



**INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO**



TRABAJO TERMINAL I

**ANBU PROTOTIPO DE MOTOR DE BÚSQUEDA DE PERSONAS QUE
TIENEN UN PERFIL DE VIOLENCIA EN LA RED SOCIAL INSTAGRAM
A TRAVÉS DE PATRONES DE RECONOCIMIENTO**

2019-A034

Presentan:

Astorga Hurtado Alan

Benítez López Daniel

López Rivera Daniel

Directores:

Dr. Raúl Acosta Bermejo

M. en C. Jorge Ferrer Tenorio

2020-1

Índice

Capítulo 1	3
1.1 Introducción	3
1.2 Problemática	4
1.3 Propuesta de Solución	4
1.4 Objetivos	4
1.4.1 General	4
1.4.2 Particulares	4
1.5 Justificación	5
1.6 Estado del Arte	5
1.6.1 Webstagram	5
1.6.2 Yooying	5
1.6.3 Metaeyes	5
1.7 Alcance	6
Capítulo 2. Marco Teórico	7
2.1 Instagram	7
2.1.1 Perfil de Usuario	7
2.1.2 Publicaciones	9
2.2 Instagram Basic Display API	10
2.3 Análisis facial	11
2.3.1 Rasgos faciales	12
2.3.2 Análisis Morfopsicológico e Imagenológico de una persona violenta	12
2.4 Arma Corta Tipo Escuadra	16
Capítulo 3. Tecnologías de Desarrollo	17
3.1 API de Instagram	17
3.1.1 Requisitos para la autenticación	17
3.2 Betaface	20
3.3 TensorFlow	24
3.4 Apache HTTP Server	26
3.5 Flask	27
Capítulo 4. Análisis de Software	28
4.1 Reglas del Negocio	28
4.2 Requerimientos del Sistema	31
4.2.1 Requerimientos Funcionales	31
4.2.2 Requerimientos No Funcionales	34
4.3 Análisis de Riesgos	36
4.4 Definición de Actores	38
4.5 Casos de Uso	38

4.5.1 Diagrama de Casos de Uso	41
4.6 Modelado de la Base de Datos	42
4.6.1 Diagrama Entidad Relación	42
4.6.2 Esquema Relacional	43
4.6.3 Diccionario de Datos	44
Capítulo 5. Diseño de Software	48
5.1 Arquitectura del Sistema	48
5.2 Diagrama de Procesos	50
5.3 Diagramas de Secuencia	51
5.4 Vistas del Sistema	52
Capítulo 6. Trabajo a Futuro	60
6.1 Conclusiones de este Documento	60
6.2 Trabajo a Futuro	60
Capítulo 7. Anexos	61
Anexo 1	61
Análisis facial	61
La cara en el plano Mediosagital	61
Altura Facial	61
La Frente	62
Las Cejas	62
Los Ojos	62
La Nariz	62
Relación Nasofacial.	63
Formas de la nariz	64
Los Labios	65
La Barbilla	65
La Oreja	66
El cuello	66
Anexo 2	67
Imágenes de prueba para Betaface	68
Anexo 3	72
Diagramas y Modelos del Sistema	73
Índice de Tablas	77
Índice de Figuras	77
Referencias	79

Capítulo 1

1.1 Introducción

Hasta este año 2019 se incrementó en México el número de usuarios en redes sociales a 83 millones de usuarios, lo que representa casi el 65% de la población de todo el país[1]. Ya es poco común que un habitante de la Ciudad de México no esté presente en al menos una red social y que en esta misma comparta su día a día, opiniones, gustos, fotografías personales y eventos importantes para ellos. Los que estamos presentes en alguna red social podemos intuir que hay demasiada información personal que cedemos al utilizarlas. Información que se procesa para obtener nueva, pero ésta con un enfoque diferente. Las redes sociales terminan por saber sobre nuestros gustos, empleo, actividades, familia entre muchas otras cosas y todo con el fin de ofrecernos productos y servicios basados en esos datos.

En México la cuarta red social más usada es Instagram y ésta se caracteriza por permitir a los usuarios compartir principalmente fotos y videos[2]. A diferencia que las redes que la preceden en popularidad, en ésta red las publicaciones tienen como elemento principal las fotos del usuario.

Así como el crecimiento de usuarios en redes sociales ha aumentado, lamentablemente también lo han sido los casos de delincuencia y homicidio en todo el país. Algunas veces se ha visto en las noticias que los delincuentes, previamente, habían publicado en sus redes sociales la posesión de armas de fuego y la realización de actividades delictivas y éstas sólo se denunciaron hasta que el delito se cometió. Los delincuentes estaban anunciando en las redes sociales sus intenciones y actividades sin que alguna organización realizara acciones preventivas, esto porque no es fácil identificar este tipo de perfiles con publicaciones donde se anuncie un posible delito.

Vivimos en un tiempo donde las tecnologías se unen para crear nuevas y mejores herramientas que ayuden a los problemas que presenta nuestra sociedad. Y si la información que proporcionamos en las redes sociales se puede obtener y procesar para cualquier otro fin, entonces también se podría procesar para ayudar a prevenir futuros casos de delincuencia.

Si en la red social Instagram se pudieran procesar publicaciones donde se exhiben posesión de armas y además un análisis de rasgos faciales para identificar posibles personas violentas, entonces ayudaríamos en sus actividades a instituciones u organizaciones dedicadas a monitorear redes sociales para prevenir delitos.

Se propone en este proyecto un prototipo de motor de búsqueda que pueda ayudar a identificar en Instagram posibles perfiles de usuario violentos con base en 2 análisis: análisis de rostro y reconocimiento de arma corta tipo escuadra.

La finalidad del proyecto es aplicar los conocimientos adquiridos a lo largo de nuestra trayectoria estudiantil en sistemas computacionales, en una herramienta que ayude a tratar la problemática de delincuencia de nuestro país.

1.2 Problemática

Algunos usuarios de redes sociales publican la posesión de armas y realización de actividades delictivas sin que se tomen medidas preventivas por alguna organización o institución.

La problemática que se tratará en el proyecto radica en prevenir delitos que ciertos usuarios pueden manifestar en la red social Instagram.

1.3 Propuesta de Solución

Por medio de un sistema motor de búsqueda, identificar en la red social Instagram, perfiles de usuario con posibles rasgos violentos y que estos resultados de búsqueda ayuden en las actividades de las organizaciones dedicadas a la prevención de delitos cibernéticos en la Ciudad de México. Cómo lo hace La Policía de Ciberdelincuencia Preventiva[23].

1.4 Objetivos

1.4.1 General

Desarrollar un prototipo de motor de búsqueda que permita identificar posibles perfiles violentos con base en las características físicas de su rostro, mediante un análisis facial, y/o reconocimiento de exhibición de armas de fuego tipo escuadra de los usuarios de la red social Instagram en la Ciudad de México y con ésto ayudar en la prevención de delitos cibernéticos que realizan las organizaciones dedicadas a este fin.

1.4.2 Particulares

- Implementar en el prototipo un módulo que permita reconocer rostros de las publicaciones obtenidas de Instagram para análisis facial y con esto determinar e informar si la persona presenta rasgos de una persona posiblemente violenta.
- Obtener una métrica de rostro, mediante la aplicación de varios análisis faciales a delinquentes de la Ciudad de México para usar como base en la detección y análisis de los rostros resultantes de la búsqueda.
- Implementar en el prototipo un módulo que permita detectar armas de tipo escuadra en las publicaciones de los perfiles obtenidos de la búsqueda realizada y con ésto informar si existe posesión de armas en cada perfil.

1.5 Justificación

Ya existen sectores privados y públicos de seguridad, que utilizan las redes sociales como medio para poder identificar a supuestos delincuentes. El procedimiento que siguen es publicar una foto de la persona y después esperar hasta que los usuarios brinden información o que la policía u organización lo identifique antes[3].

Instagram es una de la redes sociales más utilizadas a nivel internacional[4] y su principal funcionalidad es permitir a sus usuarios compartir fotos y videos personales. Si la información que puede proporcionar Instagram se procesa con la finalidad de prevenir delitos, ésta puede ayudar a las instituciones u organizaciones que se dedican a monitorear redes sociales con el mismo fin y tomar las respectivas medidas preventivas.

1.6 Estado del Arte

En la investigación de software, herramientas y motores de búsqueda que actuen sobre Instagram, no se encontró alguna que realice las funcionalidades que propone ANBU (detección y análisis de rostro y detección de arma corta tipo escuadra), sin embargo, existen algunas herramientas que realizan procesos similares en el reconocimiento de imágenes y obtención de datos específicos de la red social. Cabe destacar que muchos de ellos son de código cerrado y no permiten reutilizar sus funciones.

1.6.1 Webstagram

Es un servicio donde puede consultar información sobre su cuenta de Instagram todos los días con las últimas actualizaciones. En el campo de búsqueda, se ingresa el nombre de usuario de Instagram o el enlace de perfil a buscar, como resultado muestra una estadística de todas las acciones que realiza el usuario buscado. Por ejemplo cuantas personas lo siguen, el incremento de likes, sus días de tendencia etc [5].

1.6.2 Yooying

Yooying es un motor de búsqueda que genera resultados a través de hashtags, nombres de usuario, el cual muestra el contenido más popular de la red Instagram. Se puede decir que no es más que una forma de navegar por Instagram sin la necesidad de contar con una cuenta asociada, ya que Yooying no solicita ningún tipo de registro [6].

1.6.3 Metaeyes

MetaEyes es una herramienta de Monitoreo Visual para Instagram que usa Machine Learning y Reconocimiento de Imágenes.

MetaEyes extrae imágenes de Instagram y comprende el contenido de una imagen al encapsular potentes modelos de aprendizaje automático. Clasifica rápidamente las imágenes

en miles de categorías (por ejemplo, "automóvil", "gato", "Torre Eiffel"), detecta objetos individuales y caras dentro de las imágenes. Puede crear metadatos en su catálogo de imágenes, contenido ofensivo moderado o habilitar nuevas campañas de marketing a través del análisis de sentimientos de imagen.

Detecta uno o más rostros humanos en una imagen y obtiene atributos faciales que contienen predicciones de características faciales basadas en el aprendizaje automático. Las características de los atributos faciales disponibles son: detección de edad, sexo, sonrisa, vello facial y gafas.

Detecta y etiqueta automáticamente contenido explícito como contenido para adultos o contenido violento dentro de una imagen [7].

En la Tabla 1 se muestran algunas de las características principales de cada herramienta que se consideró como comparativa de funcionalidades para el prototipo.

Software	Búsqueda de Perfiles	Búsqueda Global	Gratis	Reconocimiento Facial	Reconocimiento de arma de fuego
Webstagram	Si	Si	Si	No	No
Yooying	Si	No	Si	No	No
Metaeyes	Si	Si	No	Si	No

Tabla 1.6 Comparativa de funcionalidades de herramientas

Fuente: creación propia.

1.7 Alcance

El prototipo ANBU podrá realizar búsquedas de perfiles en la red social Instagram, con base en cierto parámetros de búsqueda como: nombre, username y ubicación. De los perfiles públicos resultantes, extraer el mayor número de publicaciones para realizar la detección de rostros, análisis facial y la detección de arma corta tipo escuadra, con el fin de informar si algún perfil resultante presenta características de un posible perfil violento. Ésta información puede ser útil a las organizaciones dedicadas a prevenir delitos en las redes sociales, como por ejemplo, la Policía de Ciberdelincuencia Preventiva de la Ciudad de México.

Capítulo 2. Marco Teórico

En este capítulo se describe Instagram como aplicación, un poco de su historia, así como sus características principales, como lo son los tipos de perfil, y las publicaciones realizadas. Por otro lado se describe la API “Instagram Basic Display API” la cual nos permite acceder a los datos descritos en Instagram, mostrando cuáles son los permisos y limitaciones que nos ofrece.

De igual forma se describen las principales características que lleva a cabo el análisis facial y la descripción de lo que es un arma corta tipo escuadra.

2.1 Instagram

Instagram es una aplicación móvil y red social que ofrece a los usuarios compartir fotos y videos. Fue un éxito desde su lanzamiento con más de un millón de usuarios registrados en sus primeros 2 meses.

Instagram fue desarrollado en San Francisco por Kevin Systrom y Mike Krieger. Crearon una aplicación prototipo de una idea que originalmente se llamó Burbn, que permitía a las personas registrarse en su aplicación web móvil.

Decidieron que la aplicación era muy similar a otras aplicaciones móviles ya establecidas, por lo que se centraron únicamente en la comunicación a través de imágenes. Eliminaron todas las funciones de la aplicación, excepto subir fotos, comentar y dar me gusta. Se renombró Instagram que se refería al hecho de que los usuarios estaban enviando un tipo de telegrama instantáneo.

Instagram se lanzó el 6 de Octubre de 2010 y su crecimiento fue casi instantáneo. De un puñado de usuarios, pronto se convirtió en la aplicación de fotografía número uno que reunió a 100,000 usuarios en una semana, aumentando a 1 millón en dos meses. Según Kevin Systrom, la aplicación en sí tardó sólo ocho semanas en construirse, pero fue el resultado de más de un año de trabajo. Facebook lo compró por mil millones de dólares en 2012. Ahora tiene más de 600 millones de usuarios activos y sigue aumentando rápidamente.[8]

2.1.1 Perfil de Usuario

Existen múltiples tipos de cuentas de Instagram, éstas dependen del tipo de publicaciones que se quieren hacer y a quién van dirigidas [9]. Los tipos de cuenta de acuerdo a su giro son:

- Cuenta personal.
- Blog.
- Público (comunidad temática).
- Tiendas de Internet y tiendas fuera de línea.
- Cuentas comerciales (cafeterías y restaurantes, agencias turísticas, manufactura, etc.)

- Cuentas de marca.
- Cuentas de famosos.
- Bots
- Cuentas de desembarco.
- Cuentas de vídeo.

Estos perfiles pueden ser públicos (visibles para cualquiera que los busque) o privados (sólo el dueño de la cuenta puede aceptar quién puede ver el contenido). La forma en que se ven todos los perfiles se muestra en la figura 2.1.1

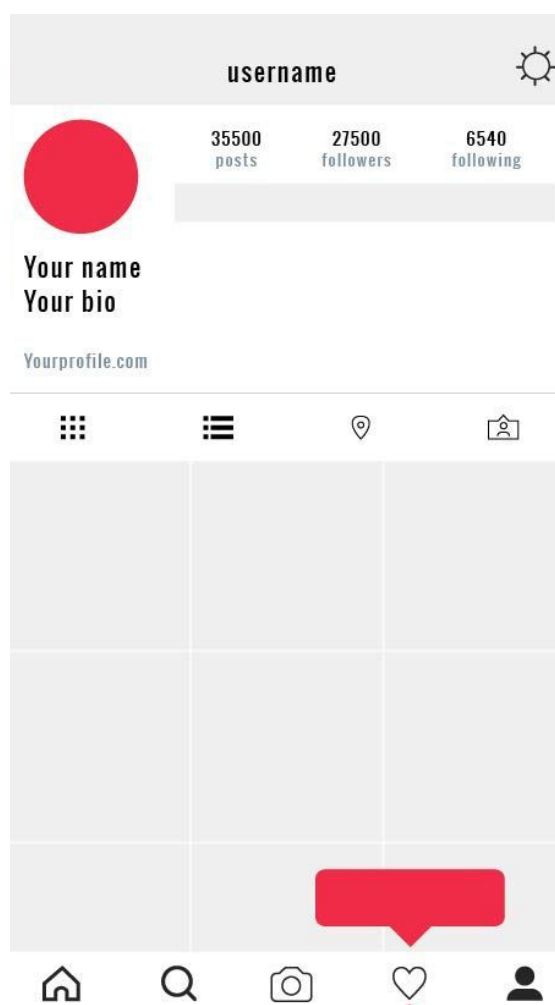


Figura 2.1.1 Perfil de usuario [9]

La información que se puede obtener, independientemente del tipo de cuenta y de la privacidad de la misma, es la que se muestra en la imagen anterior. En la parte superior encontramos el nombre de usuario que es único. Se observa en color rojo la imagen de perfil. A la derecha se encuentra el número de publicaciones realizadas por el usuario, seguido del número de seguidores y del número de perfiles a los que sigue. Debajo de la foto de perfil se encuentra el nombre de la persona, seguido de una breve descripción de quién es. Debajo de la descripción se encuentra un enlace elegido por el usuario, ya sea a un sitio web en particular o a su perfil de otra red social. En caso de ser un perfil público nos encontramos con las publicaciones del usuario que se pueden ver en forma de mosaico o de lista, por ubicación y finalmente las publicaciones en las que aparece y ha sido etiquetado.

2.1.2 Publicaciones

Como cabecera de la publicación tenemos primero la imagen de perfil y el nombre del usuario que la publicó, seguido de la ubicación que es opcional. Posteriormente encontramos las imágenes de dicha publicación, que pueden ser desde 1 hasta 10 elementos de foto o vídeo de no más de 1 minuto cada uno. Abajo tenemos los íconos de “Like” (Me gusta), Comentar y Enviar. Debajo se encuentra el contador de personas que indicaron que les gusta esa publicación, seguido del nombre del usuario y la descripción de la publicación. Esta descripción puede ir vacía o con texto, y éste texto a su vez puede contener etiquetas o “Hashtags”. Finalmente aparecen los comentarios que otras personas realizaron acerca de esa publicación, en la figura 2.1.2 se pueden apreciar las características anteriores.

