

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingeniería

Aplicación de Reconocimiento Biométrico para la Seguridad Ciudadana en el Distrito Esteros perteneciente a la Zona 8 de la Policía Nacional del Ecuador

Walter Oswaldo Gómez Vargas

Ingeniería en Sistemas

Trabajo de integración curricular presentado como requisito para la obtención del título de Ingeniero en Sistemas

Quito, 3 de diciembre de 2019

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

COLEGIO DE CIENCIAS E INGENIERIA

**HOJA DE CALIFICACIÓN
DE TRABAJO DE INTEGRACIÓN CURRICULAR**

**Aplicación de Reconocimiento Biométrico para la Seguridad
Ciudadana en el Distrito Esteros perteneciente a la Zona 8 de la
Policía Nacional del Ecuador**

Walter Oswaldo Gómez Vargas

Calificación:

Nombre del Profesor, Título Académico: Fausto Pasmay, MSc.

Firma del Profesor:

Quito, 3 de diciembre de 2019

Derechos de Autor

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante:

Nombres y apellidos:

Walter Oswaldo Gómez Vargas

Código:

00018308

Cédula de identidad:

171054998-9

Lugar y fecha:

Quito, diciembre de 2019

RESUMEN

El presente proyecto tiene como objetivo optimizar las estrategias operacionales que maneja el Distrito Esteros de la Zona 8 de la Policía Nacional del Ecuador. Este objetivo se persigue mediante la mejora del registro e identificación de los ciudadanos que se encuentran requeridos por la justicia y así, poder evitar suplantaciones de identidad.

Para este fin, se propone el desarrollo de una aplicación tecnológica, que utilice datos biométricos, que de manera dinámica y escalable permita identificar a personas aplicando patrones de identificación. Proporcionando así, datos confiables, exactos y eficientes de los individuos que son demandados por la Ley; coadyuvando al desarrollando de la planeación estratégica que se desarrolla en cada unidad territorial en la cual brinda servicio la institución policial, circuitos y subcircuitos que constituyen el Distrito Esteros perteneciente a la jurisdicción del Comando de la Zona 8.

Palabras clave: seguridad ciudadana, estrategias operacionales, aplicación tecnológica, reconocimiento biométrico, patrones de identificación.

ABSTRACT

The present project objective is to optimize the operational strategies managed by the Esteros District of Zone 8 of the National Police of Ecuador. This objective is being pursued by improving the registration and identification of citizens who are required by justice and through it avoiding identity theft.

In order to achieve this objective, this project proposes the development of a technological application, which uses biometric data, so that in a dynamic and scalable way to identify people applying identification patterns. Thus, providing reliable, accurate and efficient data of the individuals who require their registration, in compliance with the constitutional mission, that police servants belonging to the Esteros District of the National Police of Ecuador are required to comply, contributing to the development of strategic planning, which takes place in each territory of the circuits and sub circuits of this police jurisdiction.

Keywords: citizen security, operational strategies, technological application, biometric recognition, identification patterns.

TABLA DE CONTENIDO

INTRODUCCIÓN	10
Objetivo General.....	12
Objetivos Específicos.....	12
DIAGNÓSTICO SITUACIONAL DEL DISTRITO ESTEROS	13
DEFINICIÓN DEL PROBLEMA	20
JUSTIFICACIÓN	21
IDENTIFICACIÓN BIOMÉTRICA	22
Aspectos Generales.....	22
Estructura Operacional.....	23
ANÁLISIS E IMPLEMENTACIÓN DE LA APLICACIÓN	26
Diagrama de Casos de Uso	26
Diagrama de Clases.....	27
Hardware.....	28
Software	28
FLUJO DEL PROCESO DE IDENTIFICACIÓN BIOMÉTRICA	29
DETALLE TÉCNICO DE LA HERRAMIENTA DE DESARROLLO.....	31
Diseño de las Interfaces del Cliente.....	31
Programación.....	32
Ejecución de la Aplicación	33
REFERENCIAS BIBLIOGRÁFICAS.....	41
ANEXO A: DIAGRAMAS DE FLUJO	42
ANEXO B: DIAGRAMA DE CLASES.....	44
ANEXO C: MODELO DE BASE DE DATOS	47

ÍNDICE DE TABLAS

Tabla 1. Circuitos y Subcircuitos Distrito Esteros.....	13
Tabla 2. Cuadro Estadístico Acumulado, Zona 8.....	16
Tabla 3. Cuadro Estadístico por Delitos, Distrito Esteros.....	16
Tabla 4. Cuadro Estadístico a Nivel de Circuitos, Distrito Esteros.....	17
Tabla 5. Cuadro Estadístico a Nivel de Subcircuitos, Distrito Esteros.....	18

ÍNDICE DE FIGURAS

Figura 1. Mapa Distrito Esteros.....	14
Figura 2. Mapa de Georreferenciación de Delitos del CMI, Distrito Esteros.....	19
Figura 3. Arquitectura de un Sistema de Reconocimiento Biométrico.....	25
Figura 4. Diagrama Casos de Uso.....	27
Figura 5. Flujo Proceso de Identificación biométrica.....	30
Figura 6. Plantilla Interfaz Gráfica Huella Digital.....	31
Figura 7. Programación Registro Huella Digital.....	33
Figura 8. Interfaz de Usuario para el Registro de la Base de Datos.....	35
Figura 9. Interfaz Gráfica de los Registros de la Base de Datos.....	36
Figura 10. Interfaz Registro Huella Digital.....	37
Figura 11. Interfaz Registro Huella a Persona.....	38
Figura 12. Interfaz Huella Guardada.....	38
Figura 13. Interfaz Verificación e Identificación.....	39
Figura 14. Interfaz Identificación.....	39

INTRODUCCIÓN

La Institución Policial, acogiendo al proyecto gubernamental de ordenamiento territorial para la desconcentración de los servicios que brinda el poder ejecutivo en territorio, el cual en su momento fue rectorado por la SENPLADES, ahora por la Secretaría Técnica Planifica Ecuador. Desconcentró los servicios policiales a nivel de Zonas de Planificación, Distritos y Circuitos Administrativos, unidades territoriales constituidas con base de la división política administrativa del país considerando la extensión territorial y densidad poblacional.

Sin embargo, la Policía Nacional, vio la necesidad de bajar de nivel territorial por el tipo de servicio que brinda a la ciudadanía. Es así, que se crearon los subcircuitos, unidades territoriales netamente policiales, constituyéndose a nivel país un total de 1.884 subcircuitos, sumándole a ello la implementación del Modelo de Gestión Policial, el cual se fundamenta en la optimización de recursos bajo el principio de territorio – responsabilidad, el cual consiste en la asignación del recurso humano y logístico en función de la caracterización delictual en territorio.

Con lo antes descrito, breve cierto análisis de la problemática delictual que presenta el país se logró determinar al Comando Policial de la Zona 8 para el desarrollo de este proyecto, conformado por los cantones de Guayaquil, Durán y Samborondón pertenecientes a la provincia del Guayas, constituido por 12 Distritos, 67 Circuitos y 274 subcircuitos. La Zona 8, con cerca de 4 millones de habitantes, es considerada la capital económica del Ecuador, donde las actividades comerciales generan un dinamismo único y particular. En consecuencia, de estas condiciones se desprende una complejidad social, fenómenos criminógenos, propios de una alta migración interna promovida por el movimiento económico y la generación de empleo local.

Siendo el Distrito Esteros, uno de los distritos con mayor aporte delincencial en la Zona 8, el cual se encuentra ubicado al sur de la ciudad de Guayaquil, con una población aproximada de 276.236 habitantes¹ y una densidad poblacional de 15.076 hab/Km². Territorio donde existe gran afluencia de población flotante que acuden a realizar actividades comerciales y financieras en diferentes centros de comercio como en Centros Comerciales, Puerto Marítimo, entidades bancarias, locales comerciales, mercados entre otros. El Distrito Esteros, es uno de los doce (12) distritos que conforman el Comando Policial de la Zona 8, está dividido en cinco (5) circuitos y diecinueve (19) subcircuitos. Su problemática delictual se centra en la violencia y la delincuencia, donde la ingesta descontrolada de alcohol y el consumo de sustancias sicotrópicas conlleva a hogares disfuncionales, factor de riesgo para el inicio de la actividad criminal a temprana edad (adolescentes). Se han identificado cuatro factores de connotación social: violencia criminal, violencia social, microtráfico/consumo de drogas y robo a personas.

Considerando la formación profesional y especializada de los funcionarios policiales, basada en el respecto a los Derechos Humanos, cuya misión es atender la seguridad ciudadana y el orden público, mediante la utilización de medios de disuasión y conciliación como alternativas al uso de la fuerza, sumándole a ello la coordinación con autoridades en los diferentes niveles de gobiernos autónomos descentralizados; esta jurisdicción ha orientado sus esfuerzos en la prevención y represión jurídica del delito, como mecanismo para garantizar el orden y la seguridad ciudadana, fundamentando su accionar en un elevado profesionalismo del talento humano, así como la optimización de sus recursos logísticos y tecnológicos. Es así, que la institución policial se ha preocupado en la formación de sus funcionarios, lo cual mediante capacitaciones constantes en operaciones tácticas y tecnológicas han logrado ir de la mano con el avance tecnológico que se posee en la actualidad, sin escatimar recursos en ello.

¹ Instituto Nacional de Estadísticas y Censos, Proyección Poblacional 2010 – 2020 a nivel de Distritos, INEC.

Objetivo General

Desarrollar una plataforma de alta disponibilidad que permita la identificación de individuos en base a la información biométrica de huellas dactilares.

Objetivos Específicos

- Obtener información exacta y detallada de las personas por medio de sus huellas dactilares, al momento de requerirlas por parte de los servidores policiales que cumplen sus actividades de seguridad ciudadana y orden público en el Distrito Esteros.
- Evitar la suplantación de identidad de personas.
- Reducir tiempos de respuesta en procedimientos y operaciones policiales.
- Optimizar el uso de recursos físicos y tecnológicos.
- Mostrar información actualizada en tiempo real de manera exacta y de fácil interpretación.
- Establecer protocolos de comunicación para consumir datos demográficos y biométricos del Registro Civil a nivel nacional.
- Establecer e implementar protocolos de cooperación con organismos de control nacionales según surja la necesidad.
- Ofrecer una aplicación multiplataforma de fácil acceso y uso para los servidores policiales del Distrito Esteros, que trabaje de manera eficaz y eficiente sin importar el medio de comunicación.
- Extender su uso y portabilidad a entidades que están inmersas en la seguridad ciudadana que lo requieran.

DIAGNÓSTICO SITUACIONAL DEL DISTRITO ESTEROS

Dentro del proyecto de desconcentración de los servicios de las instituciones públicas, el Comando Policial de la Zona 8, se encuentra constituido por 12 Distritos, 67 Circuitos Administrativos y 274 subcircuitos, estas últimas unidades territoriales netamente policiales según el Modelo de Gestión de la institución policial; jurisdicciones donde se prestan los servicios de policía, con la optimización de recursos tanto humano como logístico bajo el principio de territorio – responsabilidad.

