

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

**“ESQUEMA DE SEGURIDAD PARA LA APLICACIÓN
SICOP DE LA POLICÍA NACIONAL”**

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

**MAGISTER EN SEGURIDAD INFORMÁTICA
APLICADA**

JOSUÉ JEFFERSON GUARTATANGA ROBAYO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

A Dios, que nos ha conservado con vida y salud.

A mis padres, José e Hilda, quienes me ofrecen su apoyo incondicional.

A Roberto Varela y John Wells por el privilegio de trabajar con ellos.

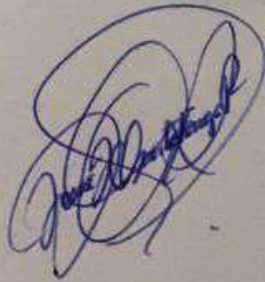
A nuestros profesores, por todos los conocimientos y consejos transmitidos.

DEDICATORIA

A mis padres, quienes son un pilar fundamental en mi vida.

A mi novia, por el ánimo y cariño que me brinda siempre.

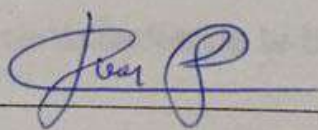
A mis familiares y amigos

A handwritten signature in blue ink, consisting of several overlapping loops and curves, located at the bottom left of the page.

TRIBUNAL DE SUSTENTACIÓN



MGS. LENIN FREIRE
DIRECTOR DEL MSIA



MGS. JUAN C. GARCÍA
PROFESOR DELEGADO POR LA
SUBDECANA DE LA FIEC

RESUMEN

El propósito de este proyecto es implementar un esquema de seguridad para la aplicación piloto SICOP de la Policía Nacional que permita la privacidad e integridad de los datos mediante procesos de encriptación y sincronización, la gestión de auditoría del manejo de la aplicación y la seguridad en contra de daños a la aplicación y al Sistema Operativo.

Con esta propuesta la Policía Nacional podrá tener:

- Privacidad a la información sensible de los datos.
- Consistencia en los datos consultados de la base local, ubicada en la patrulla.
- Seguridad contra daños al Sistema Operativo y al Software.
- Mejora la productividad en el trabajo del personal de la Policía.

ÍNDICE GENERAL

AGRADECIMIENTO	ii
DEDICATORIA	iii
TRIBUNAL DE SUSTENTACIÓN.....	iv
RESUMEN.....	v
ÍNDICE GENERAL.....	vi
ÍNDICE DE FIGURAS	viii
INTRODUCCIÓN.....	xii
GENERALIDADES.....	1
1.1. Descripción del problema.....	1
1.2. Solución propuesta.	7
METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN.....	8
2.1. Implementación del proceso de encriptación para datos relevantes de la Base Patrulla.	8
2.2. Implementación del proceso de sincronización de datos para ciertas tablas de la Base Patrulla.	16
2.3. Implementación para reportes de auditoría en Servidor Intermedio.	32
2.4. Implementación de seguridad en: El Sistema Operativo por restricción de funcionalidades; El Código fuente de SICOP.....	46
ANÁLISIS DE RESULTADOS.....	49

3.1. Confidencialidad de los datos en la Base Patrulla.....	49
3.2. Integridad y disponibilidad de los datos mediante procesos de sincronización Base Intermedia – Base Patrulla y Base Patrulla – Base Intermedia.	52
3.3. Integridad del Sistema Operativo y Confidencialidad del código fuente de SICOP.	56
CONCLUSIONES Y RECOMENDACIONES.....	58
BIBLIOGRAFÍA.....	60
GLOSARIO.....	61

ÍNDICE DE FIGURAS

Figura 1.1: Diagrama de funcionamiento SICOP.	3
Figura 1.2: Sincronización Base15 – Base Intermedia y Ausencia de sincronización Base Intermedia – Base Patrulla.....	4
Figura 2.1: Porción de código del Script que encripta los datos de la tabla de personas.....	9
Figura 2.2: Porción de código del Script que encripta los datos de la tabla de vehículos	9
Figura 2.3: Tabla de registros de queries para la consulta manual	10
Figura 2.4: Consulta de personas mediante la cédula de identidad	10
Figura 2.5: Consulta del dueño del vehículo mediante el identificador de la persona	10
Figura 2.6: Consulta del vehículo mediante el número de placa	11
Figura 2.7: Consulta del vehículo mediante el número de motor.....	11
Figura 2.8: Consulta del vehículo mediante el número de chasis.....	11
Figura 2.9: Diseño del servicio web para la consulta genérica	12
Figura 2.10: Búsqueda parametrizada del query solicitado a ejecutar	13
Figura 2.11: Consulta completada mediante el parámetro de búsqueda “llave”	14
Figura 2.12: Ejecución de la consulta completa almacenada en la variable “query”	14
Figura 2.13: Porción de código del Script que encripta los datos de la tabla de usuarios.....	15
Figura 2.14: Diseño del servicio web para la autenticación en SICOP utilizando algoritmo de encriptación sha1	15