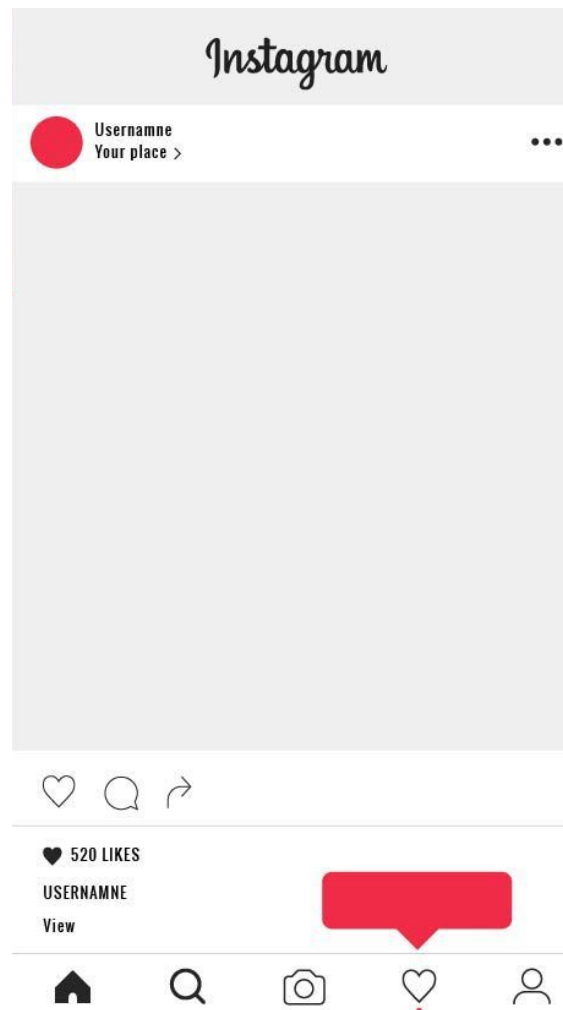


Figura 2.1.2 Publicación de usuario [9]

2.2 Instagram Basic Display API

Instagram Basic Display API (Pantalla Básica de Instagram). Permite a los usuarios de nuestra aplicación obtener, la información básica de cada perfil, fotos y videos en sus cuentas de Instagram.[10]

Permisos:

- Obtener un token de acceso de usuario de Instagram y permisos de un usuario de Instagram.
- Obtener el perfil de un usuario de Instagram.
- Obtener las imágenes, videos y álbumes de un usuario de Instagram.

Limitaciones:

- No se puede usar la API para crear cuentas de usuario o iniciar sesión en una aplicación.
- Las historias no son compatibles.
- Los comentarios no son compatibles.
- Las ideas no son compatibles.
- Las publicaciones promocionadas que contienen medios de Instagram no son compatibles.
- El depurador de tokens de acceso de API Graph no admite tokens de acceso de usuario de Instagram.

2.3 Análisis facial

La Imagenología Computacional es el proceso por el cual se optimiza el estudio de las proporciones faciales [11]. Los puntos que son tomados para el análisis facial se muestran en la figura 2.3.1



Figura 2.3.1 Puntos clave en el análisis facial [11]

Descripción de los puntos faciales:

- **Plano horizontal de Frankfort:** Línea que se dibuja desde el aspecto superior del canal auditivo externo hasta el punto más inferior del borde infraorbital mientras que los ojos de la persona están en forma paralela con respecto al piso.
- **Trichion (Tr):** Es el punto en el plano medio sagital donde se inicia la línea de implantación del pelo.

- **Glabela (G):** Es la zona más prominente de la frente en el plano mediosagital
- **Mentón (Me):** Es el punto más bajo del tejido blando de la barbilla.
- **Nasion (N):** Depresión profunda donde se unen la piel de la frente con la raíz de la nariz
- **Surco Mentolabial (Si):** Zona más posterior entre el labio inferior y la barbilla.
- **Punto Subnasal (Sn):** Donde termina la columela (base) y comienza el labio superior.
- **Pogonion (Pg):** Punto más prominente del tejido blando de la barbilla

Para obtener más información sobre las características faciales consultar el Anexo 1.

2.3.1 Rasgos faciales

La Morfopsicología o Psicomorfolología es una pseudociencia que se encarga de estudiar el carácter, las tendencias y el estado emocional de una persona a través de la lectura del rostro o los rasgos faciales. [12]

Un análisis de Psicomorfolología toma los siguientes aspectos del rostro de una persona.

- Principales
 - Esqueleto facial
 - Triángulo del rostro
 - Masa muscular
- Secundarios
 - Simetría facial

2.3.2 Análisis Morfopsicológico e Imagenológico de una persona violenta

En un artículo sobre asesinos seriales se cita el libro “*Las caras del mal*” escrito por la periodista y escritora Mónica G. Álvarez donde la escritora define la Morfopsicología como una ciencia que analiza las estructuras faciales y las relaciona con la personalidad. Éste mismo artículo también muestra las principales características Morfopsicológicas de 9 asesinos seriales famosos, según Paloma Ramón experta en Morfopsicología[13].

Las características se muestran en la siguiente tabla 2.

La Imagenología se define como el conjunto de técnicas y procedimientos para obtener imágenes del cuerpo humano para utilizarse con fin médico o científico[24]. Para nuestro proyecto nos referimos al análisis imagenológico como el resultado de medición de las características del rostro después de analizar la foto presentada con la herramienta Betaface que se describe en el capítulo 3.

Rostro	Análisis Morfopsicológico	Análisis Imagenológico
1(figura 2.3.2)	La forma de su cara, abrupta y angulosa, frente alta, hendiduras en las sienes, marcadas aletas vibrantes de la nariz (nariz de toro), falta de carnosidad, asimetría en los hemisferios faciales[13].	arched eyebrows (cejas arqueadas) : no (100%) big lips (labios grandes) : no (44%) big nose (nariz grande) : yes (3%) bushy eyebrows (cejas pobladas) : no (91%) double chin (barbilla partida) : no (100%) high cheekbones (pómulos altos): no (82%) oval face (rostro ovalado) : yes (3%) pointy nose (nariz puntiaguda) : no (76%) receding hairline (entradas): no (32%)
2(figura 2.3.3)	Su frente ancha, panorámica y alta, ángulos rectos en su mandíbula, nariz con aleta vibrante, su boca es demasiado pequeña para la anchura de la zona instintiva, la asimetría entre los hemisferios derecho e izquierdo[13]	arched eyebrows (cejas arqueadas) : no (100%) big lips (labios grandes) : no (14%) big nose (nariz grande) : yes (33%) bushy eyebrows (cejas pobladas) : no (10%) double chin (barbilla partida) : no (100%) high cheekbones (pómulos altos): no (73%) oval face (rostro ovalado) : no (3%) pointy nose (nariz puntiaguda) : no (18%) receding hairline (entradas): no (87%)
3(figura 2.3.4)	El marco de su cara, muy anguloso, las cejas prominentes y bastante pobladas, la aleta vibrante de su nariz, poca carnosidad, por no decir nula en sus mejillas[13]	arched eyebrows (cejas arqueadas) : no (49%) big lips (labios grandes) : no (9%) big nose (nariz grande) : yes (17%) bushy eyebrows (cejas pobladas) : yes (100%) double chin (barbilla partida) : no(63%) high cheekbones (pómulos altos): no (44%) oval face (rostro ovalado) : yes

		(32%) pointy nose (nariz puntiaguda) : no (15%) receding hairline (entradas): no (46%)
4(figura 2.3.5)	Asimetría entre los dos hemisferios de la cara, gran atonía en los ojos, nariz ancha en la punta, boca átona.[13]	arched eyebrows (cejas arqueadas) : no (76%) big lips (labios grandes) : no (43%) big nose (nariz grande) : yes (100%) bushy eyebrows (cejas pobladas) : yes (38%) double chin (barbilla partida) : no (66%) high cheekbones (pómulos altos): no (64%) oval face (rostro ovalado) : yes (31%) pointy nose (nariz puntiaguda) : yes (30%) receding hairline (entradas): no (59%)
5(figura 2.3.6)	Estructura ósea (marco facial) y los receptores (boca, nariz, ojos), frente ancha y un poco alta en retracción lateral, diferencia entre los hemisferios, la mandíbula cuadrada, boca pequeña, y ojos con tonicidad enorme. [13]	arched eyebrows (cejas arqueadas) : no (100%) big lips (labios grandes) : no (49%) big nose (nariz grande) : yes (74%) bushy eyebrows (cejas pobladas) : no (92%) double chin (barbilla partida) : yes (41%) high cheekbones (pómulos altos): no (52%) oval face (rostro ovalado) : no (13%) pointy nose (nariz puntiaguda) : no (96%) receding hairline (entradas): yes (75%)

Tabla 2.3 Análisis de un rostro violento

Fuente: creación propia

Imágenes de los rostros descritos en la Tabla 2



Figura 2.3.2 Rostro 1

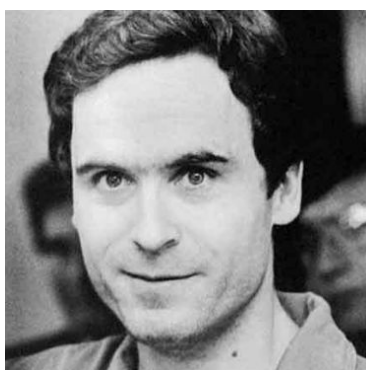


Figura 2.3.3 Rostro 2



Figura 2.3.4 Rostro 3



Figura 2.3.5 Rostro 4

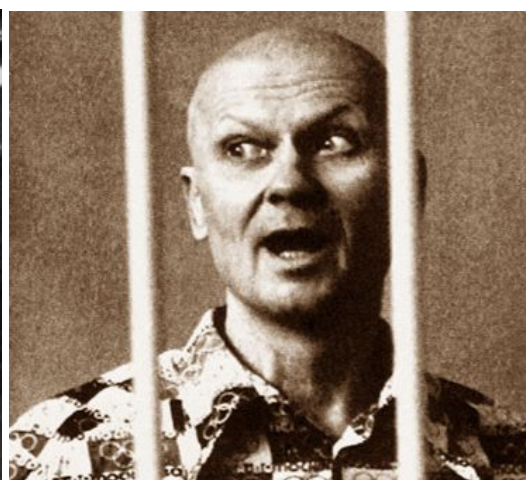


Figura 2.3.6 Rostro 5

Considerando los resultados devueltos por la herramienta Betaface, se puede observar que no existe un conjunto de características comunes que pertenezcan a los asesinos. Por lo que podemos intuir que no hay rasgos exactos que defina un asesino o un delincuente. Dicho lo anterior y sumando que la Morfopsicología es una pseudociencia, no nos basaremos en los criterios que ésta propone y tampoco en los resultados que arrojó la herramienta Betaface sobre estos rostros.

También otro aspecto a considerar es que los rasgos faciales de los delincuentes de la Ciudad de México, difieren de los presentados en la tabla 2 (Estadounidenses) por lo que se optará por analizar rostros de personas detenidas por asalto, secuestro y asesinato en la Ciudad de México y el Estado de México y con base en los resultados, generar una métrica comparativa que determinará si el rostro analizado pertenece a una persona posiblemente violenta.

2.4 Arma Corta Tipo Escuadra

Las armas tipo escuadra son las más comunes de encontrar o fácil de adquirir:

En periódicos como Excélsior, el Universal y otros, se menciona que incluso la venta y compra de las mismas es abundante en México esto por su tamaño y fácil adquisición de municiones [14].

Descripción de un arma tipo escuadra:

- Pueden ser disparadas por una sola mano.
- Calibre pequeño que va de 20 mm, 11 mm, 9 mm, etc.
- Se clasifican como uso de defensa personal.
- Son de fabricación industrial, es decir pasan por pruebas de calidad para poder obtener un certificado.
- Se llama pistola si carece recamaras giratorias.
- Las más modernas son semiautomáticas.
- Rango de distancia de 10 a 50 metros.

Imágenes de ejemplo arma tipo escuadra



Figura 2.4.1 Ejemplo 1 arma corta [15]



Figura 2.4.2 Ejemplo 2 arma corta [14]

Capítulo 3. Tecnologías de Desarrollo

En el presente capítulo se describen las herramientas que se usarán para el desarrollo del motor de búsqueda, los componentes externos al sistema que ayudarán en la detección y análisis de rostro y la detección de arma corta, así como las tecnologías para instanciar el sistema y que pueda dar el servicio. Como tecnologías principales usaremos: API de Instagram, la cual nos permitira el acceso a los datos de la aplicación Instagram; Betaface para el análisis y reconocimiento de rostros; TensorFlow para el reconocimiento de armas cortas tipo escuadra; Apache HTTP para montar el sistema brindar los servicios y Flask como framework por su compatibilidad con Python 3.

Se eligió el lenguaje de programación Python por su creciente uso en distintos sistemas y su característica multiparadigma que nos ayudará a implementar las diferentes herramientas en el mismo sistema[25].

3.1 API de Instagram

Como herramienta la API de Instagram nos brindará los datos necesarios para los análisis tanto facial como de arma corta.

Con fines de desarrollo se usará un modo Sandbox Mode, este modo es un entorno totalmente funcional que permite probar la API antes de enviar la aplicación para su revisión. El modo Sandbox nos permite lo siguiente.

- Las aplicaciones en sandbox están restringidas a 10 usuarios
- Los datos están restringidos a los 10 usuarios y a los 20 medios más recientes de cada uno de esos usuarios.
- Límites de tasa API reducidos

Para ello es necesario realizar un autenticación por medio del protocolo OAuth 2.0, tomando en cuenta que todas las solicitudes a la API deben realizarse a través de SSL (<https://> not <http://>).

3.1.1 Requisitos para la autenticación

- La autenticación permite realizar solicitudes en nombre de un usuario, para ello es necesario un `access_token`.
- Un `access_token` son exclusivos de un usuario y deben ser almacenados de forma segura, también pueden caducar en cualquier momento.

Proceso para recibir un `access_token`:

1. Dirigir al usuario a url de autorización
 - a. Se solicita al usuario iniciar sesión.
 - b. Se preguntará al usuario si desea otorgar a nuestra aplicación el acceso a sus datos.

- c. El servidor redirigirá al usuario.
- 2. Server-side flow
 - a. Se redirigirá al usuario a una URL
`https://api.instagram.com/oauth/authorize/?client_id=CLIENT-ID&redirect_uri=REDIRECT-URI&response_type=code`
 - b. En este punto, le presentamos al usuario una pantalla de inicio de sesión y luego una pantalla de confirmación para otorgarle a su aplicación acceso a sus datos de Instagram.
- 3. Recibe la redirección de Instagram.
 - a. Una vez que un usuario autoriza su aplicación, emitimos una redirección a su `redirect_uri` con un parámetro de código. `http://your-redirect-uri?code=CODE`
 - b.

URI DE REDIRECCIONAMIENTO REGISTRADO	REDIRECT_URI PARÁMETRO PASADO A / AUTORIZAR	¿Válido?
<code>http://yourcallback.com/</code>	<code>http://yourcallback.com/</code>	si
<code>http://yourcallback.com/</code>	<code>http://yourcallback.com/?this=that</code>	si
<code>http://yourcallback.com/?this=that</code>	<code>http://yourcallback.com/</code>	no
<code>http://yourcallback.com/?this=that</code>	<code>http://yourcallback.com/?this=that&another=true</code>	si
<code>http://yourcallback.com/?this=that</code>	<code>http://yourcallback.com/?this=that&another=true</code>	no
<code>http://yourcallback.com/callback</code>	<code>http://yourcallback.com/</code>	no
<code>http://yourcallback.com/callback</code>	<code>http://yourcallback.com/callback?type=mobile</code>	si

Tabla 3.1 URI de redireccionamiento API Instagram

- c. Si el usuario rechaza su solicitud de aprobación, lo redirigiremos a su `redirect_uri` con los siguientes parámetros:
 - i. `error : access_denied`
 - ii. `error_reason : user_denied`
 - iii. `error_description : el usuario rechazó su solicitud`
`http://your-redirect-uri?error=access_denied&error_reason=user_denied&error_description=The+user+denied+your+request`
- 4. Solicitud del `access_token`
 - a. Se debe intercambiar el código que fue recibido en el paso anterior por un token de acceso. Para realizar este intercambio, se debe de publicar el código, junto con algunos parámetros de identificación de la aplicación.

b. Parámetros requeridos:

- i. ID_cliente : su ID de cliente
- ii. client_secret : el secreto de tu cliente
- iii. grant_type : authorization_code es actualmente el único valor admitido
- iv. redirect_uri : el redirect_uri que utilizó en la solicitud de autorización.
Nota: este tiene que ser el mismo valor que en la solicitud de autorización.
- v. código : el código exacto que recibió durante el paso de autorización.

Ejemplo de una petición de acces_token:

```
curl -F 'client_id=CLIENT_ID' \  
-F 'client_secret=CLIENT_SECRET' \  
-F 'grant_type=authorization_code' \  
-F 'redirect_uri=AUTHORIZATION_REDIRECT_URI' \  
-F 'code=CODE' \  
https://api.instagram.com/oauth/access_token
```

Figura 3.1.1 Petición de acces_token

fuentes: creación propia

Si la solicitud realizada obtuvo éxito, el access_token obtenido será como el siguiente

```
{  
  "access_token": "fb2e77d.47a0479900504cb3ab4a1f626d174d2d",  
  "user": {  
    "id": "1574083",  
    "username": "snoopdogg",  
    "full_name": "Snoop Dogg",  
    "profile_picture": "..."  
  }  
}
```

Figura 3.1.2 Respuesta de acces_token

fuentes: creación propia

3.2 Betaface

Para el desarrollo del sistema, se necesitará el uso de una herramienta capaz de identificar rostros en una primera instancia. En este caso una de las herramientas que se encontró fue Betaface.