Bajando de nivel y focalizándose en el Distrito Esteros, está jurisdicción la conforman cinco (5) circuitos y diecinueve (19) subcircuitos, unidades territoriales que permiten brindar el servicio policial de manera directa a la ciudadanía.

En la Tabla 1, se detalla cada una de las unidades territoriales que forman parte del Distrito Esteros, con su respectiva codificación de identificación, la cual permite el anclaje con diferentes bases de datos de instituciones públicas que se acogen al proyecto gubernamental de desconcentración de servicios.

UNIDADES TERRITORIALES - DISTRITO ESTEROS			
CÓDIGO CIRCUITO	NOMBRE CIRCUITO	CÓDIGO SUBCIRCUITO	NOMBRE SUBCIRCUITO
09D02C01 09D02C01 09D02C01 09D02C01	ESTEROS	09D02C01S01 09D02C01S02 09D02C01S03 09D02C01S04	ESTEROS 1 ESTEROS 2 ESTEROS 3 ESTEROS 4
09D02C02 09D02C02 09D02C02	MALVINAS 1	09D02C02S01 09D02C02S02 09D02C02S03	MALVINAS SUR 1 MALVINAS SUR 2 MALVINAS SUR3
09D02C03 09D02C03 09D02C03	MALVINAS 2	09D02C03S01 09D02C03S02 09D02C03S03	MALVINAS NORTE 1 MALVINAS NORTE 2 MALVINAS NORTE 3
09D02C04 09D02C04 09D02C04 09D02C04	TRINITARIA NORTE	09D02C04S01 09D02C04S02 09D02C04S03 09D02C04S04	TRINITARIA NORTE 1 TRINITARIA NORTE 2 TRINITARIA NORTE 3 TRINITARIA NORTE 4
09D02C05 09D02C05 09D02C05 09D02C05 09D02C05	TRINITARIA SUR	09D02C05S01 09D02C05S02 09D02C05S03 09D02C05S04 09D02C05S05	TRINITARIA SUR 1 TRINITARIA SUR 2 TRINITARIA SUR 3 TRINITARIA SUR 4 TRINITARIA SUR 5

Tabla 1. Circuitos y Subcircuitos, Distrito Esteros

Fuente: Policía Comunitaria, Distrito Esteros.

El Distrito Esteros, durante los últimos 5 años ha sido uno de los distritos con una alta problemática delictual a nivel país, donde la violencia criminal ha superado en cierta manera a la violencia social por un sin número de aspectos que se analizarán en el desarrollo de este proyecto.

En la Figura 1, se puede apreciar la problemática delictual por medio del criterio de semaforización a nivel de circuitos; donde se evidencia que el circuito Esteros donde se concentra la mayor carga delictiva en este Distrito, seguido del circuito colindante, Malvinas Sur, Malvinas Norte, Trinitaria Sur y por último Trinitaria Norte.

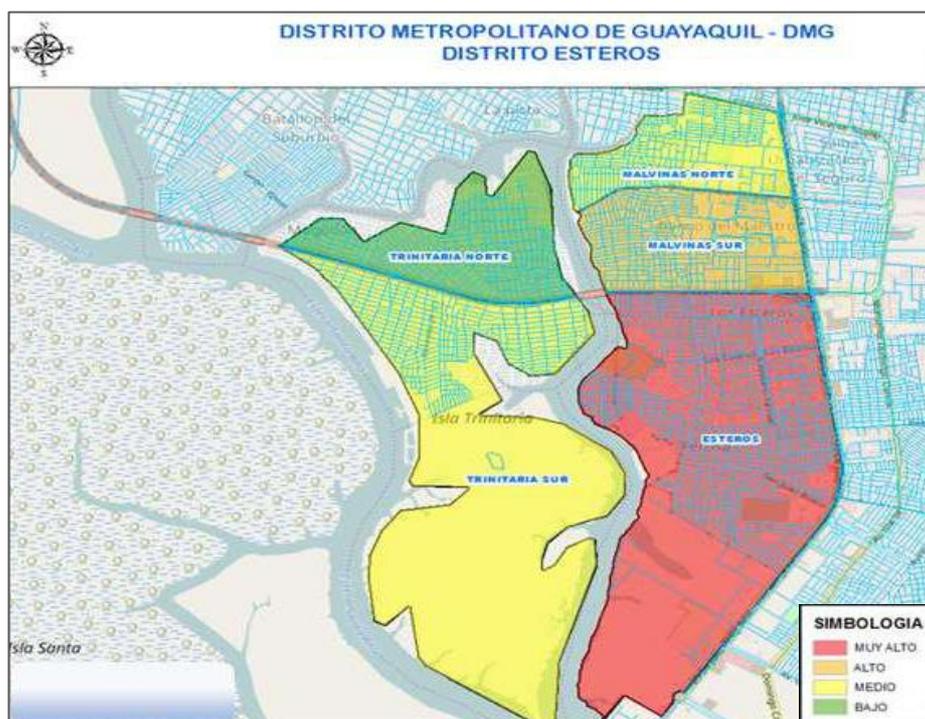


Figura 1. Mapa Distrito Esteros.

Fuente: DAID Zona 8.

Dentro del análisis delictual, en este distrito se ha establecido cuatro factores de connotación social: violencia criminal, violencia social, microtráfico-consumo de drogas y robo a personas.

Durante el año 2019, el Distrito Esteros su comportamiento delictual se ha mantenido en crecimiento, lo cual ha dado a lugar a que esta jurisdicción sea priorizada, es decir, focalizar todo el accionar policial a fin de contrarrestar los hechos delictivos.

Es preciso señalar que el Estado Ecuatoriano dentro de su política de seguridad ciudadana, ha coordinado con la Policía Nacional del Ecuador la aplicación de una herramienta de monitoreo y planificación estratégica denominada Cuadro de Mando Integral (CMI), la cual permite a través del Departamento de Análisis de Información del Delito (DAID), examinar estrategias operacionales y situacionales asociadas al comportamiento delictual para la aplicación de acciones eficaces y eficientes, en el control y prevención del delito.

La base primaria de esta herramienta son las denuncias presentadas y validadas por la Fiscalía General del Estado, referente a los delitos de mayor connotación social como son: Homicidios y Asesinatos, Robo a Personas, Robo a Domicilios, Robo a Unidades Económicas, Robo a Carros, Robo a Motos, Robo de Accesorios, Bienes y Autopartes en Vehículos y Robo en Ejes Viales o Carreteras.

El Distrito Esteros, es uno de los territorios de la Zona 8, donde la violencia y delincuencia presenta un incremento constantemente. Como se observa en la Tabla No. 2, CMI, que esta jurisdicción concentra el 8% de la problemática delictiva de la Zona 8 en lo que va del año 2019, registra un incremento del 12% con respecto al año anterior, con un total de 1.073 delitos lo que da como resultado de un incremento de 116 eventos más que el año anterior, ocupa la sexta posición del ranking a nivel de Distrito de la Zona 8.

DISTRITOS	TOTAL CMI						
	TOTAL	FRECUENCIA		VARIACIÓN		PORCENTAJE	
	01 ene al 31 ago 2018	01 ene al 30 ago 2018	01 ene al 30 ago 2019	V.A.	V.%	2018	2019
MODELO	2098	2093	2526	433	20,7%	18%	20%
9 DE OCTUBRE	1689	1687	1995	308	18,3%	15%	15%
FLORIDA	1147	1143	1270	127	11,1%	10%	10%
SUR	1126	1123	1188	65	5,8%	10%	9%
PORTETE	917	915	1136	221	24,2%	8%	9%
ESTEROS	960	957	1073	116	12,1%	8%	8%
PASCUALES	887	886	1027	141	15,9%	8%	8%
NUEVA PROSPERINA	758	750	921	171	22,8%	7%	7%
DURAN	937	932	809	-123	-13,2%	8%	6%
CEIBOS	173	173	190	17	9,8%	2%	1%
SAMBORONDON	120	120	127	7	5,8%	1%	1%
PROGRESO	97	97	115	18	18,6%	1%	1%
DMG	11359	11324	12912	1.588	14,0%	100%	100%

Tabla 2. Cuadro Estadístico Acumulado Zona 8.

Fuente: DAID Zona 8.

Realizando un análisis más exhaustivo, se observa en la Tabla No. 3, que todos los delitos de mayor connotación que son monitoreados en el CMI, en el Distrito Esteros presentan un incremento en lo que va del año con respecto al año anterior, siendo el Robo a Personas el delito que caracteriza a esta jurisdicción. Cabe mencionar que los Homicidios/Asesinatos han presentado un incremento considerable del 56% con respecto al año 2018, indicador que identifica a este territorio como uno de los más violentos de la Zona 8.

DISTRITO	TOTAL	FRECUENCIA		VARIACIÓN		PORCENTAJE	
	01 ene al 31 ago 2018	01 ene al 30 ago 2018	01 ene al 30 ago 2019	V.A.	V.%	2018	2019
HOMICIDIOS/ASESINATOS	16	16	25	9	56,3%	2%	2%
ROBO A PERSONAS	603	602	621	19	3,2%	63%	58%
ROBO DOMICILIO	79	78	93	15	19,2%	8%	9%
ROBO A UNIDADES	20	20	23	3	15,0%	2%	2%
ROBO A CARROS	77	76	100	24	31,6%	8%	9%
ROBO A MOTOS	87	87	109	22	25,3%	9%	10%
ROBO DE BIENES,	78	78	102	24	30,8%	8%	10%
ROBO EN EJES VIALES O	0	0	0	0	0,0%	0%	0%
TOTAL CMI	960	957	1073	116	12,1%	100%	100%

Tabla 3. Cuadro Estadístico por Delitos - Distrito Esteros.

Fuente: DAID Zona 8.

A nivel de circuitos, Esteros es el territorio donde se concentra el 34% de la carga delictual del Distrito Esteros comportamiento que lo ha mantenido en estos últimos cinco años, sin embargo, el circuito Trinitaria Norte es el que presenta el mayor incremento en lo que va del año con respecto al año 2018, registrando un incremento de un poco más del 41%, lo cual se evidencia en la Tabla No. 4 que se detalla a continuación.

ESTEROS	TOTAL	FRECUENCIA		VARIACIÓN		PORCENTAJE	
	01 ene al 31 ago 2018	01 ene al 30 ago 2018	01 ene al 30 ago 2019	V.A.	V.%	2018	2019
ESTEROS	299	299	360	61	20,4%	31%	34%
TRINITARIA NORTE	119	119	168	49	41,2%	12%	16%
TRINITARIA SUR	218	216	253	37	17,1%	23%	24%
MALVINAS SUR	151	150	136	-14	-9,3%	16%	13%
MALVINAS NORTE	173	173	156	-17	-9,8%	18%	15%
TOTAL	960	957	1073	116	12,1%	100%	100%

Tabla 4. Cuadro Estadístico a Nivel de Circuitos - Distrito Esteros.

