y poder verificar, bajo las reglas anteriormente descritas, si un perfil corresponde realmente a una persona real o si se trata de suplantación de identidad.

Las tecnologías usadas en este proyecto cumplen el propósito de facilitar la consulta de datos y la presentación de estos al usuario, de una forma que sea entendible y le dé al usuario herramientas para poder determinar si un perfil es falso o no, más allá de la evaluación inicial de la aplicación. Este proyecto fue desarrollado bajo la metodología Scrum, y su propósito, como se explicó anteriormente, permite ejecutar consultas de diversos perfiles y nos permite determinar si son falsos o no de acuerdo una serie de reglas de verificación cruzando datos de la herramienta de código abierto Sherlock y el API de Twitter.

Al inicio del proyecto se debe hacer una gran inversión de capital financiero para poner en marcha toda la infraestructura para desarrollar este proyecto. Posteriormente, al implementar el sistema de identificación de perfiles falsos en las redes sociales, luego de que se hagan todas las pruebas con el cliente, se espera que en el cuarto año se comience un crecimiento exponencial debido a que ya se cuenta con el producto final y cualquier modificación sobre este es trabajo adicional. Los ingresos se mantendrían con un crecimiento estable y constante.

Aunque con las pruebas realizadas, se pudo encontrar perfiles falsos que intentaban suplantar celebridades o cuentas de influencers, en un futuro esta herramienta debe refinar las reglas establecidas para poder hacer frente a casos de suplantación de identidad de personas que no tienen un perfil alto o simplemente no cuentan con los números de seguidores que las cuentas de celebridades tienen. Adicionalmente, se puede hacer uso de un módulo de inteligencia artificial (IA) para automatizar el proceso de consulta y verificación de perfiles. De igual forma, se deberá integrar distintas fuentes de información para contar con mayor cantidad de datos con el fin de cruzarlos con los datos ya existentes y de esta forma mejorar la eficacia de detección de perfiles, así como refinar las reglas para la verificación de perfiles y abarcar más plataformas.

En cuanto a los perfiles que no pertenezcan a personas famosas o influencers, las reglas de validación deben ser refinadas para que la identificación de suplantación de identidad sea acertada. Dicha refinación de las reglas debe incluir varios componentes, entre los cuales debe existir un componente de comparación de imágenes para determinar si las imágenes de los distintos perfiles son similares o iguales. Así mismo, se deben incorporar más fuentes de datos para poder tener un mayor entendimiento de los perfiles. Con mayor cantidad de datos, la tarea de

verificar si un perfil intenta copiar la información de otro sería más fácil. También, para refinar las reglas, a futuro se debería incluir un módulo de deep learning que, a partir de casos confirmados de suplantación de identidad, sea capaz de discernir entre un perfil falso y uno real una vez haya sido entrenado y cuente con la información necesaria de cada perfil.

A futuro, la identificación de perfiles falsos debería ser a través de IA o módulos de deep learning que hayan sido entrenados con casos reales de suplantación de identidad y cuenten con distintas fuentes de información. Así, la verificación de perfiles se trataría de una tarea automatizada con base en casos reales. Esto significaría que además de contar con mayor información acerca de cada perfil a comparar, la IA o módulo de deep learning también sería capaz de identificar patrones que utilizan las cuentas falsas y de esta forma reconocerlas más fácilmente.

BIBLIOGRAFÍA

- *El Espectador*. (13 de 5 de 2022). Obtenido de El Espectador: <https://www.elespectador.com/tecnologia/cuidado-delincuentes-quieren-robar-su-identidad-en-las-redes-sociales>
- *El Tiempo*. (18 de 4 de 2022). Obtenido de El Tiempo: <https://www.eltiempo.com/unidad-investigativa/robo-de-identidad-en-redes-mujer-denuncia-amenazas-por-suplantacion-665522>
- Hansford, B. (2 de 2 de 2021). *UNODC*. Obtenido de UNODC: https://www.unodc.org/mexicoandcentralamerica/es/webstories/2020/2021_02_02_aumenta-la-proporcin-de-menores-vctimas-de-trata--los-nios-vctimas-se-multiplican-por-cinco-la-tendencia-general-de-la-trata-de-personas-ha-empeorado-de-forma-paralela-al-covid-19
- Pesantes, K. (23 de 05 de 2022). *Primicias*. Obtenido de Primicias: <https://www.primicias.ec/noticias/tecnologia/twitter-cuantos-bots-tiene-son-problema/>
- Romero, I. (20 de 12 de 2020). *metricool*. Obtenido de metricool: <https://metricool.com/fake-profiles/>
- *Valora Analitik*. (9 de 5 de 2022). Obtenido de Valora Analitik: <https://www.valoraanalitik.com/2022/05/09/suplantacion-en-redes-sociales-una-amenaza-en-colombia/>