¿Qué es Betaface?

‘Betaface API’ es un servicio web de detección y reconocimiento de rostros. Puede escanear archivos de imagen cargados o URL de imágenes, encontrar caras y analizarlas. La API también proporciona servicios de verificación (comparación de rostros) e identificación (búsqueda de rostros), así como también puede mantener múltiples bases de datos de reconocimiento definidas por el usuario (espacios de nombres).

Información general de los rostros:

- Detección de caras múltiples (posiciones, tamaños, ángulos).
- 123 ubicaciones de puntos de referencia (22 básicos, 101 pro).
- Imágenes de la cara recortadas.

Clasificación:

- Estimar género, edad, etnia, emoción (sonrisa / neutral)
- Detectar anteojos, bigote y barba

Mediciones extendidas:

- Descripción de las características faciales y faciales (forma, tamaño relativo y ubicación)
- Ojos, cabello, piel, ropa y colores de fondo
- Cantidad de vello facial
- Peinado aproximado (longitud, grosor, forma)

Cuenta con 5 planes de suscripción, desde el gratuito sin registro que incluye el análisis de 500 imágenes diarias, hasta 300,000 por 1300 euros al mes.

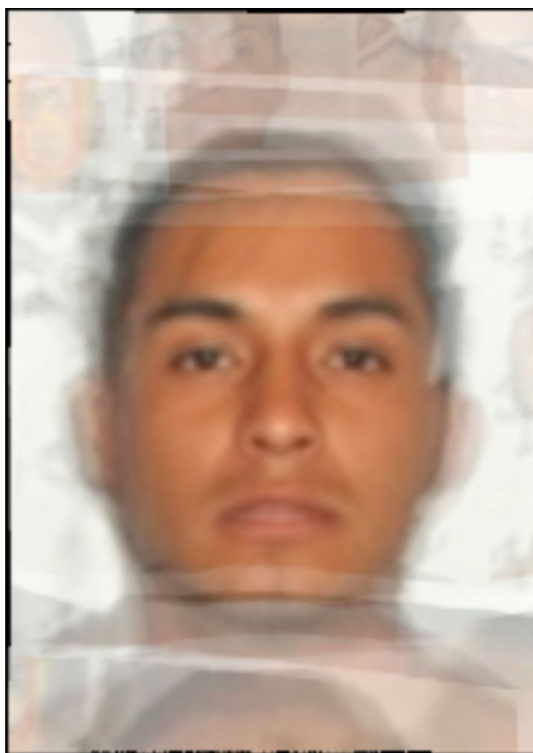
En la página oficial se encuentra la documentación debida para el uso de la API, se muestran algunas operaciones en la Tabla 3.2.

Uri	Method	Description
*	OPTIONS	CORS support
FaceInfo_Delete	POST	FaceInfo_Delete
FaceInfo_New	POST	FaceInfo_New
FaceInfo_SetFaceImagePoints	POST	FaceInfo_SetFaceImagePoints
FaceInfo_SetPoints	POST	FaceInfo_SetPoints
FaceInfo_SetTags	POST	FaceInfo_SetTags
FaceInfo_Update	POST	FaceInfo_Update
GetFaceImage	POST	Retrieve cropped face image and points coordinates in cropped face image coordinates
GetImageFileInfo	POST	Retrieve image and faces information or processing status using image file SHA-256 hash code
GetImageInfo	POST	Retrieve image and faces information or processing status
GetRecognizeResult	POST	Get results of recognition request or processing status
GetTransformResult	POST	GetTransformResult
GetVerifyResult	POST	GetVerifyResult
RecognizeFaces	POST	Execute recognition request for each of face ids and specified list of targets (comma separated list either of face ids, or persons and namespaces as name@namespace.com or all@namespace.com)
SetPerson	POST	Assign person name (John Doe@mynamespace.com) to one or more face ids

Tabla 3.2 Operaciones de la API de Betaface [16]

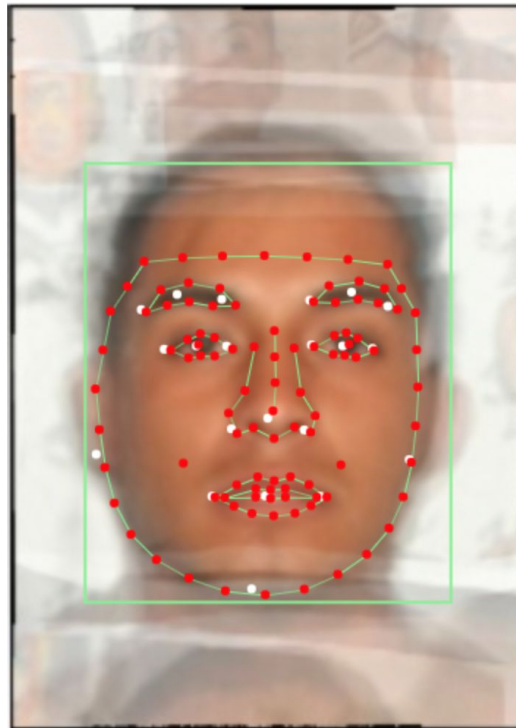
Después de obtener los datos de esta herramienta y para determinar si un rostro es o no violento, se analizaron más de 70 rostros de responsables de hechos ilícitos capturados por la Fiscalía General de Justicia del Estado de México con esta API, y se muestran en el Anexo 2.

Posteriormente utilizando la llamada 'TransformFaces' de la API de Betaface, se obtiene un rostro promedio que combina las características de todos los rostros antes mencionados, ver figura 3.2.1.



*Figura 3.2.1 Rostro Promedio Betaface
fuente: creación propia*

Al ingresar esa imagen a la API de Betaface, obtenemos los siguientes resultados:



*Figura 3.2.2 Obtención de los 101 puntos faciales
fuente: creación propia*

Y de los datos obtenidos, prescindiendo de aquellos que no corresponden a las características físicas del rostro (por ejemplo: color de cabello, uso de collar, aretes o sombrero) tenemos:

arched eyebrows (cejas arqueadas)	: no (69%)
big lips (labios grandes)	: no (70%)
big nose (nariz grande)	: yes (11%)
bushy eyebrows (cejas pobladas)	: yes (11%)
double chin (barbilla partida)	: yes (22%)
high cheekbones (pómulos altos)	: no (63%)
oval face (rostro ovalado)	: yes (20%)
pointy nose (nariz puntiaguda)	: no (80%)
receding hairline (entradas)	: yes (11%)

Figura 3.2.3 Descripción de los puntos faciales por Betaface

De modo que si se igualan o rebasan esos parámetros, éste será catalogado como posible rostro violento.

3.3 TensorFlow

Para el desarrollo del módulo de análisis de imágenes que hará el reconocimiento de arma corta tipo escuadra se utilizará la herramienta TensorFlow.

TensorFlow es la plataforma de Aprendizaje Profundo más importante del mundo. Este desarrollo open-source de Google va más allá de la Inteligencia Artificial, pero su flexibilidad y gran comunidad de desarrolladores lo ha posicionado como la herramienta líder en el sector del Deep Learning.

¿Qué es TensorFlow?

TensorFlow es una biblioteca de software de código abierto para computación numérica, que utiliza gráficos de flujo de datos. Los nodos en las gráficas representan operaciones matemáticas, mientras que los bordes de las gráficas representan las matrices de datos multidimensionales (tensores) comunicadas entre ellos.[18]

TensorFlow es una gran plataforma para construir y entrenar redes neuronales, que permiten detectar y descifrar patrones y correlaciones, análogos al aprendizaje y razonamiento usados por los humanos.

La arquitectura flexible de TensorFlow le permite implementar el cálculo a una o más CPU o GPU en equipos de escritorio, servidores o dispositivos móviles con una sola API. TensorFlow fue desarrollado originalmente por investigadores e ingenieros que trabajaban en el equipo de Google Brain Team, dentro del departamento de investigación de Machine Intelligence, con el propósito de llevar a cabo el aprendizaje automático y la investigación de redes neuronales profundas.

Sin embargo, el sistema es lo suficientemente general como para ser aplicable a una amplia variedad de otros dominios igualmente.

En mayo de 2016 Google anunció TPU (Tensor Processing Unit). Se trata de una construcción ASIC específica para el aprendizaje automático y adaptada para TensorFlow.

El TPU es un acelerador de Inteligencia Artificial programable, orientado para utilizar o correr modelos más que para entrenarlos. Google anunció que habían usado TPUs en sus centros de datos durante más de un año, descubriendo que su rendimiento era 10 veces mayor (energéticamente) en tareas de aprendizaje automático que los sistemas tradicionales.

Algunos ejemplos de aplicación de TensorFlow:

1. Para mejorar la fotografía de los smartphones

Una de las aplicaciones más interesantes está en los teléfonos. Por ejemplo, el Píxel 2 que se lanzó este año, incluye efecto bokeh con una sola cámara. Se crea un modo retrato que separa a la persona del fondo, cuando esto era algo reservado para dispositivos con doble cámara. Y esto se consigue con el TensorFlow de Machine Learning, entrenando un modelo de TensorFlow en el backend, pero también ejecutándose en el propio teléfono. No es tarea sencilla.

2. Para ayudar al diagnóstico médico

El sector de la salud es uno de los campos que más se están revolucionando y que mayor impacto tendrá para todos nosotros como sociedad en los próximos años. TensorFlow ya está mejorando las herramientas que utilizan los médicos, por ejemplo ayudándoles a analizar radiografías. El Deep Learning va a permitir a los facultativos médicos pasar más tiempo con los pacientes, además de permitirles hacer actividades más interesantes y emocionantes. El Deep Learning podría estar en los dispositivos que llevan los médicos con ellos, por lo que definitivamente hay necesidad de que TensorFlow funcione en gran variedad de dispositivos.

3. Procesamiento de imágenes

Una de las aplicaciones más conocidas de TensorFlow es el software automatizado de procesamiento de imágenes, DeepDream. Se trata de un programa de visión artificial creado por el ingeniero de Google Alexander Mordvintsev, que utiliza una red neuronal convolucional para encontrar y mejorar patrones en imágenes mediante pareidolia algorítmica, creando así una apariencia alucinógena, similar a un sueño, creando imágenes deliberadamente sobre procesadas.

En nuestro caso, utilizaremos COCO-SSD, un modelo previamente entrenado portado para TensorFlow. Para explicarlo, echemos un vistazo a lo que significa cada término - "COCO" y "SSD".

COCO significa "Common Objects in Context" (Objetos comunes en contexto), y son los datos sobre los que se entrenó el modelo. Esta colección de imágenes se utiliza principalmente para la detección de objetos, la segmentación y los subtítulos, y consta de más de 200 mil imágenes etiquetadas que pertenecen a una de las 90 categorías diferentes, como "persona", "autobús", "cebra" y "raqueta de tenis".

Luego, está el término "SSD", que señala la arquitectura del modelo. SSD significa "Single Shot Detector", y es una arquitectura de red neuronal hecha de una única red neuronal convolucional de avance que predice las etiquetas de los objetos de la imagen y su posición durante la misma acción. La contraparte de esta característica de "disparo único" es una

arquitectura que utiliza un "generador de propuestas", un componente cuyo propósito es buscar regiones de interés dentro de una imagen.[19]

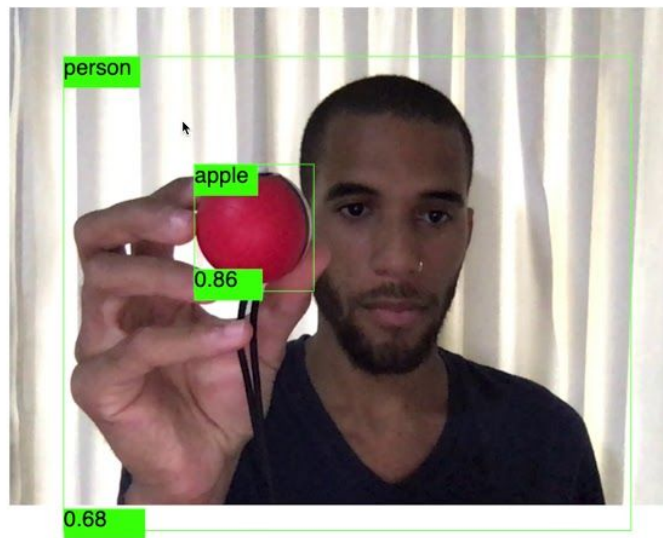


Figura 3.3 Ejemplo COCO-SDD [19]

3.4 Apache HTTP Server

El motivo por el cual se usará Apache HTTP Server es por ser de licencia y código abierto además de su popularidad para implementar sitios web. Esto supone una ventaja en la documentación disponible para su mantenimiento y ejecución.

Apache es un software de servidor web gratuito y de código abierto, se lanzó en 1995 y ha sido el servidor web más popular en Internet desde abril de 1996. En febrero de 2015 celebró su vigésimo cumpleaños como proyecto. [23]

Sus principales características son:

- Soporte de seguridad SSL y TLS.
- Puede realizar autenticación de datos utilizando SGDB.
- Puede dar soporte a diferentes lenguajes, como Perl, PHP, Python y tcl.

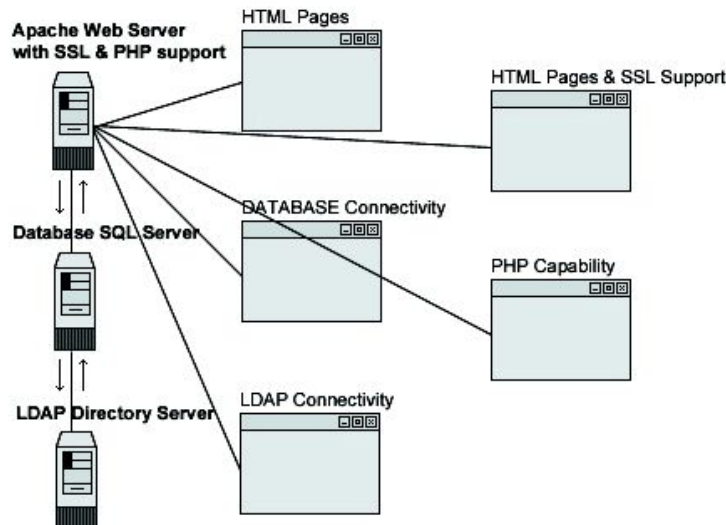


Figura 3.4 Server Apache [21]

3.5 Flask

Para el motor de búsqueda ANBU, Flask es una de las mejores opciones, por ser un framework ligero a diferencia de Django, al igual la documentación y ejemplos que se encuentran en la red son fáciles de reutilizar. Su compatibilidad con python es una de las principales causas por las que se elige el framework ya que tanto las herramientas Betaface y TensorFlow están desarrolladas en este lenguaje.

Flask es un framework ligero de aplicación web que permite la implementación con python. Está basado en la especificación WSGI de Werkzeug y el motor de templates Jinja2 y tiene una licencia BSD [22].



Figura 3.5 Logo framework Flask [22]

Características:

- Es un micro framework
- Contiene un servidor web de desarrollo.
- Depurador y soporte para pruebas unitarias.
- Compatible con wsgi (protocolo para servir páginas web en python)
- Manejo de rutas
- Soporte de cookies seguras de forma nativa.
- Sirve para construir servicios como APIs REST, o aplicaciones de contenido estático.
- Es Open Source amparado por una licencia BSD.

Capítulo 4. Análisis de Software

En este capítulo se presenta el análisis del sistema contemplando las funcionalidades de este y con base en esas ideas se generaron las reglas del negocio, requerimientos del sistema, análisis de riesgos, casos de uso y modelado de la base de datos.

4.1 Reglas del Negocio

Dentro de las reglas del negocio la acción “Realizar Búsqueda” se entiende como el proceso de ingresar los datos básicos de búsqueda del perfil de Instagram como: nombre, username y/o ubicación y con base en ellos mostrar los perfiles de Instagram coincidentes, así como la evaluación del sistema para el análisis facial y la detección de fotos con arma corta tipo escuadra.

Con el término “Perfil” nos referimos a una cuenta de la red social Instagram.

Id	Nombre	Descripción	Tipo
RN1	Ingreso de campos para Búsqueda	Para realizar una búsqueda es necesario ingresar al menos un username o nombre de persona de los perfiles a buscar.	Restricción
RN2	Cantidad de perfiles resultantes de la búsqueda	Se mostrarán a lo máximo 20 perfiles resultantes por búsqueda.	Restricción
RN3	Privacidad de perfil pública para análisis	Los perfiles que empataron con algún parámetro de búsqueda pueden ser de tipo públicos o privados. El sistema sólo considerará para análisis los perfiles de tipo públicos.	Restricción
RN4	Unicidad de perfiles resultantes en una búsqueda	Todos los perfiles resultantes de la búsqueda realizada deben ser únicos y	Restricción

		no repetidos para esa búsqueda en específico	
RN5	Cantidad máxima de fotos de perfil para análisis	Por cada perfil resultante en la búsqueda realizada, se contemplarán a lo máximo 20 fotos tanto para el análisis facial y el análisis de arma corta.	Restricción
RN6	Tipo de arma corta en análisis de arma	El sistema sólo reconocerá, en las fotos de perfil, el arma corta tipo escuadra.	Observación
RN7	Determinación de perfil violento	Si el análisis facial arroja un resultado positivo se calificará como posible perfil violento. Si el análisis de arma arroja un resultado positivo se calificará como posible perfil violento. Si ambos análisis resultan positivos se calificará el perfil como potencialmente violento.	Observación
RN8	Sin perfiles resultantes en la búsqueda	El sistema puede no encontrar perfiles que cumplan con la privacidad de perfil o con los parámetros ingresados para realizar la búsqueda.	Restricción
RN9	Múltiples rostros en publicaciones del perfil	Si en alguna foto de las publicaciones del perfil a analizar se encuentra un grupo de personas, el	Observación

		sistema deberá hacer el análisis facial de cada rostro detectable e indicar la evaluación que tiene para cada uno.	
RN10	Solo rostros del género masculino	Los rostros que se analizarán con las características de un rostro facial violento solo abarcan al género masculino, esto no impide la detección de rostros femeninos pero si se descartaran.	Restricción
RN11	Generación de reportes	Los reportes deben contener todos los datos referentes a la búsqueda; fecha, nombre ingresado, username ingresado, ubicación ingresada, número de resultados, número de perfiles calificados como potencialmente violentos, número de perfiles calificados como posiblemente violentos, nombres de perfiles resultantes y username de perfiles resultantes.	Observación

Tabla 4.1 Reglas de Negocio.