Fuente: DAID Zona 8.

En la Tabla 5, se presenta un ranking a nivel de subcircuito con respecto a la variación absoluta anual 2019 vs. 2018 de los delitos de mayor connotación social que son monitoreados en el CMI, donde se observa que los diez primeros territorios están compuestos por los subcircuitos que conforman los circuitos de: Esteros, Trinitaria Norte y Trinitaria Sur. Siendo, Trinitaria Norte 1, el subcircuito que registra un incremento considerable de los delitos del CMI con un total de 32 eventos, lo que representa una variación porcentual del 91%; seguido de los subcircuitos Esteros 4, Esteros 1 y Esteros 2 que registran un incremento de 25, 21 y 20 delitos, respectivamente.

Cabe mencionar que con este análisis también se identificó ocho subcircuitos que presentan una reducción en la incidencia delictiva, donde Malvinas Norte 1 es el territorio que registra un decremento considerable de 15 delitos en lo que va del año con respecto al año

2018; seguido de Malvinas Norte 3 y Malvinas Sur 2 con una reducción de 7 y 6 delitos, respectivamente.

		TOTAL CMI				
ORD.	SUBCIRCUITOS	01 ene al 31 ago 2018	01 ene al 30 ago 2018	01 ene al 30 ago 2019	V.A	V.P
10 INCREMENTO	1 TRINITARIA NORTE 1	35	35	67	32	91,4%
	2 ESTEROS 4	29	29	54	25	86,2%
	3 ESTEROS 1	34	34	55	21	61,8%
	4 ESTEROS 2	113	113	133	20	17,7%
	5 TRINITARIA NORTE 2	38	38	57	19	50,0%
	6 TRINITARIA SUR 1	21	21	37	16	76,2%
	7 TRINITARIA SUR 5	28	28	39	11	39,3%
	8 TRINITARIA SUR 2	41	41	51	10	24,4%
	9 MALVINAS NORTE 2	18	18	23	5	27,8%
	10 TRINITARIA SUR 4	30	29	34	5	17,2%
08 DECREMENTO	11 TRINITARIA NORTE 4	20	20	20	0	0,0%
	12 TRINITARIA NORTE 3	26	26	24	-2	-7,7%
	13 MALVINAS SUR 3	27	26	23	-3	-11,5%
	14 ESTEROS 3	123	123	118	-5	-4,1%
	15 MALVINAS SUR 1	82	82	77	-5	-6,1%
	16 TRINITARIA SUR 3	98	97	92	-5	-5,2%
	17 MALVINAS SUR 2	42	42	36	-6	-14,3%
	18 MALVINAS NORTE 3	43	43	36	-7	-16,3%
	19 MALVINAS NORTE 1	112	112	97	-15	-13,4%
TOTAL		960	957	1073	116	12,1%

Tabla 5. Cuadro Estadístico a Nivel de Subcircuitos Distrito Esteros.

Fuente: DAID Zona 8.

Realizando un análisis delictual espacial del Distrito Esteros, se observa en la Figura 2, que la concentración de los delitos de Robo a Personas se presenta en la vía Perimetral entre los circuitos de Trinitaria Norte y Trinitaria Sur, vía de acceso rápido y de conexión entre la parte sur y norte de la ciudad de Guayaquil.

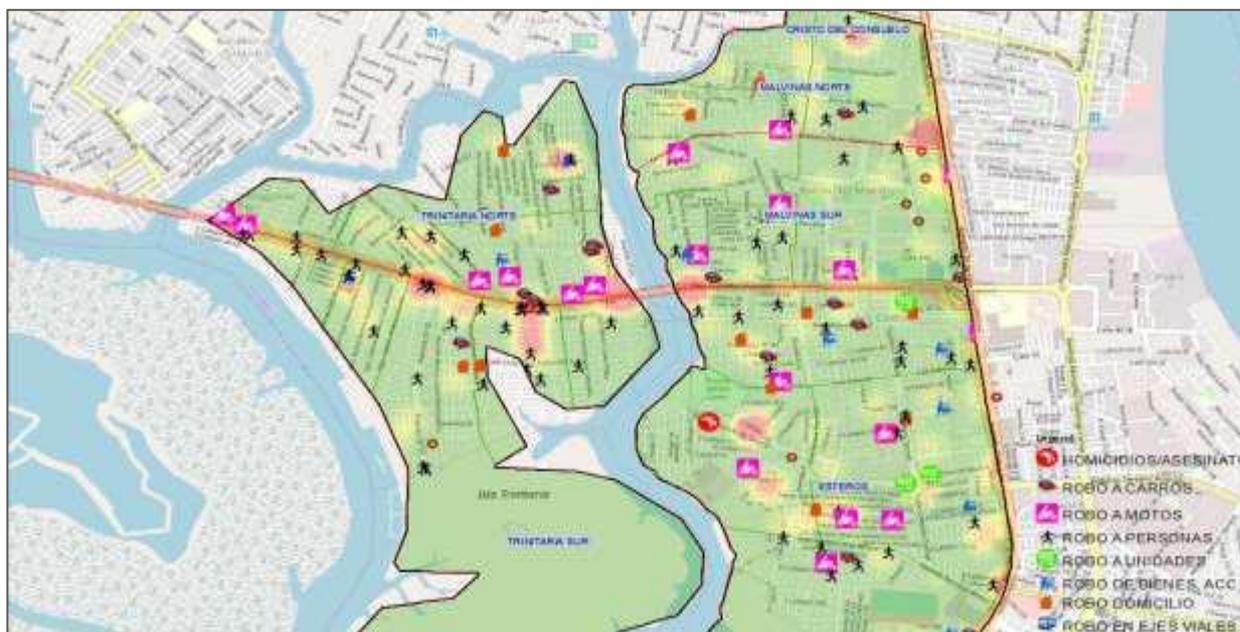


Figura 2. Mapa Georreferenciación de Delitos del CMI, Distrito Esteros.

Fuente: DAID Zona 8.

Con toda la complejidad delictual que presenta la Zona 8, la institución policial se ha focalizado en el cumplimiento de la misión institucional, en atender la seguridad ciudadana y mantener el orden público, utilizando estrategias y herramientas tecnológicas, es así, que el desarrollo de este proyecto y su implementación en la institución aportará en el accionar policial con información personal en línea de los usuarios, por así decirlo, de las personas que participan en los operativos policiales, permitiendo tener datos reales y confiables que se encuentran en bases de datos oficiales, como por ejemplo la del Registro Civil.

DEFINICIÓN DEL PROBLEMA

Tomando en consideración que los servidores policiales pertenecientes al Distrito Esteros, usualmente para la verificación de personas en esta jurisdicción demandan que se tenga un documento de identificación físico (cédula de identidad, pasaporte, credencial del lugar donde labora, etc.) o en algunos casos que la persona brinde el número de documento de identificación.

Los servidores policiales en el cumplimiento de sus funciones en algunas ocasiones es de crucial importancia saber la identidad de determinadas personas que se registra, ya que estas podrían estar suplantando una identidad lo que conllevaría a dejar de lado la verificación de antecedentes o registros delictuales, procedimientos relevantes para la prevención y disuasión de los índices delictuales.

Es así como los servidores policiales del Distrito Esteros en el desarrollo de sus actividades rutinarias requieren saber la identificación exacta y el pasado judicial de individuos sospechosos los cuales no poseen documentos de identificación o proporcionan números de cedula que no les podría pertenecer

Por lo que ante la falta de una herramienta tecnológica que permita saber esta información de manera inmediata, se podría incurrir en dejar libre a algún antisocial que se encuentra requerido por la justicia.

JUSTIFICACIÓN

El desarrollo de la aplicación de Reconocimiento Biométrico para la Seguridad Ciudadana en el Distrito Esteros surge de la necesidad de obtener información importante de manera confiable, y en el menor tiempo posible, de cualquier persona que los servidores policiales pertenecientes al Distrito Esteros tengan la necesidad de hacerlo, sin importar en qué parte geográfica de su jurisdicción se encuentren, ni qué medio de comunicación utilicen.

Con tan solo poner la huella dactilar en un lector biométrico de la persona que se requiere la información se podrá evitar suplantaciones de identidad; optimizando los recursos y las estrategias operacionales que mantiene el Distrito Esteros.

IDENTIFICACIÓN BIOMÉTRICA

Aspectos Generales

De forma general la biometría se describe por el estudio de las características que los seres humanos poseen. En la actualidad estas características pueden ser usadas con métodos automáticos para poder identificar y autentificar personas. Es así, que la biometría es parte de seguridad informática, donde los sistemas de seguridad dentro de sus puntos críticos requieren diferenciar e identificar personas.

La técnica de la identificación de reconocimiento biométrico nace de la necesidad de poder identificar a los seres humanos, de acuerdo a las características físicas únicas que tenemos cada individuo, siendo la huella dactilar uno de los rasgos físicos vinculados a los seres humanos que siempre estarán presentes, y que cumplen propiedades de los rasgos identificativos como son: la universalidad, la unicidad, la aceptabilidad y la permanencia; lo que permitirá la identificación de las personas de manera inmediata.

Las particularidades comunes de identificación humana son los que se representan con las características físicas como la huella digital, retina e iris, rayas de mano, entre otros (biometría estática) y los que se establecen con las características conductuales como la escritura manuscrita, voz, gestos, entre otros (biometría dinámica).

Los sistemas de identificación biométrica, en la actualidad han mejorado la manera de rescatar las características y minucias de la huella dactilar, es decir realizan la extracción de las huellas de manera más minuciosa y detallada. Entonces el proceso de identificación de un individuo en una base de datos con plantillas dactilares existentes puede alcanzar un umbral de confiabilidad del 99.9 %, la diferencia estaría relacionada con interferencias como suciedad, heridas, asperezas o falta de dedos².

² Kenneth R, Moses. (s.f.). *The Fingerprint: Automated Fingerprint Identification System*. Estados Unidos (Washington): Department of Justice Office of Justice Programs.

Es preciso indicar que todos los sistemas de reconocimiento no son 100% perfectos, también existe susceptibilidad a fallos, por ejemplo, en sistemas de reconocimiento de geometría de la mano, enfermedades como artritis, reumatismo pueden causar interferencias, en un sistema de reconocimiento de iris-retina, gafas, o infecciones oculares pueden causar interferencias.