4.2 Requerimientos del Sistema

Los requerimientos del sistema se realizaron con base en las reglas de negocio que se describen en la sección anterior 4.1 Reglas del Negocio. Estos requerimientos se dividen en funcionales como en no funcionales.

Los requisitos funcionales describen las funcionalidades básicas que debe realizar el sistema. Los requisitos no funcionales describen las posibles funcionalidades o características no obligatorias o necesarias para que el sistema cumpla con sus funciones principales. Dentro de estos se clasifican como Propuesto para los requerimientos que se pueden implementar en un futuro o que otorgarían características funcionales extra. La clasificación Definido implica que el sistema tendría que implementar esa característica pero no necesariamente al no implementarla afecta en las funcionalidades básicas.

4.2.1 Requerimientos Funcionales

Id	Nombre	Descripción	Origen
REQF1	Realizar búsquedas con base en los campos introducidos	El sistema debe ser capaz de buscar en Instagram los perfiles que empaten con alguno de los campos de búsqueda ingresados; nombre, username, ubicación.	RN1,RN3,RN4
REQF2	Búsqueda por campo ubicación	Para incluir el campo ubicación en la búsqueda de perfiles se debe ingresar previamente un nombre o username.	RN1
REQF3	Informe de resultados de búsqueda	Una vez realizada la búsqueda el sistema debe mostrar la información de los perfiles resultantes, o en caso contrario, indicar que no hubo alguna coincidencia.	RN2,RN8, RN11

REQF4	Información de la cuenta	De cada perfil resultante de la búsqueda, se desplegará la información de la misma: username, nombre, biografía, enlaces a las fotos analizadas y la evaluación del motor como posible persona violenta.	RN7
REQF5	Enlaces a las fotos con resultados positivos en el análisis facial y en el análisis de detección de arma corta	En los resultados de búsqueda el sistema debe incluir los enlaces externos a las fotos del perfil que fueron analizadas y donde el sistema detectó presencia de arma corta tipo escuadra y/o resultado positivo al análisis facial.	RN5,RN6, RN7, RN10
REQF6	Registro de búsquedas	El sistema debe almacenar los datos generados por cada búsqueda realizada. Los datos que se deben almacenar son: fecha de realización de la búsqueda, nombre ingresado, username ingresado, ubicación ingresada, número de resultados, número de perfiles calificados como potencialmente violentos, número de perfiles calificados como posiblemente violentos, nombres	RN10,RN11

		de perfiles resultantes, username de perfiles resultantes y los enlaces de las fotos por perfil, que arrojaron positivo al análisis facial y/o análisis de arma corta.	
REQF7	Identificación y evaluación de múltiples rostros en publicaciones	El sistema debe ser capaz de identificar en una publicación los n rostros que se presenten, así como el análisis facial individual y sus resultados.	RN9

Tabla 4.2.1 Requerimientos Funcionales.

4.2.2 Requerimientos No Funcionales

Id	Nombre	Descripción	Origen
REQNF1	Detección de perfiles etiquetados en publicaciones con resultados positivos en los análisis facial y/o de arma corta	En algunas publicaciones se pueden encontrar otros username de perfiles que pueden estar involucrados en la foto que dio positivo a los análisis facial y/o de arma corta. El sistema podría guardar esos username para futuras búsquedas relacionadas.	Propuesto
REQNF2	Muestra de origen de publicación y antigüedad	Si las publicaciones analizadas contienen una fecha y ubicación obtenible, el sistema debe informar sobre la antigüedad y ubicación de la misma.	Definido
REQNF3	Análisis de texto en la publicaciones con resultados positivos a los análisis facial y/o de arma corta	El análisis del texto descriptivo que acompaña la imagen, ya sea hashtag o pie de imagen, debe poder analizarse y determinar con base en alguna métrica, si el texto es posiblemente violento.	Propuesto

Tabla 4.2.2 Requerimientos No funcionales

En la siguiente matriz se muestran la relación entre las reglas de negocio (primer columna) y los requerimientos funcionales del sistema (primera fila).

	REQF1	REQF2	REQF3	REQF4	REQF5	REQF6	REQF7
RN1	✓	✓					
RN2			✓				
RN3	✓						
RN4	✓						
RN5					✓		
RN6					✓		
RN7				✓	✓		
RN8			✓				
RN9							✓
RN10					✓	✓	
RN11			✓			✓	

Tabla 4.2.3 relación requerimientos, reglas de negocio

4.3 Análisis de Riesgos

En el análisis de riesgos consideramos los aspectos más influyentes que si llegan a ocurrir pueden detener parcial o completamente las funcionalidades del sistema. Los grados de impacto Medio y Bajo representan riesgos que tienen alternativas accesibles de implementación mientras que el grado de impacto Alto representa un riesgo que implicaría una reingeniería del sistema en ese módulo específico.

Id	Nombre	Descripción	Grado de Impacto
R1	Limitante de publicaciones obtenibles por perfil	La versión de prueba que se maneja en la API únicamente devuelve a lo máximo 20 publicaciones por perfil buscado. El sistema puede conseguir publicaciones en las que no haya coincidencias para calificar el perfil como posible perfil violento y por lo tanto descartarlo.	Medio
R2	Cantidad de perfiles devueltos por búsqueda mediante la API	Para hacer uso de la API se requiere poseer un perfil propio para realizar la búsqueda y este solo devuelve máximo 20 perfiles como resultado. El sistema se puede ver limitado en el análisis si dicho proceso solo toma en cuenta 20 perfiles para analizar.	Medio
R3	Detección de la API Instagram de exceso de consultas por cuenta	El uso de la API está limitado y condicionado a un determinado número de consultas. El	Alto

		sistema necesita distintas cuentas para obtener más publicaciones y así hacer una búsqueda más extensa. La API podría detectar el uso constante y cortar el servicio.	
R4	Consistencia en las publicaciones analizadas y privacidad de perfil	Los usuarios de la red social pueden modificar su privacidad y/o eliminar publicaciones que resultaron positivas a alguno de los análisis. Esto afecta al momento de realizar reportes o consultas a las publicaciones que en su momento se registraron con al \geq un grado de violencia.	Medio
R5	Resolución y filtros en la obtención de imágenes desde la API Instagram	La resolución y/o la presencia de filtros en las fotos de las publicaciones en los perfiles obtenidos en la búsqueda, pueden afectar al análisis de imagen al momento de determinar la presencia de arma corta así como la detección y análisis facial.	Bajo
R6	Conexión a los componentes de análisis y reconocimiento facial y de arma corta	Los componentes que están dedicados a la parte de análisis de fotos pueden perecer o perder la conexión con lo que	Alto

		impactaría de lleno en la función principal del sistema.	
--	--	--	--

Tabla 4.3 Análisis de Riesgos.

4.4 Definición de Actores

Los usuarios finales que se pretenden para el sistema son personas dedicadas a monitorear redes sociales con la finalidad de prevenir delitos y peligros que se cometan o anuncien a través de estas. En la Ciudad de México se contempla como posibles usuarios a un grupo pequeño y específico de la Policía de Ciberdelincuencia Preventiva.

Para el análisis de casos de uso definimos nuestro actor “Usuario General” como un usuario con las características antes mencionadas.

4.5 Casos de Uso

Dentro de los casos de uso la acción “Realizar Búsqueda” se entiende como el proceso de ingresar los datos básicos de búsqueda de perfil de Instagram como: nombre, username, y ubicación y con base en ellos mostrar las cuentas de Instagram coincidentes. También dentro de esta acción se desempeña el reconocimiento y análisis facial, así como la detección de arma corta.

Identificador	CU1
Nombre	Realizar Búsqueda
Actores	Usuario General
Propósito	Obtener datos con la API de Instagram con base en los parámetros de búsqueda ingresados. Posteriormente analizar esos datos y emitir la evaluación de violencia de los perfiles resultantes.
Entradas	Datos de búsqueda: <ul style="list-style-type: none"> ● Nombre ● username de Instagram ● Ubicación
Salidas	Con base en los resultados de búsqueda: <ul style="list-style-type: none"> ● Listado con las cuentas de instagram y datos de cada una de ellas que el motor detectó. También se mostrará la evaluación de violencia de perfil a la que el motor llegó. ● Mensaje especificando que el motor no encontró coincidencia alguna
Precondiciones	Ingreso obligatorio de los campos Nombre y/o username y/o ubicación.

Tabla 4.5.1 Caso de uso Realizar Búsqueda.

Identificador	CU2
Nombre	Consultar Búsquedas Previas
Actores	Usuario General
Propósito	Consultar las búsquedas previas registradas en el sistema para referencia o generación de reportes
Entradas	Datos de búsqueda de registro: <ul style="list-style-type: none"> • Fecha • Nombre buscado • username de Instagram buscado • Ubicación
Salidas	Con base en los resultados de búsqueda en la base de datos: <ul style="list-style-type: none"> • Listado con los registros de búsqueda existentes que empataron con los parámetros de búsqueda. • Mensaje especificando que no se encontró registro previo en el sistema.
Precondiciones	Ninguna

Tabla 4.5.2 Caso de uso Consultar Búsqueda Previa.

Identificador	CU3
Nombre	Generar Reporte
Actores	Usuario General
Propósito	Realizar un reporte con detalles de la búsqueda realizada o realizar reporte con detalles de una búsqueda previa registrada en el sistema.
Entradas	Datos de búsqueda de registro: <ul style="list-style-type: none"> • Fecha • Nombre buscado • Nombre de usuario Instagram • Ubicación
Salidas	Con base en la búsqueda de registros previos: <ul style="list-style-type: none"> • Listado con los registros de búsqueda existentes • Mensaje especificando que no se encontró registro previo en el sistema • Reporte generado Después de haber realizada la búsqueda: <ul style="list-style-type: none"> • Reporte generado
Precondiciones	Registro existente de búsqueda en el sistema

Tabla 4.5.3 Caso de uso Generar Reporte.

4.5.1 Diagrama de Casos de Uso

El siguiente diagrama modela la interacción del Usuario General con los 3 casos de uso del sistema.

Para el prototipo del sistema se consideraron 3 escenarios básicos donde se verían reflejadas las principales funcionalidades.

Realizar Búsqueda: Comprende la acción de búsqueda en Instagram como se menciona antes en el la tabla de casos de uso Tabla 4.5.1.

Consultar Búsquedas Previas: Este caso de uso comprende las consultas de búsquedas que están registradas en el sistema y está denotado con una flecha de tipo “include” hacia Realizar Búsqueda ya que es necesario haber realizado al menos una búsqueda con el sistema para desplegar la información de esa búsqueda. El comportamiento se describe en la Tabla 4.5.2.

Generar Reporte: En este caso de uso se despliega el reporte generado a partir de los resultados de búsqueda o los resultados de varias búsquedas. La acción tiene flechas de “Extend” provenientes de Realizar Búsqueda y Consultar Búsquedas ya que ambas acciones dentro de su ejecución pueden llamar a Generar Reporte.

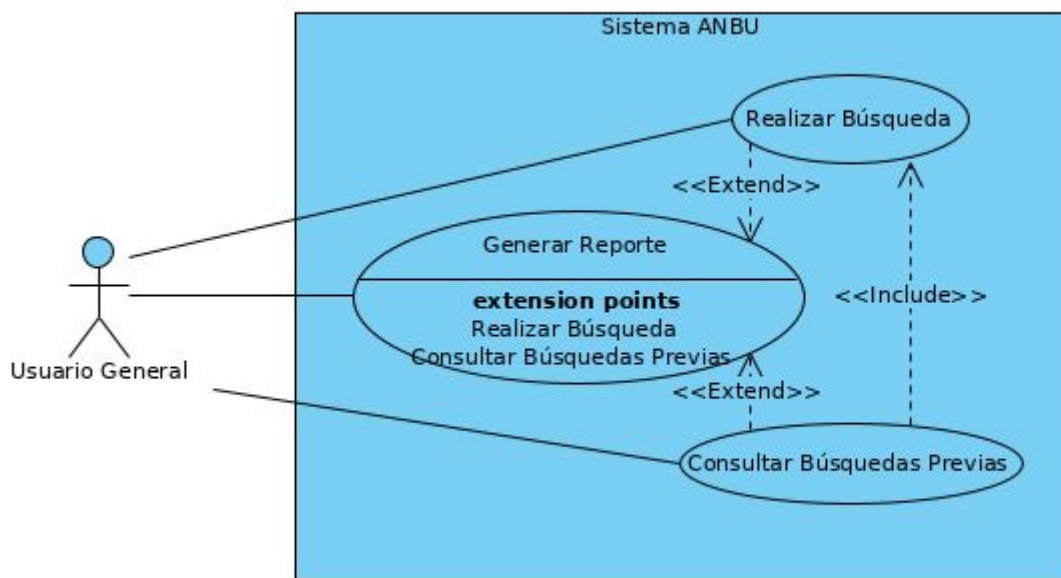


Figura 4.5.1 Diagrama Caso de uso, realizado con Visual Paradigm Enterprise.

4.6 Modelado de la Base de Datos

El modelado de la base de datos se realizó con base en las reglas del negocio y requerimientos que se definen en los puntos anteriores de Reglas del Negocio y Requerimientos del Sistema.

4.6.1 Diagrama Entidad Relación

En este diagrama se muestra la relación que tienen las entidades y este diagrama se obtuvo siguiendo la siguiente lógica de negocio:

De una búsqueda realizada con el sistema, pueden o no resultar perfiles coincidentes. Un perfil puede tener ninguna o muchas publicaciones de las cuales cada una de ellas se analizarán con el módulo detector de rostro y el módulo detector de arma corta, de estos 2 detectores se pasa a la sección de análisis donde se determina los valores del análisis facial, y la determinación de la presencia de arma corta tipo escuadra.

Para generar un reporte se requiere consultar una o muchas búsquedas previas con base en una fecha de registro en el sistema.

Este diagrama se puede apreciar mejor en la sección de anexos; Anexo 3.

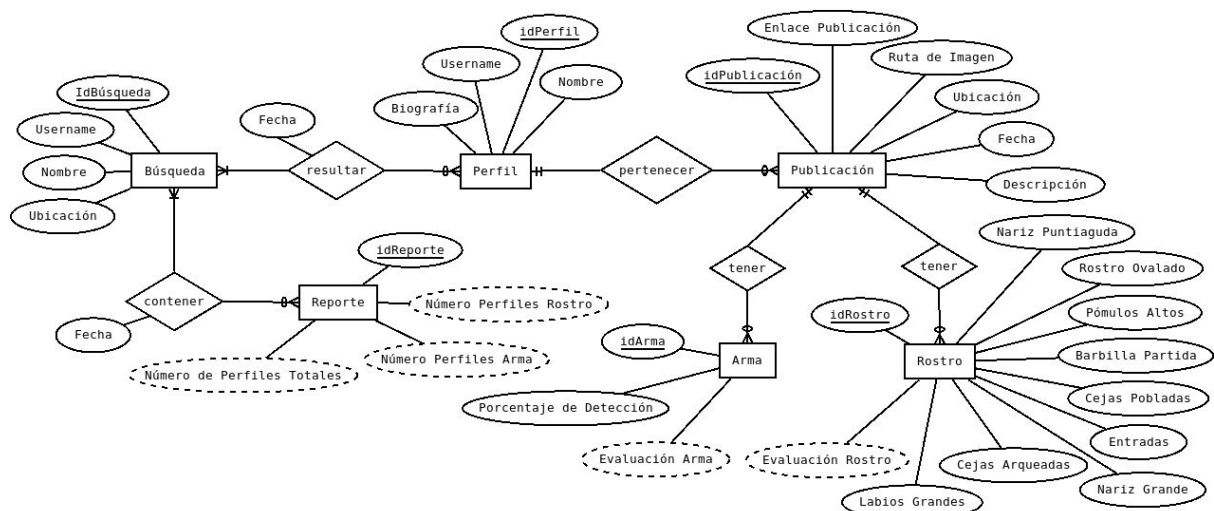


Figura 4.6.1 Diagrama Entidad Relación

4.6.3 Diccionario de Datos

El diccionario de datos especifica las relaciones con una breve descripción de su propósito de almacenamiento así como sus atributos con sus respectivos tipos de datos y reglas o constraint.

Relación: Búsqueda		
Descripción: Almacena los datos ingresados para realizar una búsqueda, así como la fecha en la que se realizó dicha búsqueda.		
Atributo	Tipo de Dato	Constraint
idBúsqueda	INT	PK
username_buscado	Varchar(30)	-
nombre_buscado	Varchar(30)	-
ubicacion	Varchar(100)	-
fecha	DATE	-

Tabla 4.6.1 Diccionario de Datos Búsqueda.

Relación: Perfil		
Descripción: Dentro de este relación se almacenan los datos referentes al perfil de Instagram.		
Atributo	Tipo de Dato	Constraint
idPerfil	INT	PK
username	Varchar(30)	-
nombre	Varchar(30)	-
biografia	Varchar(150)	-
idBúsqueda	INT	FK

Tabla 4.6.2 Diccionario de Datos Perfil.

Relación: Publicacion		
Descripción: Este relación almacena los datos de la publicación que se analizó tanto para rostro como para arma corta.		
Atributo	Tipo de Dato	Constraint
idPublicacion	INT	PK
idPerfil	INT	FK
ubicacion	Varchar(100)	-
fecha	DATE	-
enlace	Varchar(200)	-
ruta_imagen	Varchar(100)	-
descripcion	Varchar(500)	-
val_rostro	INT	-
val_arma	INT	-

Tabla 4.6.3 Diccionario de Datos Publicación.

Relación: Reporte		
Descripción: Esta relación almacena los datos referentes a los reportes generados.		
Atributo	Tipo de Dato	Constraint
idReporte	INT	PK
numPerfiles	INT	-
numPerfilesArma	INT	-
numPerfilesRostro	INT	-
fecha	DATE	-

Tabla 4.6.4 Diccionario de Datos Reporte.

Relación: reporte_busqueda		
Descripción: Esta relación almacena las ocurrencias de las búsquedas en los reportes y la fecha en la que se generó ese reporte. Los reportes informan de una o muchas búsquedas.		
Atributo	Tipo de Dato	Constraint
idBusqueda	INT	PK,FK
idReporte	INT	PK,FK
fecha	DATE	-

Tabla 4.6.5 Diccionario de Datos reporte_busqueda.

Relación: busqueda_perfil		
Descripción: Esta relación almacenará las ocurrencias de perfiles por cada búsqueda generada y también la fecha en que se realizó dicha búsqueda.		
Atributo	Tipo de Dato	Constraint
idBusqueda	INT	PK,FK
idPerfil	INT	PK,FK
fecha	DATE	-

Tabla 4.6.6 Diccionario de Datos busqueda_perfil

Relación: Arma		
Descripción: Esta relación almacenará el porcentaje de detección de arma corta		
Atributo	Tipo de Dato	Constraint
idArma	INT	PK
porcentaje	INT	-
evaluacion_arma	INT	-
idPublicacion	INT	FK

Tabla 4.6.7 Diccionario de Datos Arma

Relación: Rostro		
Descripción: Esta relación almacenará las características resultantes del análisis facial de cada rostro ocurrente en una publicación, así como su evaluación del sistema.		
Atributo	Tipo de Dato	Constraint
idRostro	INT	PK
idPublicacion	INT	FK
rostro_oval	INT	-
entradas	INT	-
cejas_pobladas	INT	-
cejas_arco	INT	-
pomulos	INT	-
nariz_grande	INT	-
nariz_puntiaguda	INT	-
labios_grandes	INT	-
barbilla_partida	INT	-
evaluacion_rostro	INT	-

Tabla 4.6.8 Diccionario de Datos Rostro

Capítulo 5. Diseño de Software

5.1 Arquitectura del Sistema

En el siguiente diagrama se muestra de forma general la interacción entre los principales módulos del sistema así como los datos de entrada y los datos de salida que generan.

Este diagrama se puede apreciar mejor en la sección de anexos, Anexo 3.

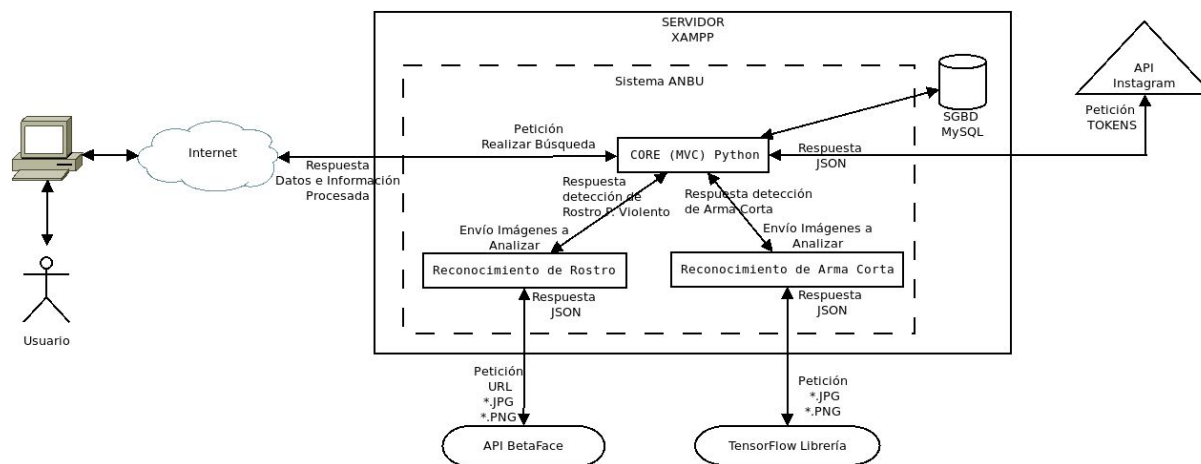


Figura 5.1 Arquitectura del Sistema.

En la tabla siguiente se detallan las funciones de cada componente y su flujo dentro del sistema para el caso básico de realizar búsqueda:

Componente	Descripción General	Componentes Ligados
Core (MVC) Python	Componente central encargado de la gestión del sistema. Recibe y responde las peticiones del usuario. Envía las imágenes a los módulos de reconocimiento de rostro y arma corta. Envía las solicitudes a la API de Instagram y realiza acciones sobre la base de datos.	SGBD MySQL, API Instagram, Reconocimiento de Rostro y Reconocimiento de Arma Corta
Sistema Gestor de Base de Datos MySQL	Componente que se encarga de la gestión de los datos.	Core (MVC) Python
Reconocimiento de Rostro	Se encarga de recibir las imágenes a reconocer y posteriormente mandarlas a	Core (MVC) Python y Betaface API

	la API Betaface. Con base en los resultados que le regresa la API, éste módulo determina si la imagen enviada contiene dentro de sí un rostro y si este presenta características violentas. Esa información la retorna al Core(MVC)	
Reconocimiento de Arma Corta	Se encarga de recibir las imágenes enviadas por el Core para ser analizarlas por medio de la librería TensorFlow. Con base en los resultados que le regresa la Librería, éste módulo determina si la imagen enviada contiene dentro de sí un arma corta tipo escuadra. Esa información la retorna al Core(MVC) para que sea almacenada en la base de datos.	Core (MVC) y Librería TensorFlow
API Instagram	Componente externo el cual recibe tokens generados para realizar la consulta de información de la red social y retorna los datos en formato JSON para posteriormente ser procesados por el Core (MVC)	Core (MVC)
API Betaface	Componente externo que realiza el reconocimiento de rostros. Realiza un análisis de la imagen dada y entrega datos sobre las facciones del rostro. Estos datos se regresan en formato JSON	Reconocimiento de Rostro
Librería TensorFlow	Componente externo que realiza el reconocimiento de arma corta tipo escuadra. Recibe la imagen a analizar	Reconocimiento de Arma Corta

	y determina si existe un porcentaje de coincidencia con que exista un arma en esa imagen. El porcentaje de que se haya encontrado un arma de ese tipo, se retorna en formato JSON.	
--	--	--

Tabla 5.1 Componentes de la Arquitectura.

5.2 Diagrama de Procesos

En el siguiente diagrama se modelan los procesos generales del sistema así como las rutas de decisión o secuencias que pueden seguir dentro del mismo.

Este diagrama se puede apreciar mejor en la sección de anexos, Anexo 3.

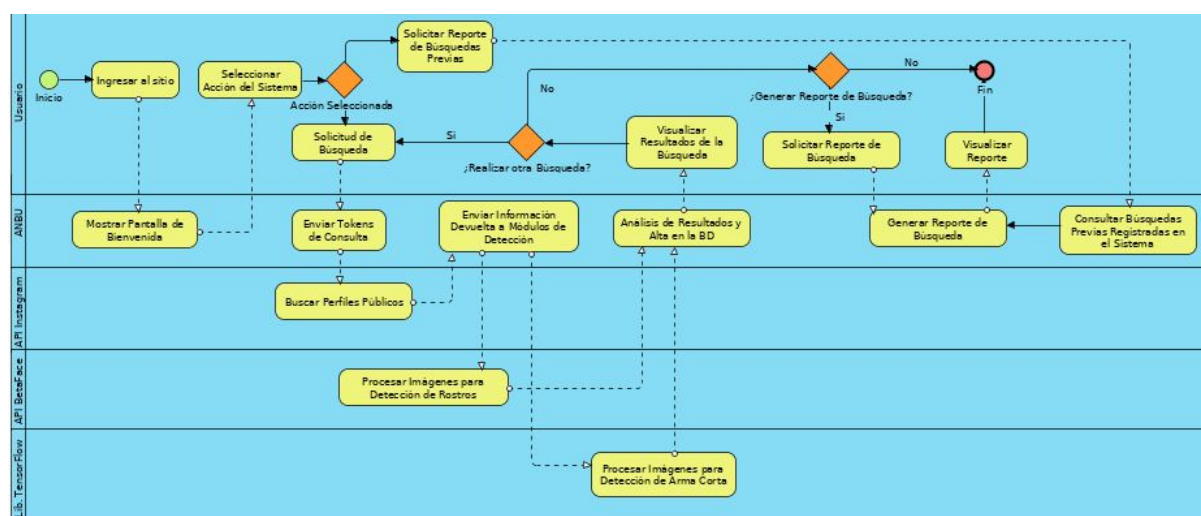


Figura 5.2 Diagrama de Procesos, realizado con Visual Paradigm Enterprise.

5.3 Diagramas de Secuencia

Diagrama de Secuencia para el Caso de Uso 1

El usuario envía los datos de búsqueda, los cuales sirven como parámetros para generar los tokens “llaves” hacia la API de Instagram, recibiendo la petición de tokens la API devuelve los datos con JSON, una vez que se reciben los datos, estos se enviarán a los módulos de Betaface y TensorFlow, respectivamente cada módulo regresara los JSON resultantes al servidor y este los almacenará en la Base de Datos, de la cual posteriormente se podrá obtener diversas consultas.

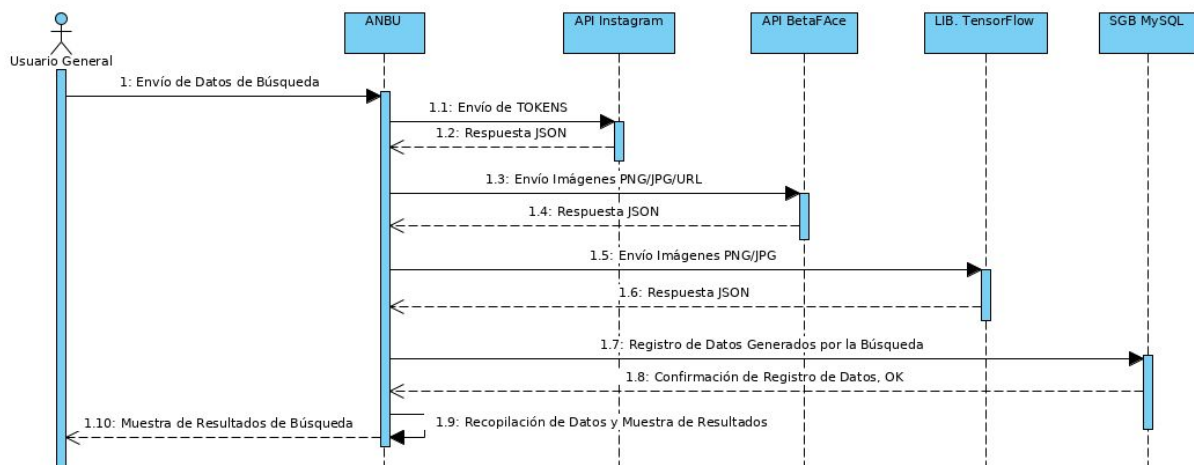


Figura 5.3.1 Diagrama de secuencia para el Caso de Uso 1, realizado con Visual Paradigm Enterprise.

Diagrama de Secuencia para el Caso de Uso 2

El Usuario podrá consultar búsquedas previas a través del servidor, esté a su vez realizará las peticiones a la Base de Datos la cual regresará las consultas solicitadas para poder mostrarlas al usuario.

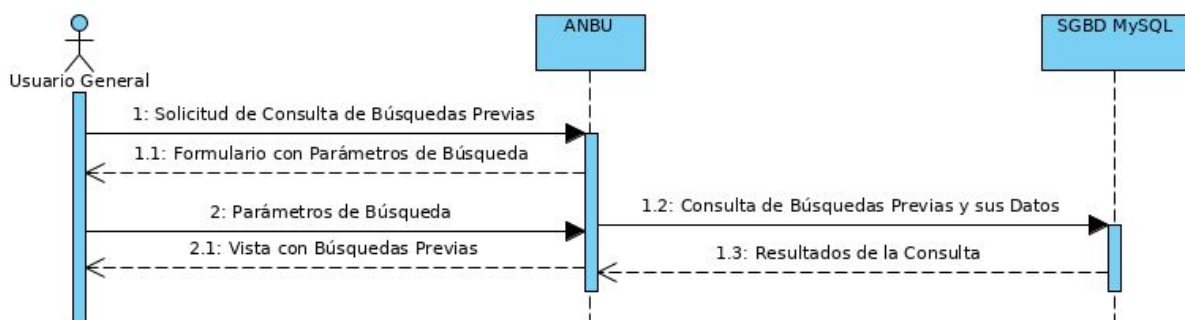


Figura 5.3.2 Diagrama de secuencia para el Caso de Uso 2, realizado con Visual Paradigm Enterprise.

Diagrama de Secuencia para el Caso de Uso 3

El usuario realiza una solicitud para poder generar el reporte, esta solicitud es mandada al servidor el cual solicita los datos necesarios a la Base de Datos, cuando se devuelven los datos solicitados se genera el reporte y posteriormente se entrega una vista al usuario.

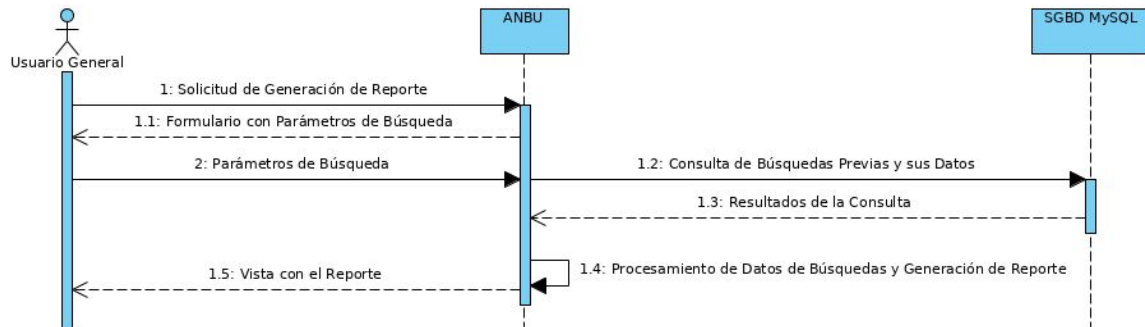


Figura 5.3.3 Diagrama de secuencia para el Caso de Uso 3, realizado con Visual Paradigm Enterprise.

5.4 Vistas del Sistema

Las vistas del sistema en su etapa final se proponen como se muestran en la imágenes siguientes. Éstas no representan las vistas definitivas por lo que pueden ser modificadas para adaptarse mejor a las funcionalidades del sistema.

Vista Pantalla de Inicio: Es la primer pantalla que se mostrará al usuario. Tiene las opciones de realizar búsqueda y consultar búsqueda.