Estructura Operacional

Para poder utilizar el reconocimiento biométrico, en nuestro caso específico, la huella digital de las personas se requiere de un hardware, que es la parte física de los dispositivos biométricos los cuales pueden ser de tipo óptico, estado sólido ó de sensores de ultrasonido. En nuestro caso particular los sensores ópticos, realizan la toma de la huella dactilar y transforman estas características únicas que se extraen en imágenes analógicas a una señal digital (0 y 1), con estándares (ISO/IEC 19794-2). De esta manera permite enviar esta información a la aplicación de identificación de reconocimiento biométrico. Y de un software que constituyen los programas, controladores, los cuales permiten trabajar con el lector biométrico en nuestra aplicación, donde requerimos invocar a las funciones definidas por el fabricante de nuestro lector y arrancamos la implementación según nuestro flujo de procesos.

[ANEXO A: Diagrama de Flujo]

Esto permite tener información mediante las características de patrones únicos que posee una persona es sus huellas digitales; para posterior ser validadas, verificadas y procesadas en un sistema informático. El cual nos proveerá un resultado luego de la autenticación e identificación respectiva.

Una vez realizada la extracción de las características físicas mediante el lector biométrico, el software de la aplicación utilizando métodos propios del lector biométrico, y de acuerdo con el flujo de procesos, nos permite tener la información mediante las características

de patrones únicos que posee una persona es sus huellas digitales; para posterior ser validados, verificados y procesados en un sistema informático, que nos proveerá del resultado pertinente luego de la autenticación e identificación respectiva.

Cabe mencionar que, para establecer el tiempo estimado de respuesta, de la información procesada en nuestra aplicación se deben considerar algunos aspectos como son: los Índices de la Base de datos, la memoria RAM, el procesador, el tipo de tecnología de almacenamiento de datos, la arquitectura de Clustering / Balanceo.

Lo que se pretende con esta arquitectura es tener redundancia de servidores, para evitar caídas, saturaciones, retardos y optimización de respuestas ante la gran carga de trabajo que se pueda procesar. Brindando así una estructura de alta disponibilidad, eficiente y tolerante a fallos.

En torno a los índices: Para nuestra base de datos local, al tener en la etapa de prueba un número menor de 10 mil registros, es suficiente utilizar índices default en nuestras tablas.

En torno a la Memoria RAM: Actualmente nuestro servidor cuenta con 8 GB RAM DIMM, lo cual es suficiente para la carga transaccional de la base de datos. Al incrementar la memoria RAM podremos manejar más tareas, procesos, permitiendo más solicitudes a ser atendidas en menor tiempo.

En torno al Procesador: Actualmente nuestro servidor posee con un procesador Intel(R) Xeon(R) CPU E5-2603 v4 @ 1.70GHz. Este procesador es suficiente para la carga transaccional, de esta manera opera sin retardos y con respuestas eficientes.

En torno a la tecnología de almacenamiento de datos, nuestro servidor utiliza discos duros con interfaz SAS (Serial Attached SCSI), al utilizar esta interfaz la velocidad de rotación aumenta a 15K que es más del doble que utilizar discos con interfaz SATA (Serial Advanced Technology Attachment) 7.2 K, por ende, el IOPS (Inputs Outputs Per Second) es mayor: los

15K SAS rinden a unos 180 IOPS y 7.2K SATA es 80 IOPS. En resumen, nuestro servidor permite procesar 12 Gbit/s

Con las anteriores características expuesta, nuestro servidor está en la capacidad de realizar búsquedas indexadas menores a 4 segundos de un total de 100 millones de registros; y este tiempo puede mejorar realizando una inversión principalmente en el Hardware, donde si se lo requiriera, podríamos aumentar la memoria RAM a 64 G (Servidor permite escalar hasta 128 G RAM), incluir otro procesador en el servidor (Servidor permite escalar hasta 2 procesadores, dependiendo del modelo puede aceptar más de 2 procesadores) , cambiar los discos duros con interfaz SAS (HDD) a unidades de disco Sólido (SSD) , mejorando así la velocidad de respuestas hasta 20 veces más rápido. Además, al incluir una arquitectura de Balanceo de Carga podremos tener más de un servidor con estas características reduciendo así significativamente los tiempos de respuesta. Teniendo una arquitectura escalable, es decir a mayor cantidad de registros y peticiones, más nodos que permitan optimizar dichas peticiones y tiempos de respuesta.

La Figura 3, nos muestra la arquitectura de un sistema de reconocimiento biométrico, donde mediante un sensor obtenemos datos biométricos, para posterior ser procesados y guardados en una base de datos, para cuando se los requiera estos datos sean aceptados o rechazados luego de ser comparados, verificados, autenticados y procesados.

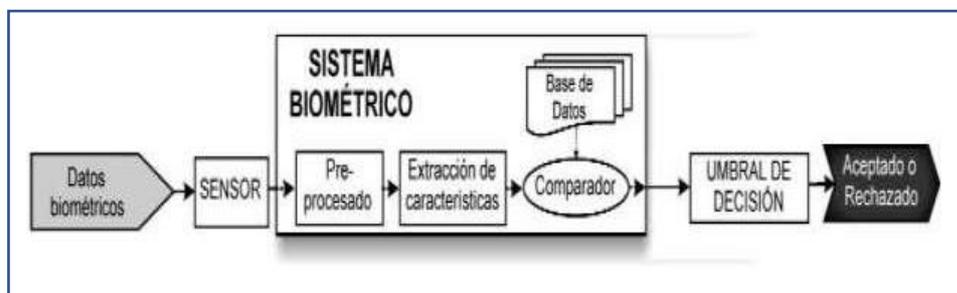


Figura 3: Arquitectura de un Sistema de Reconocimiento Biométrico.
Fuente: Biometría y Seguridad (Isdefe-UPM)

ANÁLISIS E IMPLEMENTACIÓN DE LA APLICACIÓN

Dentro de una estructura operacional de los sistemas de identificación biométricos, el registro, la identificación y la verificación son los procesos básicos e indispensables que se cumplen para poder tener datos exactos de una persona. Las huellas dactilares son exclusivas y únicas de cada persona, y nunca cambian incluso aunque pase la edad. No existen dos personas en el planeta con las mismas huellas dactilares, ni siendo hermanos gemelos idénticos comparten el patrón de huellas dactilares³.

Siendo necesario en la primera etapa contar con una base de datos sólida que nos servirá para poder comparar patrones o modelos de los rasgos característicos que tiene cada persona. Ya en la etapa de verificación es preciso contar con los datos o registros de entrada que proporcione una persona, con el fin de poderlos comparar con los datos y registros que se encuentran almacenados en la base de datos, en donde luego de la verificación pertinente tendremos el resultado si los patrones de coincidencia son afirmativos o negativos. Por último, en la etapa de identificación se establecen exclusivamente los patrones o datos a identificar, obteniendo como resultado la identidad de la persona que ha sido registrada.

La aplicación utilizará las arquitecturas de Aplicaciones Distribuidas que contemplan WebAPP(Web Services: SOAP,REST), aplicaciones móviles , aplicaciones Híbridas.

Diagrama de Casos de Uso

En la Figura 4, se muestra como un servidor policial, puede utilizar la aplicación en varios escenarios. Por ejemplo, en una revisión rutinaria en el cumplimiento de sus funciones de seguridad ciudadana, solicita a ciudadanos sospechosos su identificación, el ciudadano pone su huella dactilar en el lector e inmediatamente se obtiene los datos del ciudadano. Si se obtiene

³ INTERPOL , (2018). *Huellas Dactilares: Sistemas Automáticos*. INTERPOL

alguna alerta pendiente con la Fiscalía, el servidor policial procederá a su detención y pondrá al ciudadano a órdenes de la autoridad competente.

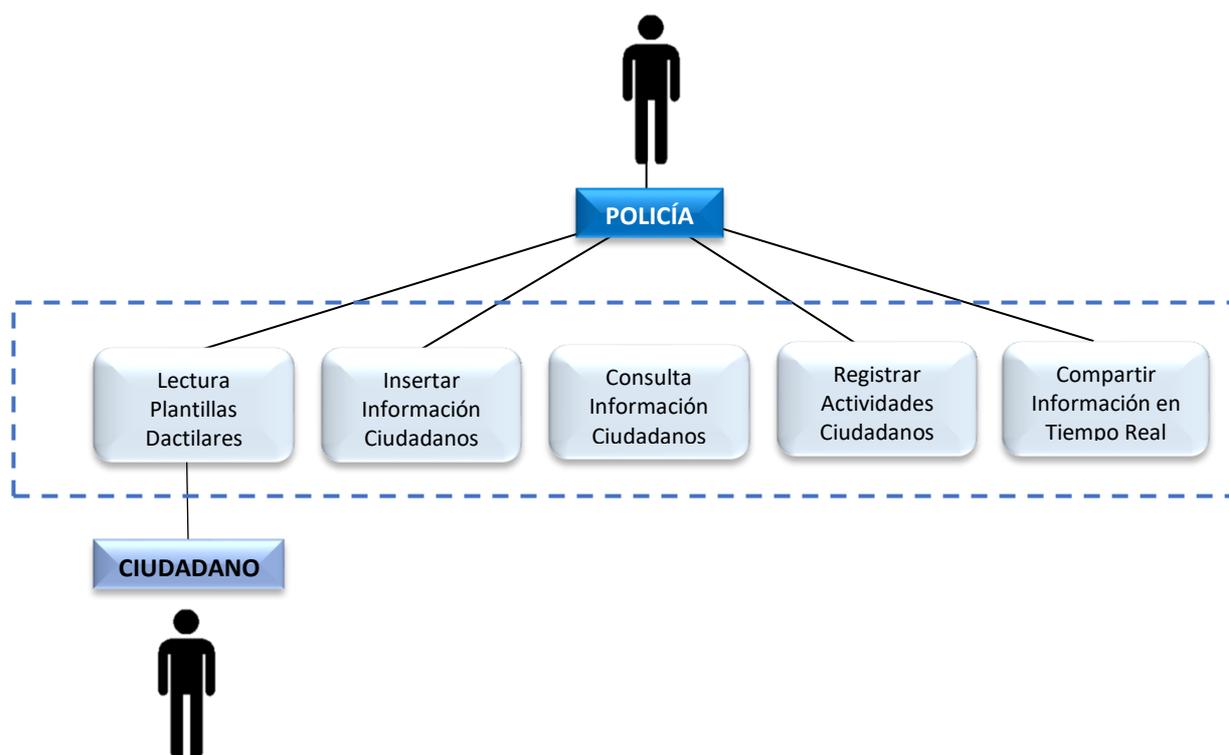


Figura 4. Diagrama Casos de Uso
Fuente: Autor del Proyecto

Diagrama de Clases

Los diagramas de clases se relacionan por medio de los atributos que hacen de identificadores; para este diseño básico, la clase principal es Ciudadano el cual tiene como identificador primario el atributo id. Ahora en la clase Somhue (AlgunaHuella) se hace una referencia al atributo id de la clase Ciudadano, dicha referencia se maneja en el atributo idciudadano de la clase Somhue. De igual manera en la clase Registros_visitas se hace una referencia al atributo id de la clase Ciudadano, dicha referencia se maneja en el atributo idciudadano. [ANEXO B: Diagrama de Clases]

Hardware

- PC-desktop, Laptop, Notebook, Tablet, Smartphone: Los dispositivos nombrados permiten interactuar con la plataforma dinámica y establecen conexión con servidores remotos. Así mismo permitirán mostrar la información de respuesta.
- Servidores remotos donde reside la base de datos con la que realizamos los procesos de verificación, ingreso de información y esto a su vez permite compartir la información y realizar notificaciones en línea.
- Lector biométrico: El dispositivo biométrico óptico, Marca: Digital Persona U. are. U 4500, Año: 2013, Firmware: SDK 1.6.1/ SDK for Android , S.O.: Windows, Linux, Android. Permite realizar la toma de huella dactilar y se sincroniza con los dispositivos para de esta manera poder complementar el proceso y realizar la presentación de la información.
- Servidores externos: Equipos que almacenan la información de las plantillas dactilares, estos son importantes ya que permiten realizar el “matching” y así poder identificar a las personas. Para nuestra aplicación trabajamos con un servidor externo que físicamente se encuentra en Ecuador, en la ciudad de Guayaquil. En este servidor reside un Web Service que receipta la huella dactilar y realiza el proceso de matching y devuelve los datos asociados del individuo; siendo ésta una aplicación distribuida.