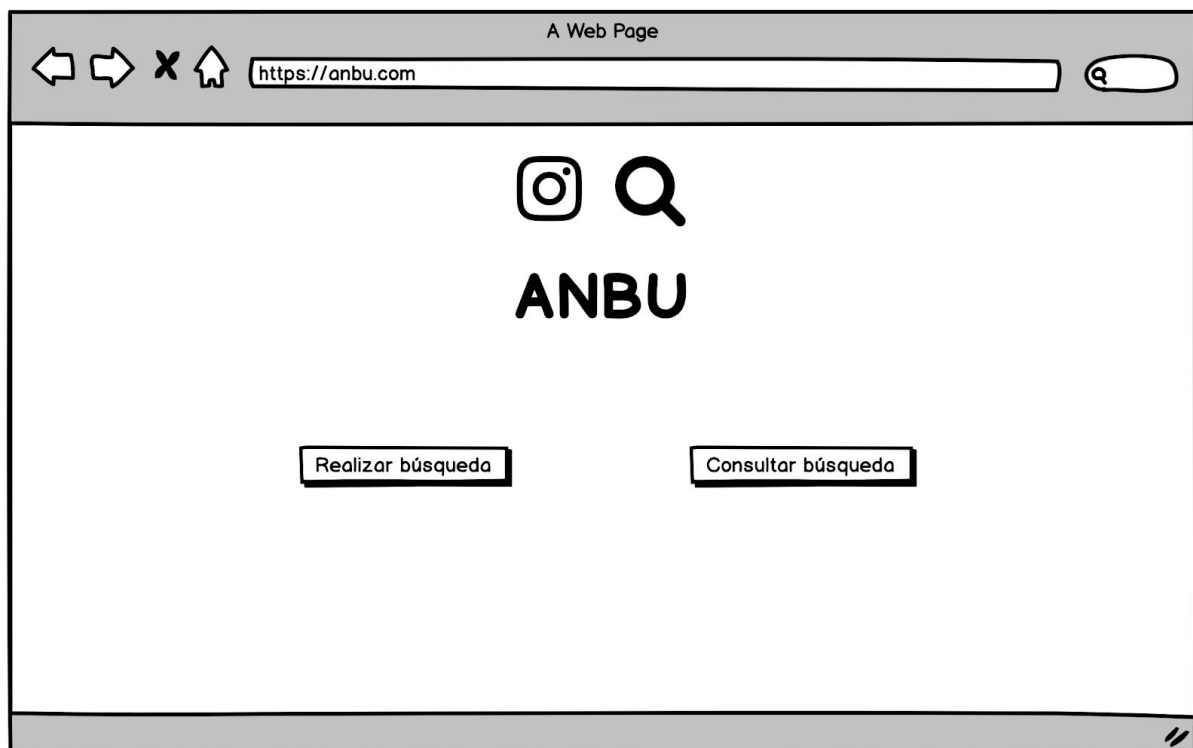
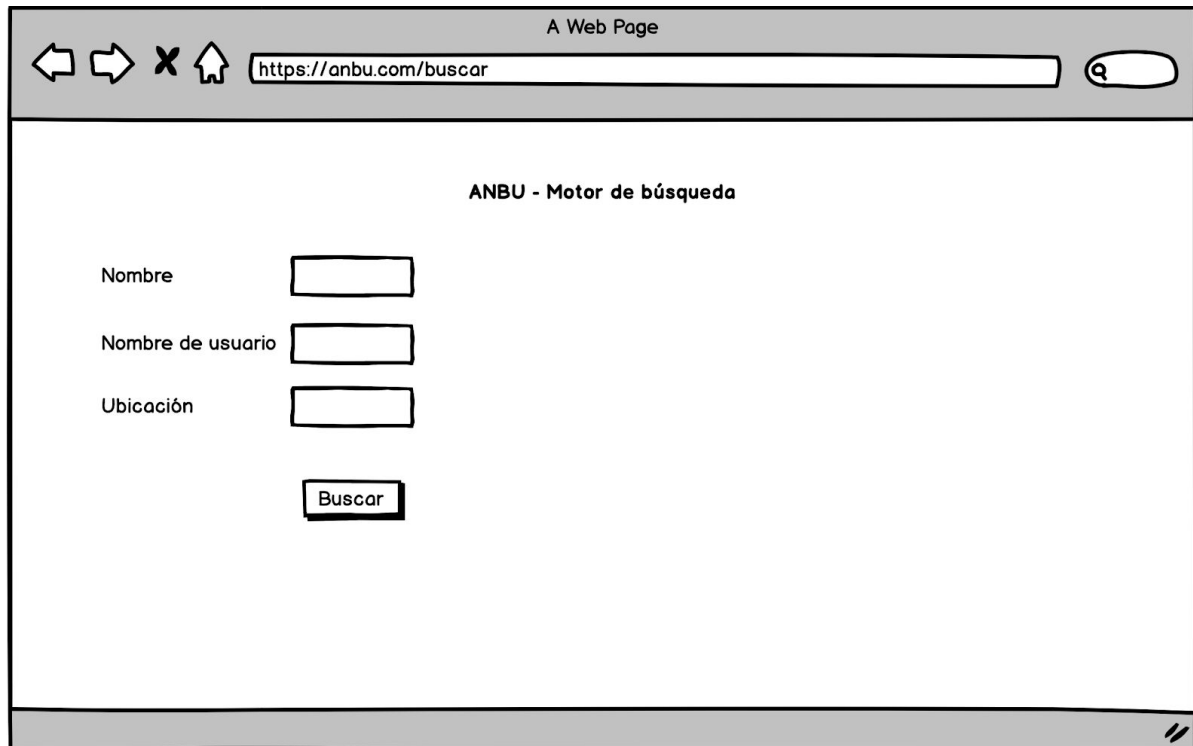


Figura 5.4.1 Vista de la pantalla de inicio.

Vista Realizar búsqueda: En esta vista se puede observar los campos que se ingresan para acotar la búsqueda: Nombre, Nombre de usuario y Ubicación. También se observa el botón Buscar el cual enviará la solicitud de búsqueda al sistema.



The image shows a web browser window titled "A Web Page". The address bar contains the URL "https://anbu.com/buscar". The main content area displays the title "ANBU - Motor de búsqueda". Below the title, there are three input fields labeled "Nombre", "Nombre de usuario", and "Ubicación". Below these fields is a button labeled "Buscar".

Nombre	<input type="text"/>
Nombre de usuario	<input type="text"/>
Ubicación	<input type="text"/>
	<input type="button" value="Buscar"/>

Figura 5.4.2 Vista de búsqueda.

Vista Muestra de Resultados: En esta vista se puede observar una tabla que contiene los resultados de la búsqueda. Dentro de esta tabla se muestran los datos de los perfiles resultantes: username, nombre, URL de perfil y ubicación.

La segunda tabla muestra los resultados generales de la búsqueda en el contexto de detección y análisis de arma y rostro. Se muestran: URL de publicación, no de rostros detectados, si se detectó algún arma tipo escuadra y el diagnóstico de perfil según el sistema.

ANBU - Resultado de la búsqueda

Búsqueda no. 1

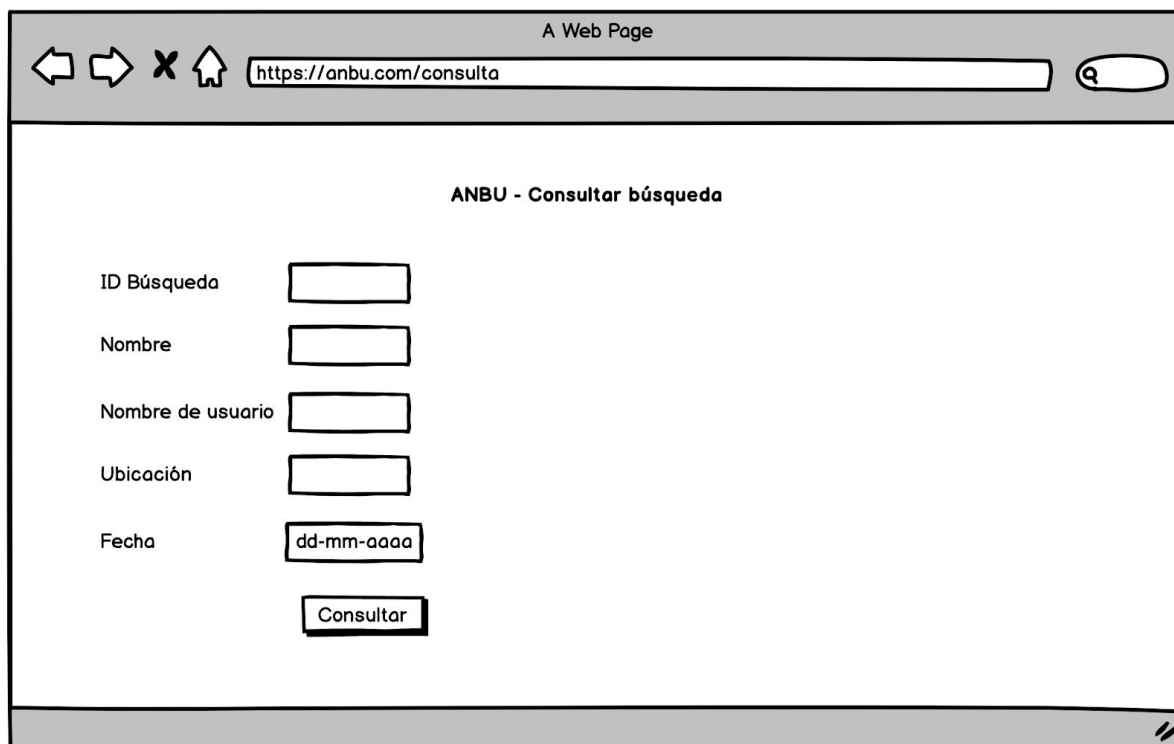
@username	Nombre	URL del perfil	Ubicación
@juanlopez	Juan López	www.instagram.com/juanlopez	Ciudad de México
@juanlopez22	Juan López	www.instagram.com/juanlopez22	Ciudad de México
@lopezjuan764	Juan López	www.instagram.com/lopezjuan764	Ciudad de México

URL publicación	No. de rostros	Arma detectada	Rostro agresivo detectado	Diagnóstico de perfil
www.instagram.com/juanlopez22/dlkms2	2	Si	Si	Posible violento
www.instagram.com/juanlopez22/cslknoiw	1	Si	No	Potencial violento
www.instagram.com/juanlopez/hdthrt5	2	No	No	Posible no violento
www.instagram.com/lopezjuan764/lej3	1	No	Si	Potencial violento

[Generar reporte](#)

Figura 5.4.3 Vista de muestra de resultados.

Vista Consultar búsqueda: Es la segunda opción de la pantalla de inicio (Figura 5.4.1). En ella se muestran los parámetros de consulta pertenecientes a las búsquedas previas. Estos son: identificador, nombre buscado, nombre de usuario buscado, ubicación ingresada y fecha en que se realizó la búsqueda.



The image shows a web browser window titled 'A Web Page' with the address bar displaying 'https://anbu.com/consulta'. The main content area is titled 'ANBU - Consultar búsqueda' and contains a form with the following fields and a button:

Field Label	Field Type / Value
ID Búsqueda	<input type="text"/>
Nombre	<input type="text"/>
Nombre de usuario	<input type="text"/>
Ubicación	<input type="text"/>
Fecha	<input type="text" value="dd-mm-aaaa"/>
<input type="button" value="Consultar"/>	

Figura 5.4.4 Vista de consulta de búsqueda.

Vista del resultado de consulta: Se despliega en forma de tablas el resultado de la consulta de búsqueda previa.

ANBU - Resultado de consulta

Búsqueda no. 1

@username	Nombre	URL del perfil	Ubicación
@juanlopez	Juan López	www.instagram.com/juanlopez	Ciudad de México
@juanlopez22	Juan López	www.instagram.com/juanlopez22	Ciudad de México
@lopezjuan764	Juan López	www.instagram.com/lopezjuan764	Ciudad de México

URL publicación	No. de rostros	Arma detectada	Rostro agresivo detectado	Diagnóstico de perfil
www.instagram.com/juanlopez22/dlkms2	2	Si	Si	Posible violento
www.instagram.com/juanlopez22/cslknoiw	1	Si	No	Potencial violento
www.instagram.com/juanlopez/hdthrt5	2	No	No	Posible no violento
www.instagram.com/lopezjuan764/lej13	1	No	Si	Potencial violento

[Generar reporte](#)

Figura 5.4.5 Vista del resultado de consulta de búsqueda.

Vista del reporte generado: Las siguientes 3 figuras, se genera a partir de seleccionar la opción “Generar Reporte” que se muestran en los botones de las vistas previas: Figura 5.4.3 y Figura 5.4.5. Se muestra los datos del reporte generado: Id de búsqueda, fecha de realización, nombre ingresado, ubicación ingresada, username ingresado; así como el despliegue de cada perfil resultante de la búsqueda y sus publicaciones con detección de arma y/o donde se detectó un posible rostro violento.

ANBU - Reporte de búsqueda

Búsqueda No. Fecha de búsqueda

Parámetros de búsqueda:

Nombre Ubicación @username

Numero de perfiles	Numero de publicaciones	Numero de rostros agresivos	Numero de armas
3	4	2	2

En esta búsqueda se encontraron 2 armas de fuego calibre corto y 2 rostros agresivos en un total de 4 publicaciones en 3 perfiles con los parámetros antes señalados.

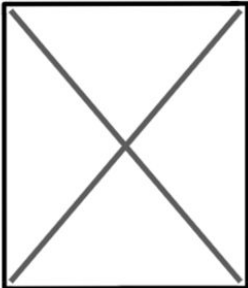
Perfil no. 1

Nombre

Nombre de usuario

Biografía

Publicación



Ubicación

Fecha

Enlace

PIe de imagen

No. de armas

No. de rostros

Resultado

1/3

Perfil no. 2

Nombre

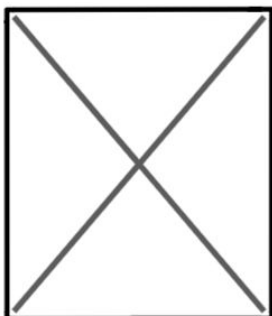
Juan López

Nombre de usuario

@juanlopez22

Biografía

Cuidado todos

Publicación

Ubicación

Ciudad de México

Fecha

31--10--2019

Enlace

www.instagram.com/juanlopez22/dlkms2

Pie de imagen

Miren mis armas

No. de armas

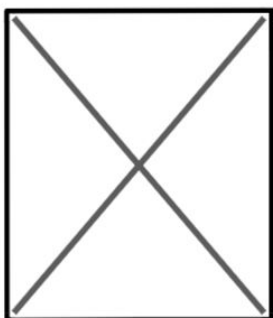
1

No. de rostros

1

Resultado

Posible violento

Publicación

Ubicación

Ciudad de México

Fecha

31--10--2019

Enlace

www.instagram.com/juanlopez22/cslknoiw

Pie de imagen

Cuidado

No. de armas

1

No. de rostros

0

Resultado

Potencial no violento

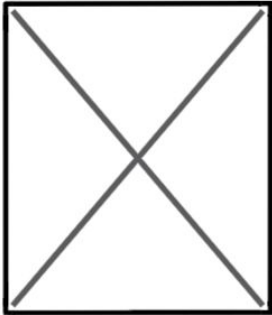
Perfil no. 3

Nombre

Nombre de usuario

Biografía

Publicación



Ubicación

Fecha

Enlace

Pie de imagen

No. de armas

No. de rostros

Resultado

3/3

Figura 5.4.6 Vista de reporte generado.

Capítulo 6. Trabajo a Futuro

6.1 Conclusiones de este Documento

Durante la investigación de métodos, herramientas, algoritmos, entre otras cosas que implica el desarrollo e implementación de este prototipo; descubrimos que existen gran cantidad de algoritmos dedicados al reconocimiento de rostros y análisis facial. Sin embargo, no existen estándares o características generales que al realizar el análisis facial, se determine si una persona realmente es violenta. Debido a esto, se contempló a la Morfopsicología como posible comparativa y terminamos por desechar la idea al realizar que se considera como una pseudociencia al no tener bases científicas[25]. Para resolver ese problema optamos por desarrollar nuestra propia métrica al analizar y obtener parámetros faciales promedio de un conjunto de delincuentes detenidos en la Ciudad de México y Estado de México por cargos de secuestro, asesinato y asalto[17].

Resultado del análisis de determinar si una persona es o no posiblemente violenta en Instagram, observamos que dentro de esta red hay más información que también podría ser considerada para el análisis; como los pies de publicación, etiquetas de otros perfiles y hashtags. Esta información tal vez podría considerarse en un trabajo a futuro para ofrecer un análisis más profundo.

6.2 Trabajo a Futuro

Para Trabajo Terminal 2, implementaremos el sistema base y haremos conexión con los módulos de detección facial y de rostro para realizar el análisis que terminará en un reporte que intente ayudar a los que consideramos como usuarios potenciales o las organizaciones dedicadas a prevenir delitos en redes sociales de nuestro país.

Capítulo 7. Anexos

Anexo 1

Análisis facial

En este anexo se presentan las características faciales que estudia la imaginología como son las medidas del rostro, las cejas, los ojos, boca, y otros aspectos del rostro.

La cara en el plano Mediosagital

Aunque no existe un plano perfecto de simetría facial en la mayoría de las personas, el plano mediosagital se divide en cinco partes iguales, cada fracción equivale a la amplitud de un ojo esto se muestra en la figura 7.1.1



Figura 7.1.1 La cara en el plano Mediosagital. [11]

Altura Facial

Está conformada en tres secciones las cuales se muestran en la figura 7.1.2

- Sección 1: conformada por el Trichion (Tr) a la Glabella (G).
- Sección 2: conformada desde la Glabella (G) hasta el punto Subnasal (Sn).
- Sección 3: conformada desde el punto Subnasal (Sn) hasta el Mentón.

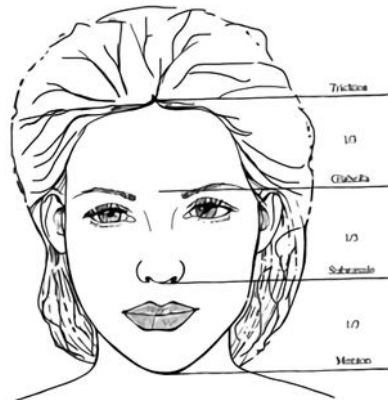


Figura 7.1.2 Altura Facial. [11]

La Frente

Corresponde a la primera sección de la altura facial, es decir de las cejas a la línea de implantación del cabello.

Las Cejas

Arco curvilíneo cubierto por vello sobre el borde de los ojos, en las mujeres se encuentra por encima del borde Supraorbitario, en el hombre descansa sobre el mismo, como podemos ver en la figura 7.1.3

.

Los Ojos

Cada ojo conforma una quinta parte de la anchura de la cara, por lo que la distancia entre ellos es igual a su anchura, si esta distancia fuera mayor se le denomina telecanto. La forma del ojo se ilustra en la figura 7.1.3 El párpado superior cubre de 7 a 15 mm de la línea de las pestañas.