Software

- Android Studio superior a 9.0: IDE que permite desarrollar aplicaciones móviles para Smartphone, Tablets, etc. que tengan como sistema operativo Android, tecnología que será utilizada para la segunda fase del proyecto
- Xcode: IDE DARA37: (Integrated Development Environment) Entorno Integrado de Desarrollo. Permite desarrollar aplicaciones móviles para Smartphone, Tablets, etc que

tengan como sistema operativo iOS, tecnología que será utilizada para la segunda fase del proyecto

- SDK Fingerprint Reader: Librerías que permiten crear acciones y eventos compatibles con el lector biométrico.
- NetBeans: IDE que permite crear aplicaciones web 3-capas y N-capas y aplicaciones móviles.
- Sistemas Operativos Windows, Android, IOS, Linux.
- JAVA: Lenguaje de programación y una plataforma informática que permite crear aplicaciones.
- Web server Glassfish, desarrollado por Oracle SUN versión 4.1.1 en el cual desplegamos los Web Services necesarios para poder recibir las solicitudes de verificación contra los registros que se encuentran en la base de datos y a la vez procesar otras peticiones como ingreso de información, notificaciones ,compartir en línea.
- Motor de Base de datos, desarrollado por PostgreSQL es donde almacenamos la información que necesitamos, registros de ciudadanos con sus respectivas plantillas biométricas dactilares, registro de actividades reportadas por los agentes, entre otros.

[ANEXO C: Modelo de Base de Datos]

FLUJO DEL PROCESO DE IDENTIFICACIÓN BIOMÉTRICA

Al utilizar el estándar internacional de minucias dactilares (ISO/IEC 19794-2), la aplicación permite trabajar con gran variedad de lectores biométricos ópticos, capacitivos. De esta manera se minimiza el problema de trabajar con diferentes lectores biométricos; se trabaja con una arquitectura distribuida la cual permite realizar el consumo de Web Services. De esta manera las transacciones se ejecutan del lado del servidor, teniendo un cliente liviano que envía parámetros y recibe resultados.

Para realizar el flujo de proceso de manera efectiva se necesita de los siguientes componentes:

- Dispositivo tecnológico.
- Lector biométrico.
- Conexión a internet.

En el dispositivo móvil se encuentra instalado y configurada la aplicación que permitirá de manera dinámica, la identificación de las personas registradas en nuestra base datos.

El lector biométrico permitirá tomar la huella dactilar y digitalizarla, permitiendo así extraer las características biométricas propias de cada individuo para su pronta identificación.

La conexión a internet permite la interacción con los servidores remotos para poder realizar el “matching” y saber de quién estamos hablando.

La figura 5 detalla el flujo de proceso de identificación desde la toma de la huella dactilar hasta la presentación de la información asociada.

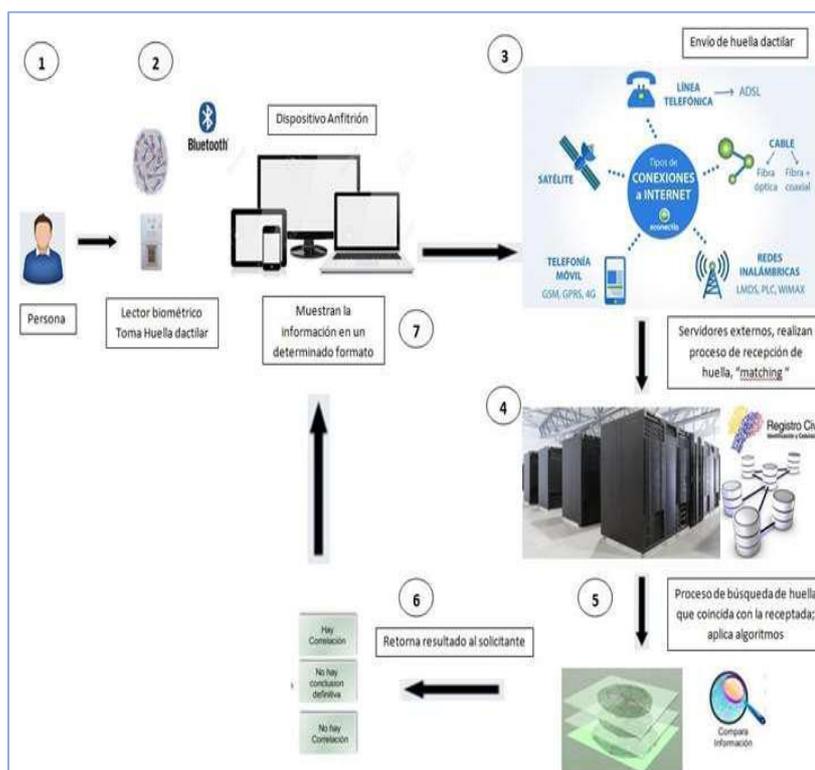


Figura 5. Flujo Proceso de Identificación Biométrica
Fuente: Autor del Proyecto

DETALLE TÉCNICO DE LA HERRAMIENTA DE DESARROLLO

NETBEANS: Desarrollo de Aplicación Cliente

Entorno Integrado de Desarrollo que utiliza la plataforma de programación JAVA. Este proyecto utiliza Java Development Kit (JDK) versión 8. Form para la identificación de personas a través de plantillas dactilares almacenadas en una base de datos.

Diseño de las Interfaces del Cliente

La Figura 6, muestra la plantilla de diseño, donde agregamos los objetos necesarios para establecer la interfaz gráfica del form que nos permitirá realizar la interacción con el usuario. Utilizamos los componentes de la librería SWING.

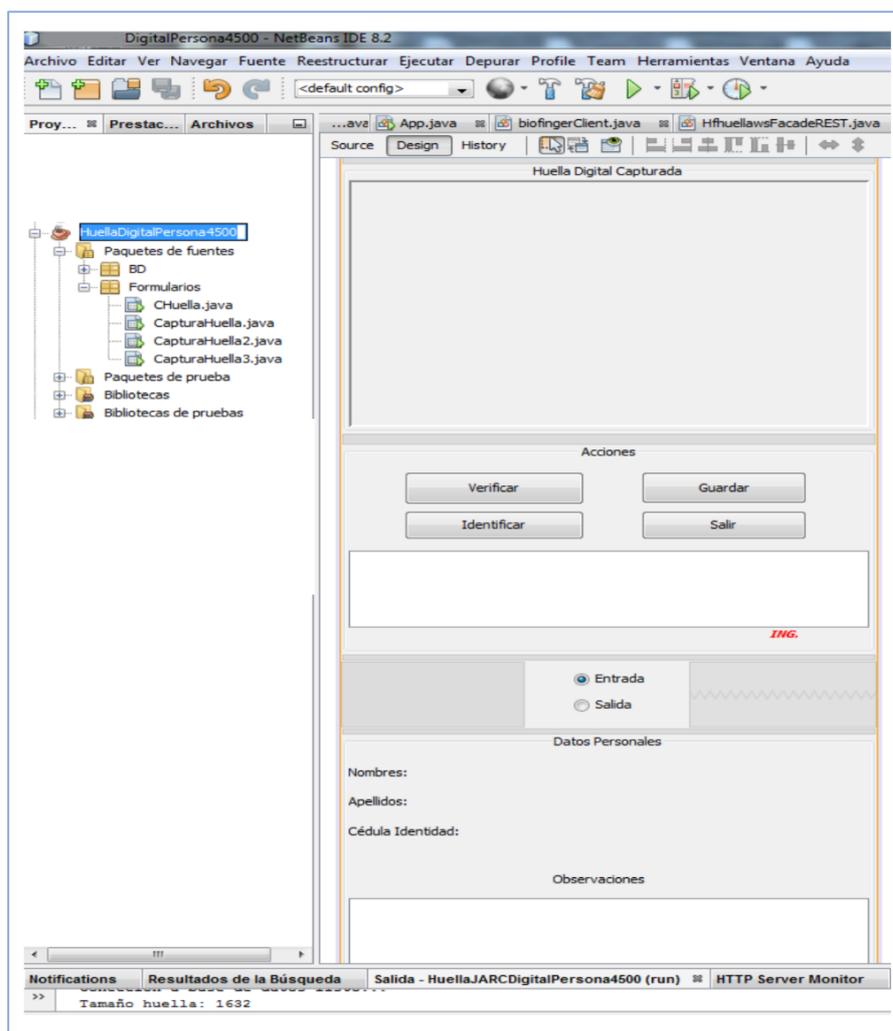


Figura 6. Plantilla Interfaz Gráfica Huella Digital

Fuente: Autor del Proyecto

Programación

En el código fuente del form añadimos las librerías y funciones necesarias para poder trabajar con el dispositivo externo. Lector Biométrico Dactilar: Tipo: Óptico, Marca: Digital Persona U. are. U 4500, Año: 2013, Firmware: SDK 1.6.1/ SDK for Android , S.O.: Windows, Linux, Android. Librerías: digital persona.jar , griuale.jar.

El lector biométrico realiza la toma de la huella dactilar y transforman estas características únicas que se extraen en imágenes analógicas a una señal digital (0 y 1), con estándares (ISO/IEC 19794-2), y de esta manera se envía la información a nuestra aplicación. Permitiendo realizar el envío de la huella digitalizada con otros datos relevantes a los servidores por medio del consumo de Web Services que residen en dichos servidores remotos para realizar los procesos de verificación de ciudadanos en nuestra base de datos, ingreso de notificaciones y poder compartir esta información en línea.