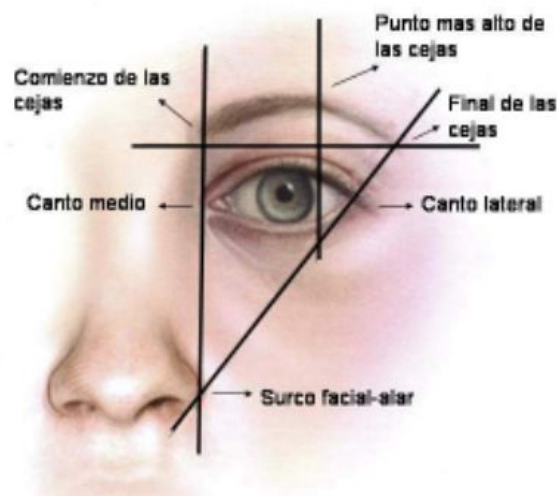


Figura 7.1.3 Detalles Ojo y Ceja [11].

La Nariz

Unidad estética facial dividida en subunidades.

- Dorso nasal.
- Paredes laterales.
- Alas.
- Punta nasal.
- Triángulos blandos.
- Columela.

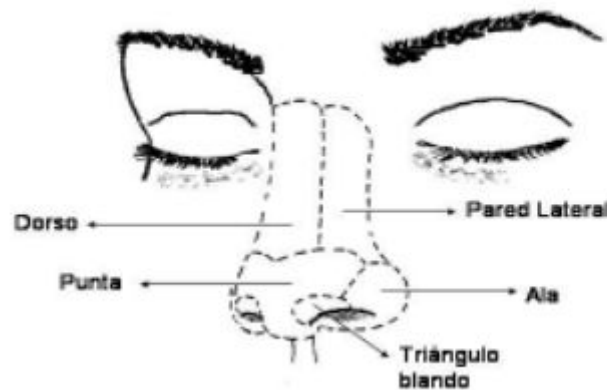


Figura 7.1.4: Subunidades de la nariz. [11]

Relación Nasofacial.

La Relación Nasofacial está constituida por 4 ángulos.

- Ángulo Nasofrontal: Conformado por la parte de la nariz a la frente, formada por una línea tangente de Nasion al Dorso Nasal, el ángulo formado es de 115° a 130° .



Figura 7.1.4.1: Ángulo Nasofrontal.[11]

- **Ángulo Nasolabial:** Parte de la Columela hasta el labio superior. el ángulo formado en el caso de las mujeres es de 95° a 100° en, caso de los hombres de 90° a 95° .

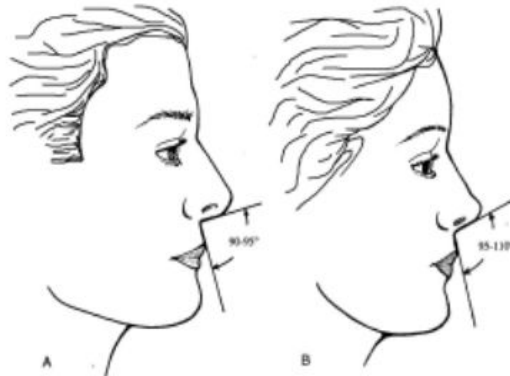


Figura 7.1.4.2 Ángulo Nasolabial. [11]

- **Ángulo Nasofacial:** Parte del Plano Facial(formado por una línea entre la Glabella con el Pogonion) con una línea tangente al dorso nasal, el ángulo nasofacial tiene una norma de 30° a 40° .



Figura 7.1.4.3 Ángulo Nasofacial. [11]

- **Ángulo Nasomental:** Es la línea tangente desde el Nasion a la Punta Nasal con la intersección de la línea desde la punta al Pogonion, el ángulo va entre 120° a 132° y las zonas importantes son la nariz y el mentón.

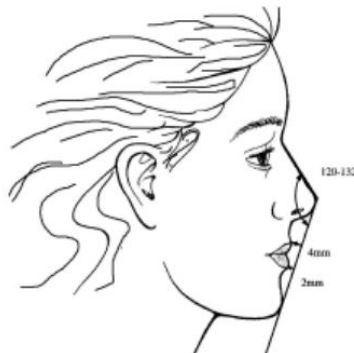


Figura 7.1.4.4 Ángulo Nasomental. [11]

Formas de la nariz

Aunque hay una gran variedad de formas de la nariz destacan principalmente tres tipos, su longitud es aproximada a el ancho de un ojo es decir una quinta parte de la cara.

- A. Tipo Leptorrinos (nariz caucásica).
- B. Tipo Mesorrinos (nariz amarilla o mestiza).
- C. Tipo Platirrinos (nariz negroide).

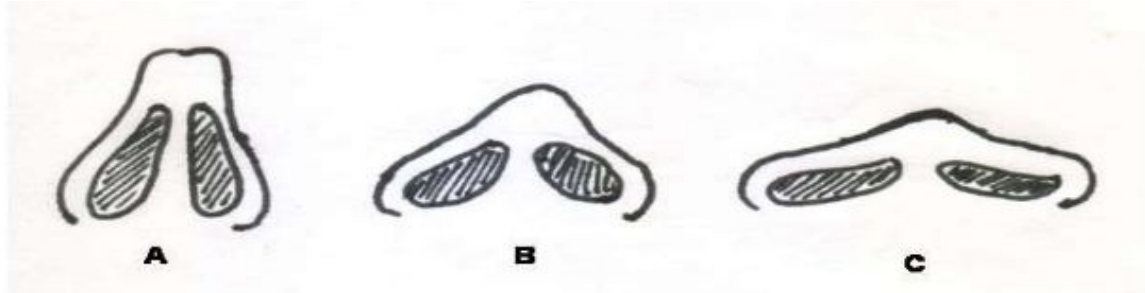


Figura 7.1.5 Formas de la nariz. [11]

Los Labios

Cubren el tercio inferior de la cara.

- Labio superior se mide desde el Punto Subnasal (Sn), hasta el punto más superior del borde libre de los mismos.
- Labio inferior comprende desde el borde inferior, hasta el Mentón.

Posición y forma

- Se traza una línea desde el Punto Subnasal (Sn) y el Pogonion (Pg), la posición del labio debe de estar detrás de la línea anterior y el Surco Mentolabial (Si).
- Se utiliza el ángulo Nasomental donde el labio superior cae detrás de la línea a 4 mm y el labio inferior cae detrás de la línea 2 mm.

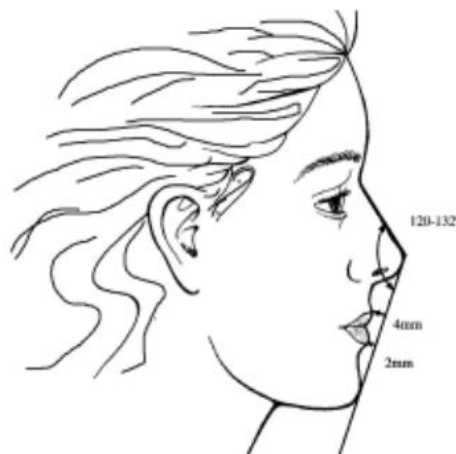


Figura 7.1.6 Posición de los labios. [11]

La Barbilla

Su posición ideal va a través de una línea que parte desde el nasion que va perpendicularmente al plano horizontal de Frankfort.



Figura 7.1.7 Posición de la barbilla. [11]

La Oreja

El eje largo de la oreja está aproximadamente a una distancia paralela al eje del dorso nasal ver figura 7.1.8

El borde superior del pabellón auricular está a nivel de las cejas y el borde inferior a nivel del al nasal.

La anchura es aproximadamente el 55% de su longitud, desde su borde helicoidal a la piel mastoidea es 15 a 25 mm y el ángulo de protrusión promedio es de 21° a 25° .



Figura 7.1.8 Posición de las orejas. [11]

El cuello

El ángulo mentocervical se halla trazando una línea perpendicular al plano horizontal de Frankfort desde la Glabella (G) al Pogonion (Pg) y esta se va a interceptar con una línea tangencial del Mentón al punto cervical (C), el rango de este ángulo va entre 80° y 95° .

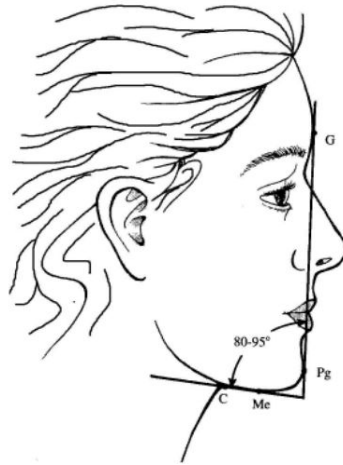


Figura 7.1.9 Posición del cuello. [11]

Anexo 2

En este anexo se muestra un catálogo de imágenes obtenidas de la Fiscalía General del Estado de México, el catálogo consta de aproximadamente 70 imágenes. Las imágenes a continuación mostradas fueron utilizadas para poder obtener las características principales de un rostro violento, mediante la herramienta Betaface. Los detalles de los resultados obtenidos se muestran el Capítulo 3 sección 3.2

Imágenes de prueba para Betaface



Figura 7.2.1 prueba 1 Betaface [17]

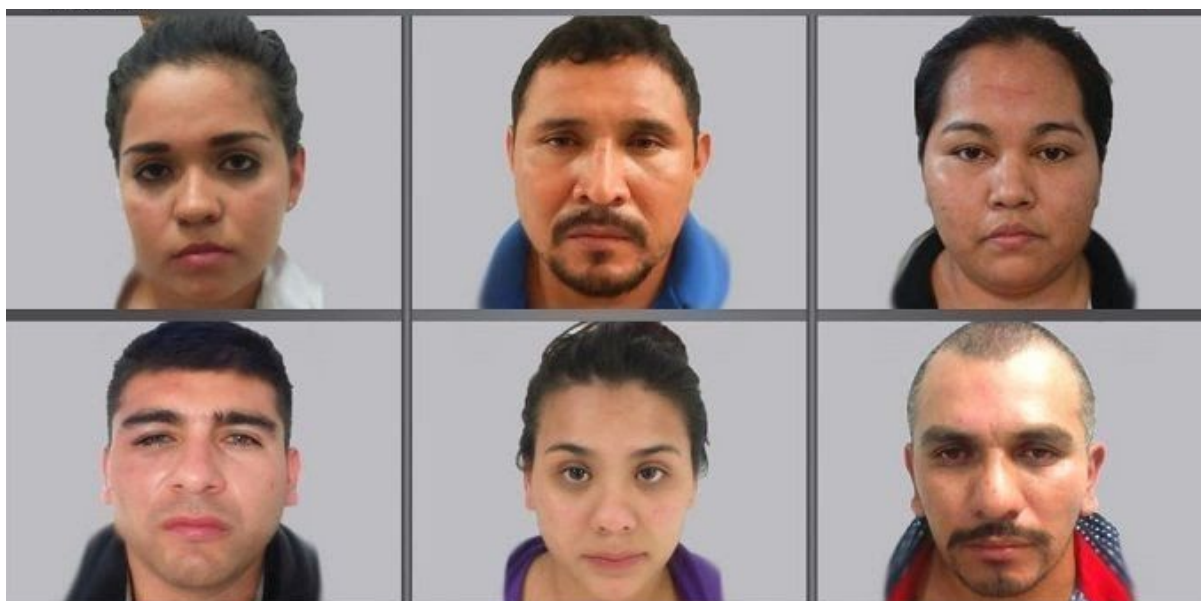


Figura 7.2.2 prueba 2 Betaface [17]



Figura 7.2.3 prueba 3 Betaface [17]



Figura 7.2.4 prueba 4 Betaface [17]



Figura 7.2.5 prueba 5 Betaface [17]



Figura 7.2.6 prueba 6 Betaface [17]



Figura 7.2.7 prueba 7 Betaface [17]



Figura 7.2.8 prueba 8 Betaface [17]



Figura 7.2.9 prueba 9 Betaface [17]



Figura 7.2.10 prueba 10 Betaface [17]



Figura 7.2.11 prueba 11 Betaface [17]

Anexo 3

Diagramas y Modelos del Sistema

Arquitectura del Sistema

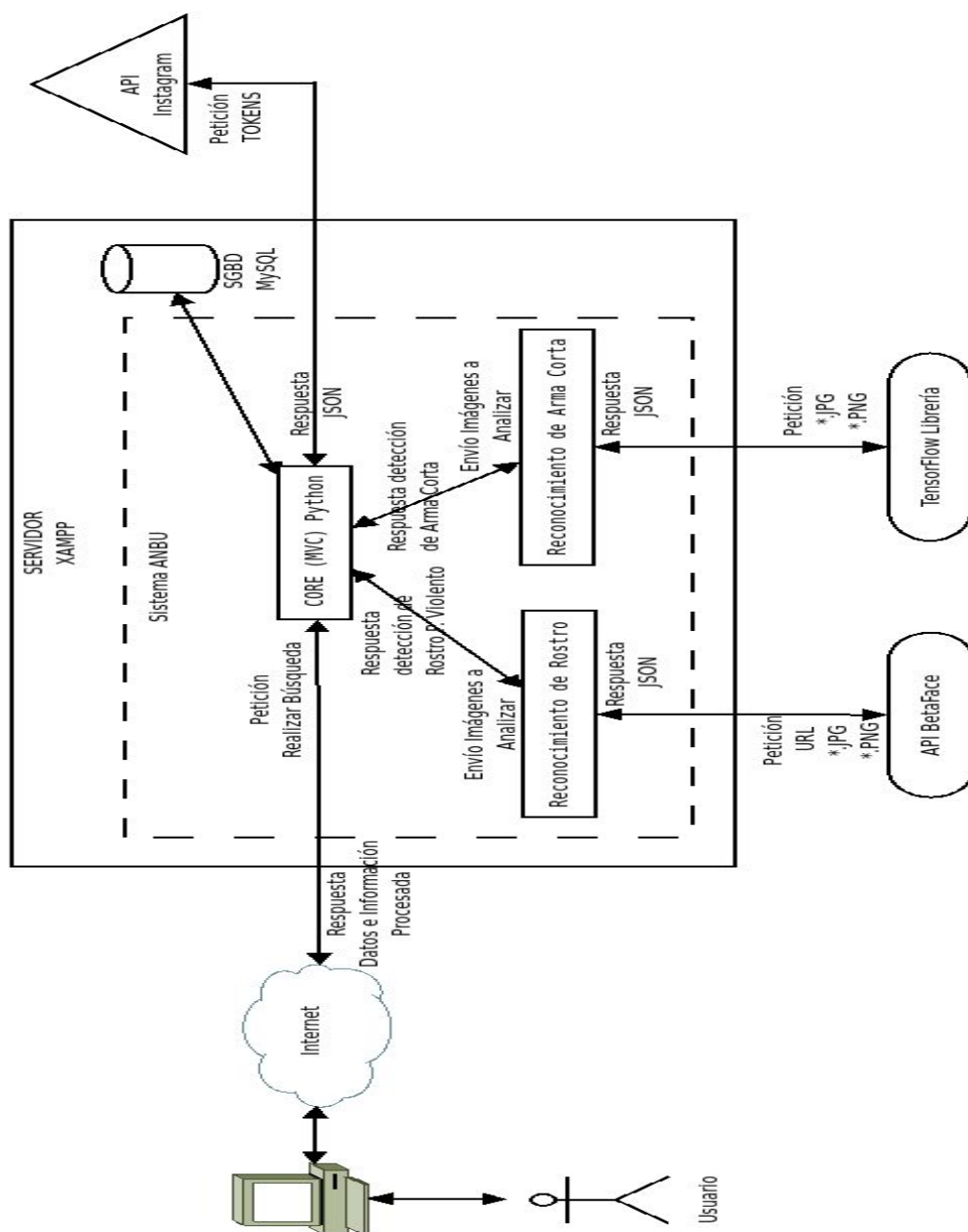
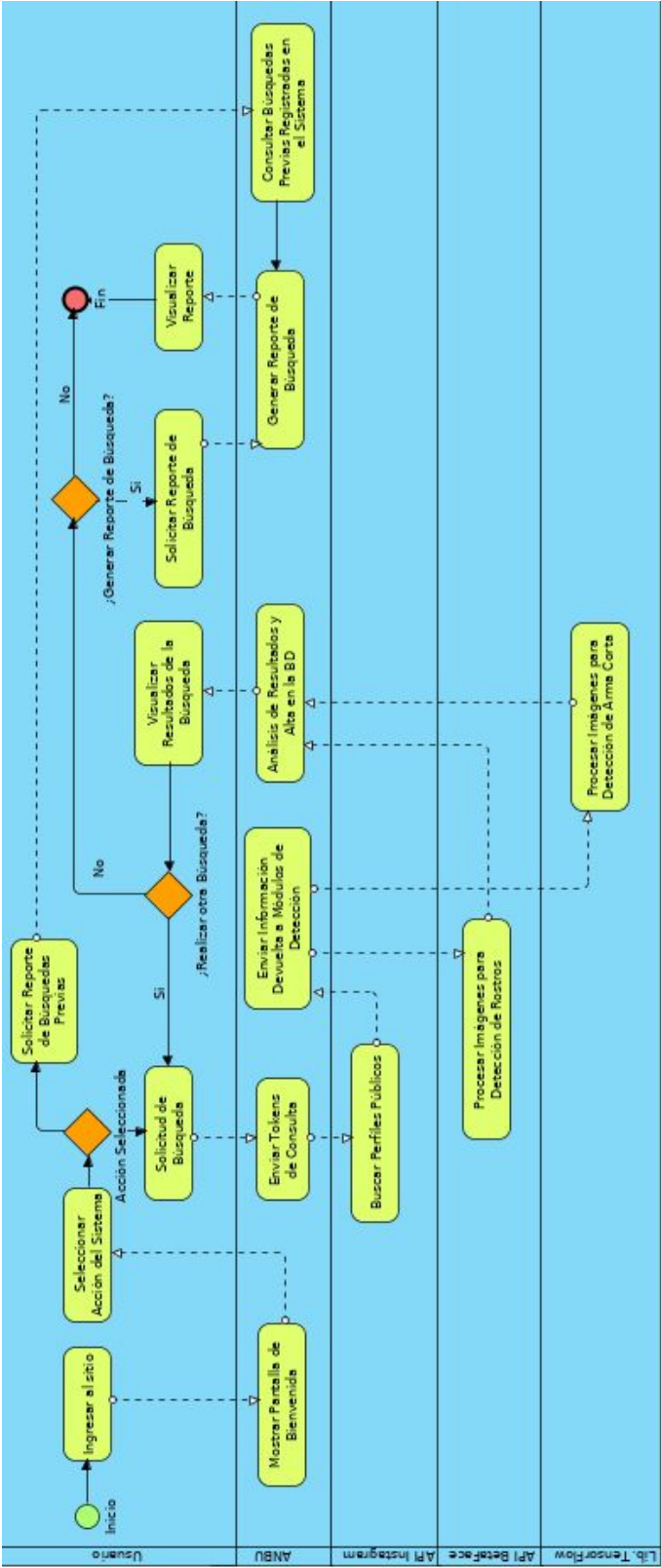
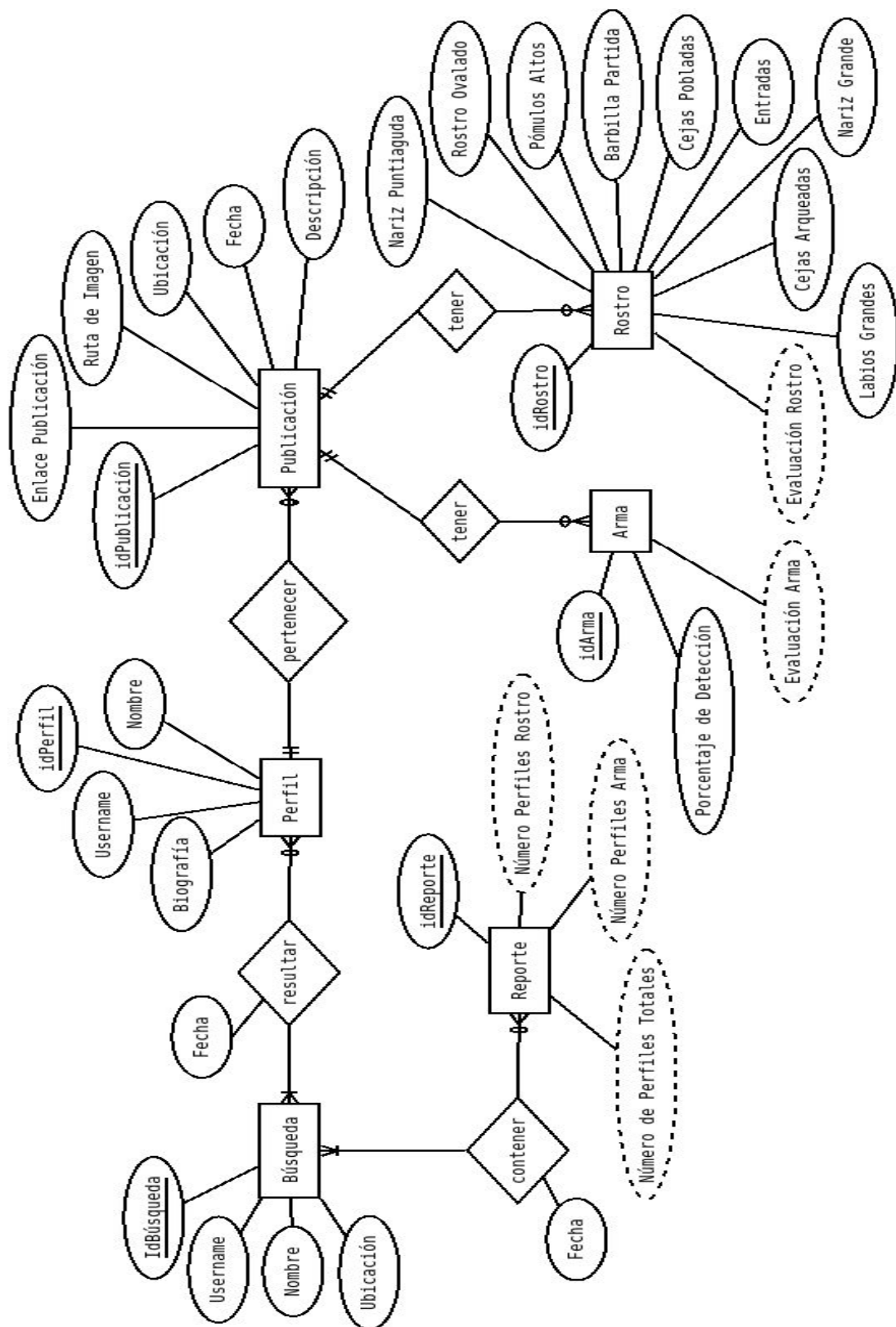