El motor de base de datos está diseñado para registrar estos eventos:

- Verificación de Ciudadano.- La tabla SOMHUE contiene las plantillas dactilares de los Ciudadanos, al recibir nuestro servidor la plantilla dactilar digitalizada realiza el proceso de matching hasta encontrar un porcentaje mayor 95% de coincidencia, una vez identificado se extrae los datos asociados a dicha plantilla dactilar por medio de la clave idciudadano el cual hace referencia a la tabla Ciudadano.
- Ingreso de Información.- La tabla registros_visitas permite registrar novedades emitidas por los servidores policiales; estas son grabadas y a la vez permiten compartir estas notificaciones en línea con los demás servidores policiales. El campo idciudadano es el que hace referencia al ciudadano en cuestión que está involucrado en dicha notificación. [ANEXO C: Modelo de Base de Datos]

La Figura 7, muestra el entorno de programación NetBeans de la captura de la huella digital que será registrado en nuestra base de datos.

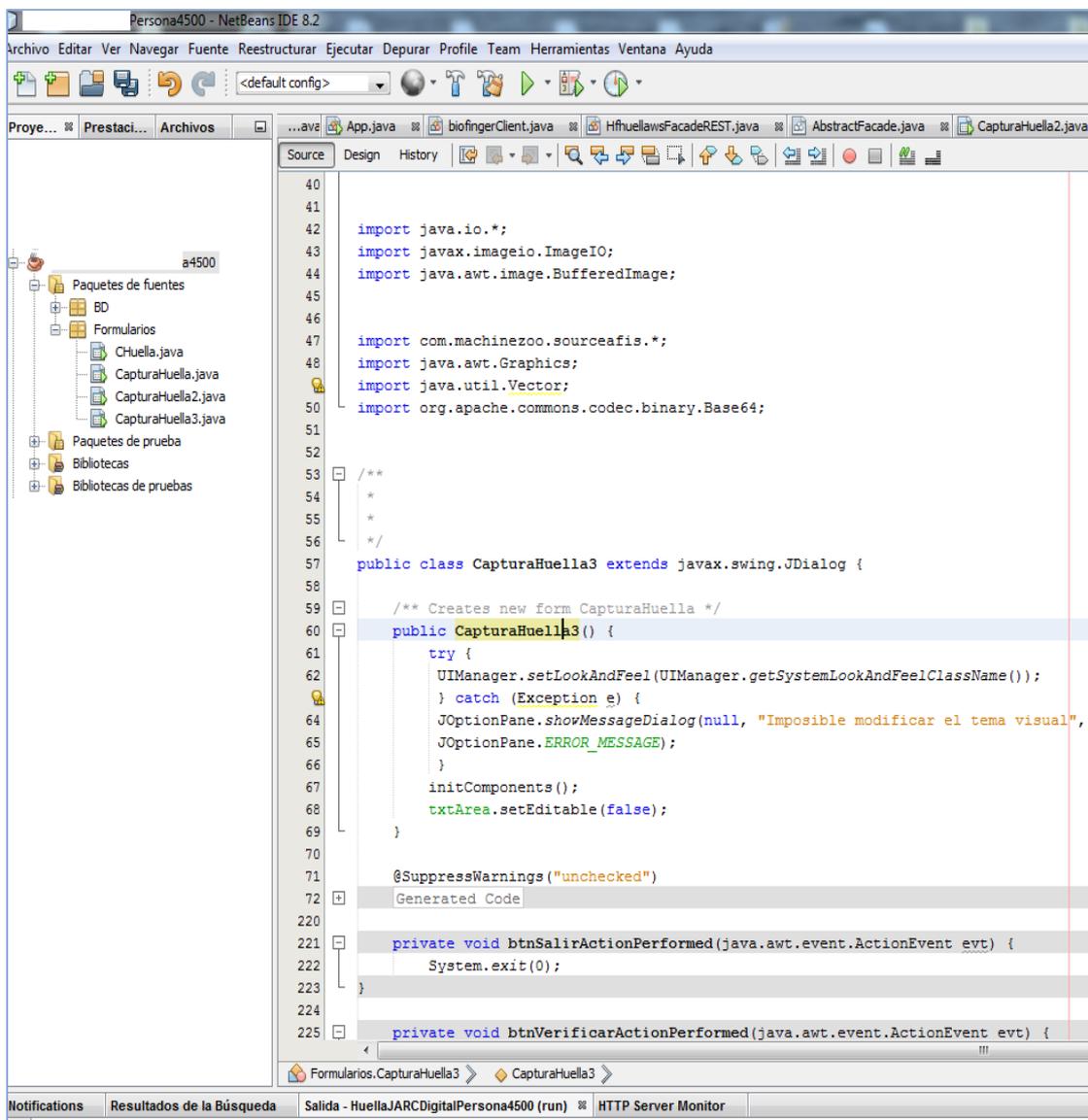


Figura 7. Programación Registro Huella Digital
Fuente: Autor del Proyecto

Ejecución de la Aplicación

Pasos para registrar e identificar.

- Form para el registro de personas y sus datos. Para efectos de prueba utilizamos una base de datos propia.

- En esta plantilla de diseño, agregamos los objetos necesarios para establecer la interfaz gráfica del form que nos permitirá realizar la interacción con el usuario.
- Utilizamos el framework Primefaces el cual utiliza el modelo Vista Controlador (MVC), esto facilita el diseño de formularios que serán útiles al momento de realizar el ingreso de información.

Nuestro proyecto posee una base de datos con información acerca de personas, por ende, este formulario solicita datos como número de cedula, nombres, apellidos, fecha de nacimiento, etc. Posterior se asignan las plantillas dactilares a cada ciudadano mediante el lector biométrico, donde se realiza el ingreso de la información que será desplegada cuando se lo requiera. En resumen, se realiza un mapeo de entidades para facilitar el uso y acceso de estas y así completar los registros necesarios para representar el uso y la eficiencia de la aplicación.

[ANEXO B]

La figura 8 muestra la interfaz gráfica de usuario para el registro de información en nuestra base de datos.

The image shows a web application interface for a citizen registry. A modal window titled "CREATE NEW CIUDADANO" is open, allowing the user to add a new record. The modal form contains the following fields:

- Cedula: 1710549989
- Nombres: Walter Oswaldo
- Apellidos: Gomez Vargas
- Fechanacimiento: 22/03/1976
- Lugaracimiento: RIOBAMBA
- Sexo: MASCULINO
- Nacionalidad: Ecuatoriana
- Estadocivil: CASADO
- Foto: Selecionar archivo photo_2019-1...08-09-14.jpg

The background interface shows a table with the following columns: Id, Cedula, Nombres, Apellidos, Fechanacimiento, Lugaracimiento, Sexo, Nacionalidad, Estadocivil, and Foto. The table contains three rows of data:

Id	Cedula	Nombres	Apellidos	Fechanacimiento	Lugaracimiento	Sexo	Nacionalidad	Estadocivil	Foto
12	0924232804					Masculino	Ecuatoriano	Casado	
23	1710549989					Masculino	Ecuatoriano	Casado	
24	0602974834					MASCULINO	Ecuatoriana	CASADO	

Figura 8. Interfaz de Usuario para el Registro de la Base de Datos
Fuente: Autor de Proyecto

La Figura 10, muestra la interfaz gráfica para el registro y asignación de la huella digital.

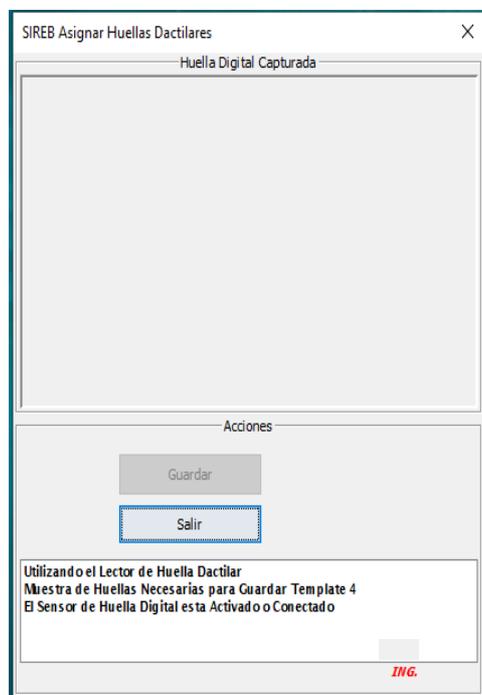


Figura 10. Interfaz Registro Huella Digital
Fuente: Autor del Proyecto

La Figura 11 y Figura 12 muestra la interfaz gráfica de la asignación de la huella a una persona específica, y la interfaz gráfica de la huella guardada respectivamente.

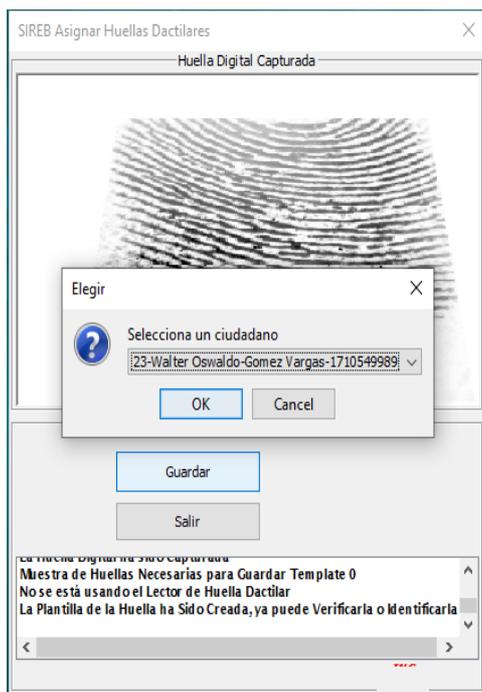


Figura 11. Interfaz Registro Huella a Persona
Fuente: Autor del Proyecto

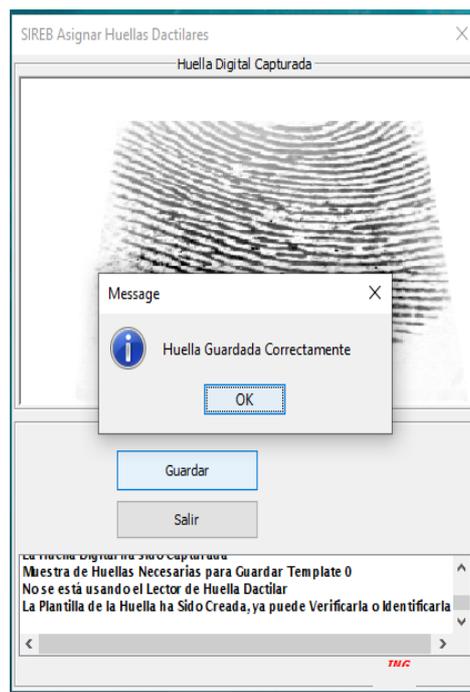


Figura 12. Interfaz Huella Guardada
Fuente: Autor del Proyecto

Utilizar el programa para identificar huellas SIREB-IDENTIFICA clic derecho en el archivo (SIREB-IDENTIFICA-PERSONA.jar), abrir con y elegir "OpenJDK Platform Binary"