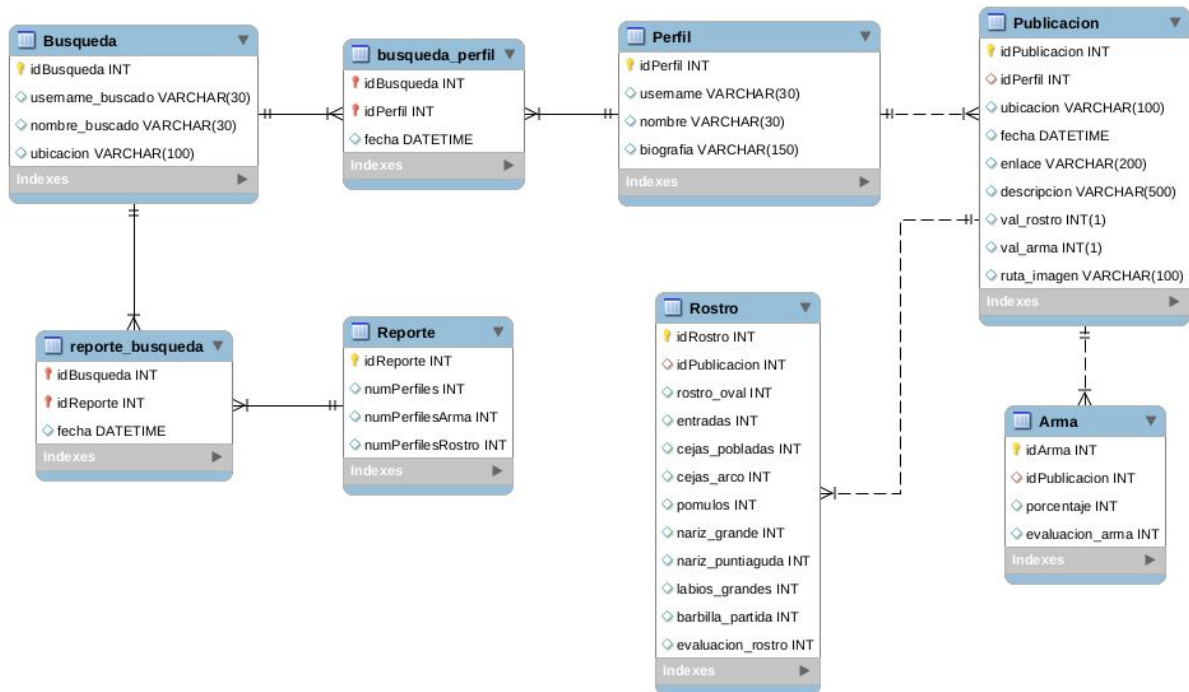
Diagrama de Procesos



Modelo Entidad Relación



Esquema Relacional



Índice de Tablas

1.6	Resumen Motores de Búsqueda -----	6
2.3	Análisis de un rostro violento -----	14
3.1	URI de redireccionamiento API Instagram -----	18
3.2	Operaciones de la API de Betaface -----	21
4.1	Reglas de Negocio -----	28
4.2.1	Requisitos Funcionales -----	31
4.2.2	Requisitos No Funcionales -----	34
4.2.3	relación requerimientos, reglas de negocio -----	35
4.3	Análisis de Riesgos -----	36
4.5.1	Caso de uso Realizar Búsqueda -----	38
4.5.2	Caso de uso Consultar Búsqueda Previa -----	39
4.5.3	Caso de uso Generar Reporte -----	40
4.6.1	Diccionario de Datos Búsqueda -----	44
4.6.2	Diccionario de Datos Perfil -----	44
4.6.3	Diccionario de Datos Publicación -----	45
4.6.4	Diccionario de Datos Reporte -----	45
4.6.5	Diccionario de Datos reporte_busqueda -----	46
4.6.6	Diccionario de Datos busqueda_perfil -----	46
4.6.7	Diccionario de Datos Arma -----	46
4.6.8	Diccionario de Datos Rostro -----	47
5.1	Componentes de la Arquitectura -----	48

Índice de Figuras

2.1.1	Perfil de usuario -----	8
2.1.2	Publicación de usuario -----	10
2.3.1	Puntos clave en el análisis facial -----	11
2.3.2	Rostro 1 -----	15
2.3.3	Rostro 2 -----	15
2.3.4	Rostro 3 -----	15
2.3.5	Rostro 4 -----	15
2.3.6	Rostro 5 -----	15
2.4.1	Ejemplo 1 arma corta -----	16
2.4.2	Ejemplo 2 arma corta -----	16
3.1.1	Petición de acces_token -----	19
3.1.2	Respuesta de acces_token -----	19
3.2.1	Rostro promedio Betaface -----	22
3.2.2	Obtención de los 101 puntos faciales -----	23
3.2.3	Descripción de los puntos faciales por Betaface -----	23
3.3	Ejemplo COCO_SDD -----	26
3.4	Server Apache -----	27
3.5	Logo framework Flask -----	27
4.5.1	Diagrama Caso de Uso -----	41
4.6.1	Diagrama Entidad Relación -----	42
4.6.2	Esquema Relacional -----	43
5.1	Arquitectura del Sistema -----	48
5.2	Diagrama de Proceso -----	50
5.3.1	Diagrama de Secuencia para el Caso de Uso 1 -----	51
5.3.2	Diagrama de Secuencia para el Caso de Uso 2 -----	51
5.3.3	Diagrama de Secuencia para el Caso de Uso 3 -----	52
5.4.1	Vista de la pantalla de inicio -----	52
5.4.2	Vista de búsqueda -----	53
5.4.3	Vista de muestra de resultados -----	54
5.4.4	Vista de consulta de búsqueda -----	55
5.4.5	Vista del resultado de consulta de búsqueda -----	56
5.4.6	Vista de reporte generado -----	57
7.1.1	La cara en el plano medio sagital -----	61
7.1.2	Altura Facial -----	62
7.1.3	Detalles de Ojo y Ceja -----	62
7.1.4	Subunidades de la nariz -----	63
7.1.4.1	Ángulo Nasofrontal -----	63
7.1.4.2	Ángulo Nasolabial -----	64

7.1.4.3 Ángulo Nasofacial -----	64
7.1.4.4 Ángulo Nasomental -----	64
7.1.5 Formas de la nariz -----	65
7.1.6 Posición de los labios -----	65
7.1.7 Posición de la barbilla -----	66
7.1.8 Posición de las orejas -----	66
7.1.9 Posición del cuello -----	67
7.2.1 Prueba 1 Betaface -----	68
7.2.2 Prueba 2 Betaface -----	68
7.2.3 Prueba 3 Betaface -----	69
7.2.4 Prueba 4 Betaface -----	69
7.2.5 Prueba 5 Betaface -----	69
7.2.6 Prueba 6 Betaface -----	70
7.2.7 Prueba 7 Betaface -----	70
7.2.8 Prueba 8 Betaface -----	71
7.2.9 Prueba 9 Betaface -----	71
7.2.10 Prueba 10 Betaface -----	72
7.2.11 Prueba 11 Betaface -----	72

Referencias

- [1] S. Caleano, "Las redes sociales en México alcanzan los 83 millones de usuarios, Marketing 4 Ecommerce, 2019. [Online]. Available: <https://marketing4ecommerce.mx/las-redes-sociales-en-mexico-alcanzan-los-83-millones-de-usuarios/>. [Accessed: 17- Sep- 2019].
- [2] F. Line, "Las 5 redes sociales más usadas en México este 2019", LINE BRANDING, 2019. [Online]. Available: <https://www.linebranding.com/redes-sociales-mas-usadas-en-mexico/>. [Accessed: 24- Sep- 2019].
- [3] La Opinión, "Policía busca a delincuente por Facebook", 2019. [Online]. Available: <https://laopinion.com/2018/02/13/policia-busca-a-delincuente-por-facebook-y-el-se-burla-de-ellos/>. [Accessed: 26- Aug- 2019].
- [4] A. Fiallos, "Detecting Topics and Locations on Instagram Photos", ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/profile/Angel_Fiallos_Ordonez. [Accessed: 16- Aug- 2019].
- [5] Webstagram.org, "Webstagram - Analytics with Instagram Search People", 2019. [Online]. Available: <https://webstagram.org>. [Accessed: 22- Oct- 2019].
- [6] yooying, "yooying-About", 2019. [Online]. Available: <https://www.yooying.com>. [Accessed: 22- Aug- 2019].
- [7] Metaeyes.com, "Metaeyes", 2019. [Online]. Available: <https://www.metaeyes.com>. [Accessed: 20- Aug- 2019].
- [8] Medium Corporation, "How Instagram Started", 2017. [Online]. Available: <https://medium.com/@obtaineudaimonia/how-instagram-started-8b907b98a767>. [Accessed: 22- Aug- 2019].
- [9] LEOGRAM, "What type of Instagram account to choose and how to protect it?", 2019. [Online]. Available: <https://leogram.com/en/blog/tips-security-instagram-accounts>. [Accessed: 09- Sep- 2019].
- [10] Facebook for Developers, "Instagram Basic Display API - Instagram Platform - Documentation - Facebook for Developers", 2019. [Online]. Available: <https://developers.facebook.com/docs/instagram-basic-display-api/>. [Accessed: 22- Oct- 2019].

- [11] D. Burgué, "La Cara, sus Proporciones Estéticas", 2019. [Online]. Available: http://www.sld.cu/galerias/pdf/sitios/protesis/la_cara,_sus_proporciones_esteticas.pdf. [Accessed: 10- Sep- 2019].
- [12] E. Ochoa, "Psicomorfología del Rostro", 2012. [Online]. Available: <http://www.elcuerponomiente.com/publicacion-23>. [Accessed: 22- Oct- 2019].
- [13] D. CARRASCO, "Las caras del mal: cómo reconocer a un psicópata por sus rasgos faciales", ELMUNDO, 2016. [Online]. Available: <https://www.elmundo.es/f5/2016/06/27/57681dfe5fdeac9658b456c.html>. [Accessed: 15- Sep- 2019].
- [14] Ministerio Público-Gerencia General de Lima Perú, "Clasificación de las Armas", 2019. [Online]. Available: https://www.mpfm.gob.pe/escuela/contenido/actividades/docs/3047_resumen_balistica.pdf. [Accessed: 15- Sep- 2019].
- [15] Bersa, "Manual de Instrucción y Seguridad", 2019. [Online]. Available: <http://www.bersa.com.ar/manuales/M-cast-TH9-40yMTH9-40y45.pdf>. [Accessed: 15- Sep- 2019].
- [16] Betaface, "Betaface API 2.0 Documentation", 2019, [Online]. Available: <https://www.betafaceapi.com/wpa/index.php/documentation>
- [17] Fiscalía General de Justicia del Estado de México, "Acciones FGJEM", 2019. [Online]. Available: <http://fgjem.edomex.gob.mx/>. [Accessed: 15- Sep- 2019].
- [18] J. Buhias, "TensorFlow, la plataforma para Inteligencia Artificial de Google", Puentes Digitales, 2015. [Online]. Available: <https://puentesdigitales.com/2018/02/14/todo-lo-que-necesitas-saber-sobre-tensorflow-la-plataforma-para-inteligencia-artificial-de-google/>. [Accessed: 23- Oct- 2019].
- [19] J. Santos, "Object Detection using Tensorflow.js", AI & Machine Learning Blog, 2019. [Online]. Available: <https://nanonets.com/blog/object-detection-tensorflow-js/>. [Accessed: 11- Oct- 2019].
- [20] D. Group, "About the Apache HTTP Server Project - The Apache HTTP Server Project", Httpd.apache.org, 2019. [Online]. Available: https://httpd.apache.org/ABOUT_APACHE.html. [Accessed: 16- Oct- 2019].
- [21] Culturación, "¿Qué es Apache? - Culturación", 2019. [Online]. Available: <http://culturacion.com/que-es-apache/>. [Accessed: 15- Oct- 2019].
- [22] Matt Makai, "Flask", 2019. [Online]. Available: <https://www.fullstackpython.com/flask.html>. [Accessed: 14- Oct- 2019].

- [23] Secretaría de Seguridad Ciudadana, "Policía de Ciberdelincuencia Preventiva", 2019. [Online]. Available: <http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html>. [Accessed: 25- Sep- 2019].
- [24] Julián Pérez Potro y María Merino, "Definición de imagenología", 2011. [Online]. Available: <https://definicion.de/imagenologia/>. [Accessed: 25- Sep- 2019].
- [25] Bermúdez Espinoza Alejandra, "¿La Morfopsicología es Ciencia o Pseudociencia?", (2015), [Online]. Available: https://www.academia.edu/15156219/LA_MORFOPSICOLOG%C3%8DA_ES_UNA_CIENCIA_O_UNA_PSEUDOCIENCIA. [Accessed: 24-Sep-2019]