- a) Poner la huella dactilar y a continuación debe mostrar la información ingresada en el formulario de datos anteriormente utilizada (paso 1)

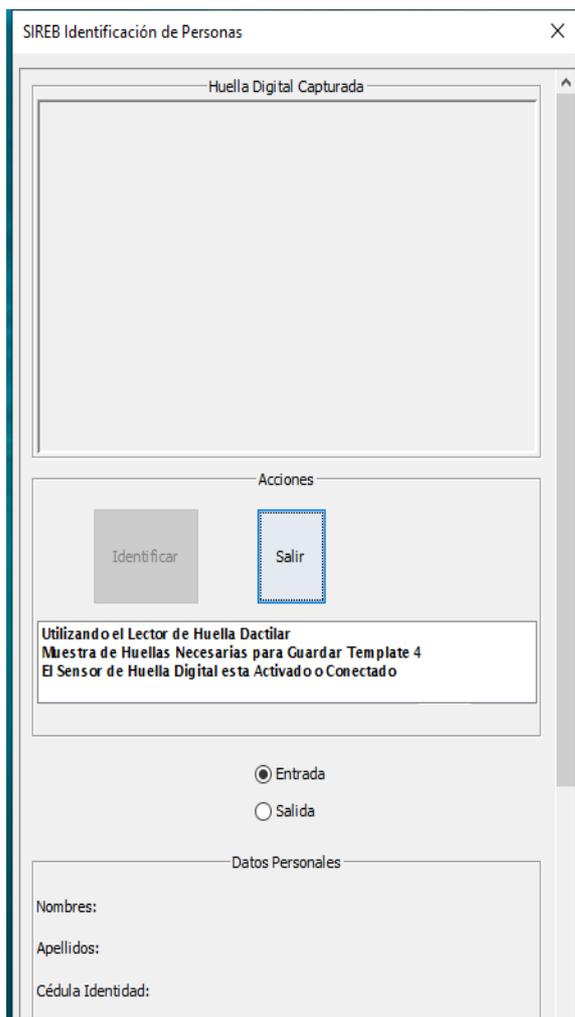


Figura 13. Interfaz Verificación e Identificación
Fuente: Autor del Proyecto

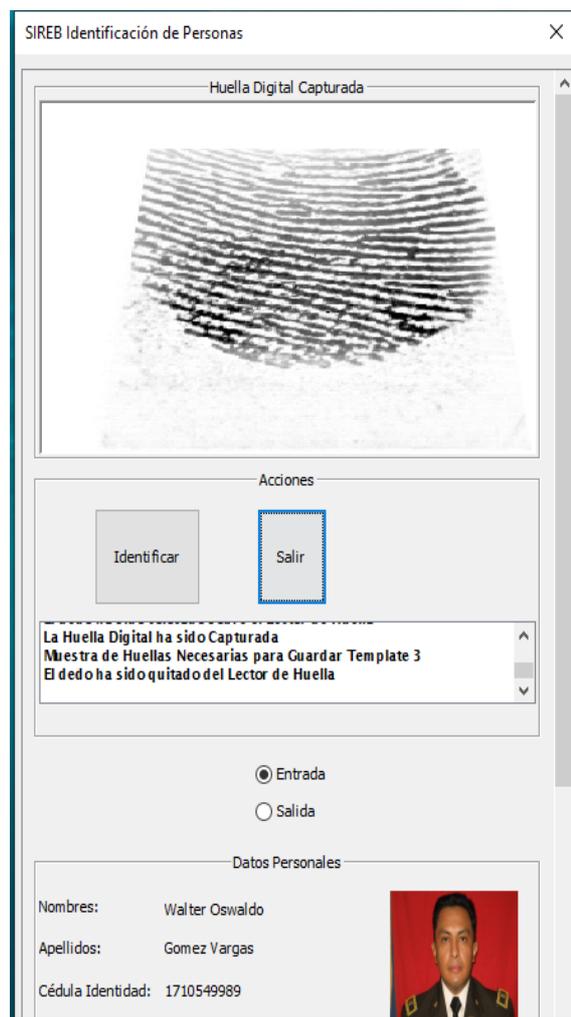


Figura 14. Interfaz Identificación
Fuente: Autor del Proyecto

CONCLUSIONES

El desarrollo de este proyecto estuvo enfocado en la reducción de los niveles de violencia y delincuencia en el Distrito Esteros, para lo cual se han optimizado las estrategias operacionales de la prevención situacional, social e investigativa, con el propósito de eliminar la oportunidad del delito con respecto a la víctima, victimario y lugar.

Los sistemas de identificación biométrica, en la actualidad han mejorado la manera de rescatar las características y minucias de la huella dactilar. Es así que el proceso de identificación de un individuo en una base de datos con plantillas dactilares existentes puede alcanzar un umbral de confiabilidad del 99.9 %, la diferencia estaría relacionada con interferencias como suciedad, heridas, asperezas o falta de dedos.

Mediante la utilización de patrones de huellas dactilares leídas en un lector biométrico de acuerdo con los rasgos físicos vinculados a los seres humanos, se puede evitar la suplantación de identidad, además de reducir los tiempos de respuesta y la optimización de los recursos humanos y tecnológicos.

Este proyecto requirió de un hardware y un software, que permitió extraer la información mediante sensores físicos las características de los patrones (huellas dactilares); para posterior ser validados, verificados y procesados en un sistema informático, que nos proveerá un resultado de manera inmediata.

Cabe señalar que se tiene pendiente la consolidación de la información que pueda ser compartida por el registro civil, que luego de las coordinaciones y alianzas estratégicas nos proveerán de la información registrada en sus bases de datos, que serán administradas con toda la información judicial que posee los registros de la Policía Nacional del Ecuador.

REFERENCIAS BIBLIOGRÁFICAS

Constituyente, A. (s.f.). Constitución de la República del Ecuador .

Delictuales, A. I. (2010). *Analisis Delictual: enfoque y metodología para la reducción del delito* .

Ecuador, P. N. (s.f.). *PLAN ESTRATEGICO 2017-2021*. Obtenido de <http://www.policiaecuador.gob.ec/plan-estrategico/>

Javier Ortega Gracia, F. A. (2008). *Bometría y Seguridad*. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Mateos, M. T. (15 de Octubre de 2005). *Técnicas biométricas aplicadas a la seguridad*. Obtenido de Grupo editorial ra-ma: https://www.ra-ma.es/libro/tecnologias-biometricas-aplicadas-a-la-seguridad_49506/

Policía Nacional, Dirección General de Operaciones. Departamento de Análisis de Información del Delito [DAID].

ANEXO A: DIAGRAMAS DE FLUJO

DIAGRAMA DE FLUJO DEL PROCESO DE LECTURA DE PLANTILLAS DACTILARES/ CONSULTA INFORMACIÓN

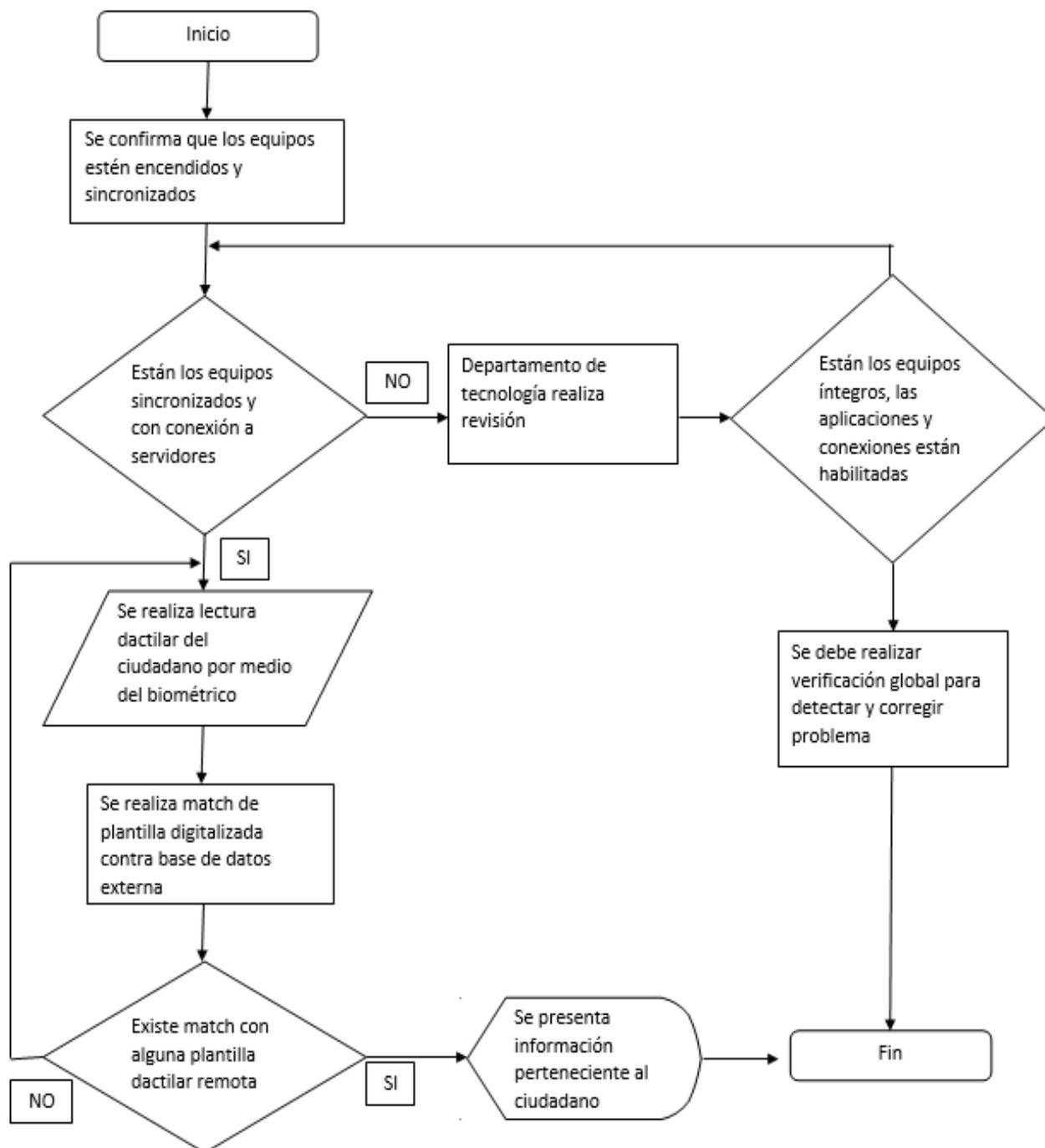
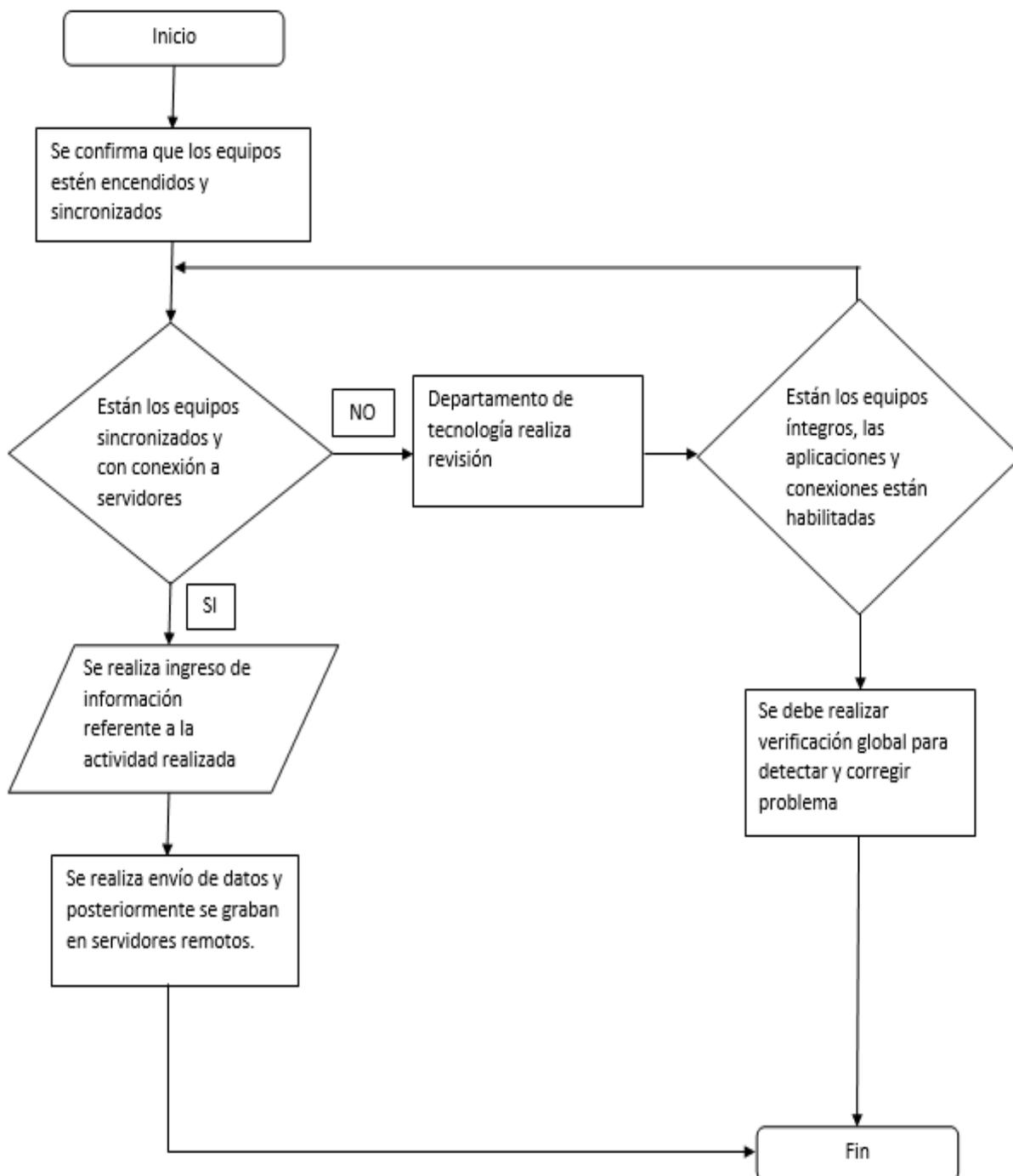


DIAGRAMA DE FLUJO DEL PROCESO DE INSERTAR INFORMACIÓN /REGISTRAR ACTIVIDADES DE CIUDADANOS.

ANEXO B: DIAGRAMA DE CLASES

CLASE CIUDADANO

Ciudadano
Integer id
String cedula
String nombres
String apellidos
Date fechanacimiento
String lugarnacimiento
String sexo
String nacionalidad
String estadocivil
Byte foto
String nomimg
String pathimg
String fullpathimg
Private void setId (integer Id)
Private integer getId ()
Private void setCedula (String cedula)
Private String getCedula()
Private void setNombres (String nombres)
Private String getNombres ()
Private void setApellidos (String apellidos)
Private String getApellidos ()
Private void setFechanacimiento (Date)
Private Date getFechanacimiento ()
Private void setLugarnacimiento String lugarnacimiento (String lugarnacimiento)
Private String getLugarnacimiento ()
Private void setSexo (String sexo)
Private String getSexo ()
Private void setNacionalidad (String nacionalidad)
Private String getNacionalidad ()
Private void setEstadocivil (String estadocivil)
Private String getEstadocivil ()
Private void setFoto (Byte foto)
Private Byte getFoto ()
Private void setNomimg (String nomimg)
Private String getNomimg ()
Private void setPathimg (String pathimg)
Private String getPathimg ()
Private void setFullpathimg (String fullpathimg)
Private String getFullpathimg ()
Private btnVerificarActionPerformed()
Private btnIdentificarActionPerformed()
Private btnGuardarActionPerformed()

CLASE SOMHUE

Somhue
String huenombre
Byte huehuella
Integer id
String huellab64
String huellaiso381
Byte huellaiso381b
Byte huehuellat
Integer idciudadano
Private void setHuenombre (String huenombre)
Private String getHuenombre ()
Private void setHuehuella (String huehuella)
Private String getHuehuella ()
Private void setId (Integer id)
Private Integer getId()
Private void setHuellab64 (String huellab64)
Private String getHuellab64 ()
Private void setHuellaiso381 (String huellaiso381)
Private String getHuellaiso381 ()
Private void setHuellaiso381b (Byte huellaiso381b)
Private Byte getHuellaiso381b ()
Private void setHuehuellat (Byte huehuellat)
Private Byte getHuehuellat ()
Private void setIdciudadano (Integer idciudadano)
Private Integer getIdciudadano ()
Private guardarHuella()
Private verificarHuella()
CrearImagenHuella()
DibujarHuella()
EstadoHuellas()

CLASE REGISTROS_VISITAS

Registros_visitas
Integer idregvisi
String cedula_visitante
String nombres_visitante
String apellidos_visitante
String observaciones
Date fecha_visita
String hora
String tipo
Integer idciudadano
Private void setIdregvisi (Integer idregvisi) Private Integer getIdregvisi ()
Private void setCedula_visitante (String cedula_visitante) Private String getCedula_visitante ()
Private void setNombres_visitante (String nombres_visitante) Private String getNombres_visitante ()
Private void setApellidos_visitante (String apellidos_visitante) Private String getApellidos_visitante ()
Private void setObservaciones (String observaciones) Private String getObservaciones ()
Private void setFecha_visita (Date fecha_visita) Private Date getFecha_visita ()
Private void setHora (String hora) Private String getHora ()
Private void setTipo (String tipo) Private String getTipo ()
Private void setIdciudadano (Integer idciudadano) Private Integer getIdciudadano ()
DPPFeatureSet extraerCaracteristicas() Private GuardarRegistro()

ANEXO C: MODELO DE BASE DE DATOS

GESTOR DEL MOTOR DE BASE DE DATOS: POSTGRESQL

1. DISEÑO DE TABLAS

Script de creación de tablas:

Tabla Ciudadano: Contiene el registro de los datos personales del ciudadano.

```
CREATE TABLE ciudadano
(
  id serial NOT NULL,
  cedula character varying (13),
  nombres character varying (50),
  apellidos character varying (50),
  fechanacimiento timestamp without time zone,
  lugarnacimiento character varying (100),
  sexo character varying(20),
  nacionalidad character varying(30),
  estadocivil character varying(30),
  foto bytea,
  nomimg character varying,
  pathimg character varying,
  fullpathimg character varying,
  CONSTRAINT pk_idreg PRIMARY KEY (id),
  CONSTRAINT unique_ced UNIQUE (cedula)
)
WITH (
  OIDS=FALSE
);
ALTER TABLE ciudadano
  OWNER TO postgres;
GRANT ALL ON TABLE ciudadano TO postgres;
GRANT ALL ON TABLE ciudadano TO public;
```

	Ciudadano
PK	id serial NOT NULL,
	cedula character varying(13),
	nombres character varying(50),
	apellidos character varying(50),
	fechanacimiento timestamp without time zone,
	lugarnacimiento character varying(100),
	sexo character varying(20),
	nacionalidad character varying(30),
	estadocivil character varying(30),
	foto bytea,
	nomimg character varying,
	pathimg character varying,
	fullpathimg character varying,

Tabla Somhue: Contiene el registro de las huellas dactilares digitalizado de cada ciudadano

```
CREATE TABLE somhue
(
  huenombre character varying(100),
  huehuella bytea,
  id serial NOT NULL,
    huellab64 character varying,
    huellaiso381 character varying,
    huellaiso381b bytea,
    huehuellat bytea,
    idciudadano integer,
  CONSTRAINT id_serial PRIMARY KEY (id)
)
WITH (
  OIDS=FALSE
);
ALTER TABLE somhue
  OWNER TO postgres;
GRANT ALL ON TABLE somhue TO postgres;
GRANT ALL ON TABLE somhue TO public;
GRANT SELECT(huehuella),UPDATE(huehuella),INSERT(huehuella),
REFERENCES(huehuella) ON somhue TO public;
```

Somhue	
	huenombre character varying(100),
	huehuella bytea,
PK	id serial NOT NULL,
	huellab64 character varying,
	huellaiso381 character varying,
	huellaiso381b bytea,
	huehuellat bytea,
	idciudadano integer,

Tabla Registros visitas: Contiene el registro de las visitas realizadas por ciudadanos

```
CREATE TABLE registros_visitas
(
  idregvisi bigserial NOT NULL,
  cedula_visitante character varying(13),
  nombres_visitante character varying(60),
  apellidos_visitante character varying(60),
  observaciones character varying,
  fecha_visita timestamp with time zone,
  hora character varying(20),
  tipo character varying(10),
```

```

idciudadano integer,
CONSTRAINT idregvisi PRIMARY KEY (idregvisi)
)
WITH (
  OIDS=FALSE
);
ALTER TABLE registros_visitas
  OWNER TO postgres;
GRANT ALL ON TABLE registros_visitas TO postgres;
GRANT ALL ON TABLE registros_visitas TO public;

```

Registros_visitas	
PK	idregvisi bigserial NOT NULL,
	cedula_visitante character varying(13),
	nombres_visitante character varying(60),
	apellidos_visitante character varying(60),
	observaciones character varying,
	fecha_visita timestamp with time zone,
	hora character varying(20),
	tipo character varying(10),
	idciudadano integer,

2. DIAGRAMA ENTIDAD RELACIÓN