Figura 2.15: Porción de código del servicio web para la autenticación en SICOP utilizando algoritmo de encriptación sha1	16
Figura 2.16: Interacción entre Base Intermedia y Base Patrulla mediante el proceso de sincronización	17
Figura 2.17: Flujo del proceso de sincronización para las tablas: personas y vehículos.	18
Figura 2.18: Flujo del proceso de sincronización para las tablas: movimientos migratorios, detenciones, órdenes de captura e impedimentos de salida.	19
Figura 2.19: Diseño general de los servicios web para el proceso de sincronización	20
Figura 2.20: Consulta de las fechas máximas en las tablas: personas y vehículos.	21
Figura 2.21: Consulta de los nuevos registros de la vista de personas de la Base Intermedia.....	22
Figura 2.22: Consulta de los nuevos registros de la vista de vehículos de la Base Intermedia.....	23
Figura 2.23: Consulta de los nuevos registros de la vista de movimientos migratorios de la Base Intermedia.....	24
Figura 2.24: Consulta de los nuevos registros de la vista de detenciones de la Base Intermedia.....	25
Figura 2.25: Consulta de los nuevos registros de la vista de órdenes de captura de la Base Intermedia.....	26
Figura 2.26: Consulta de los nuevos registros de la vista de impedimentos de salida de la Base Intermedia.....	27

Figura 2.27: Actualización de la tabla personas de la Base Patrulla con datos encriptados	28
Figura 2.28: Actualización de la tabla vehículos de la Base Patrulla con datos encriptados	29
Figura 2.29: Actualización de las tablas: movimientos migratorios, detenciones, órdenes de captura e impedimentos de salida de la Base Patrulla	30
Figura 2.30: Actualización de la tabla de usuarios de la Base Patrulla.....	30
Figura 2.31: Consulta de los registros modificados de la tabla de usuarios de la Base Patrulla	31
Figura 2.32: Actualización de los registros de la tabla de usuarios de la Base Intermedia.....	32
Figura 2.33: Diseño final de los servicios web del proceso de sincronización para registrar datos de auditoría	34
Figura 2.34: Datos de salida del elemento que escucha las métricas de flujo (tFlowMeterCatcher)	35
Figura 2.35: Datos de entrada del elemento que guarda los registros de sincronización para auditoría (tMysqlOutput)	36
Figura 2.36: Diseño final del servicios web para la consulta genérica.....	38
Figura 2.37: Datos de entrada del elemento que guarda los registros de consulta para auditoría (tMysqlOutput)	39
Figura 2.38: Diseño del servicio web del envío de registros para auditoría de las consultas manuales	40
Figura 2.39: Búsqueda de registros sobre las consultas manuales para auditoría..	41
Figura 2.40: Envío de los registros de auditoría al Servidor Intermedio	41

Figura 2.41: Actualización de los registros que ya han sido enviados al Servidor Intermedio mediante los datos de entrada id_tran y uid	42
Figura 2.42: Porción de código C#.Net del registro de hit de captura con la cámara ALPR de un vehículo robado a la base patrulla	43
Figura 2.43: Porción de código del Nodo Cliente ALPR para envío del registro de hit de captura con la cámara ALPR al Servidor Intermedio	44
Figura 2.44: Porción de código del Nodo Servidor ALPR para recibir los registros de hit de captura con la cámara ALPR e insertarlos a la Base Intermedia	45
Figura 2.45: Retraso de inicialización de SICOP (Start Delay =30 sec)	47
Figura 2.46: Bloqueo del Sistema a nivel local y de la máquina	48
Figura 3.1: Información ilegible de las tablas personas y vehículos.	50
Figura 3.2: Información legible de las tablas personas y vehículos en SICOP.	51
Figura 3.3: Registro con restricción robado que está en la base intermedia y no en la base patrulla	52
Figura 3.4: Registro de vehículo sin restricción de robado en SICOP por desactualización de la base patrulla	53
Figura 3.5: Registro de vehículo con restricción de robado en SICOP después de la sincronización	54
Figura 3.6: Registros de auditoría de sincronización Base Patrulla – Base Intermedia	55
Figura 3.7: Registros de auditoría de capturas hits en el servidor intermedio	55
Figura 3.8: Porción de código SICOP ofuscado con Javascript Obfuscator v4.4	57

INTRODUCCIÓN

Todo sistema de información que maneja datos sensibles debe proveer confianza al cliente en el manejo de los datos; si estos están distribuidos, debe haber consistencia para no generar confusión en el momento de tomar decisiones.

En la fase inicial del desarrollo del sistema piloto, SICOP, se pretendía que la aplicación realizara consultas remotas de vehículos. Estas tardaban mucho tiempo y no compensaba con las consultas automáticas realizadas a través de una cámara de lector de placas ALPR. Las consultas locales mejoraron el tiempo de respuesta. Se requiere entonces mantener la consistencia de los datos entre la base remota (Base-Intermedia, que es la fuente de datos) y la base local (Base-Patrulla) mediante la implementación de un proceso de sincronización.

La Base-Patrulla tiene todos sus datos en texto plano, por esta razón se decidió encriptar solo datos que se consideren privados. De esta manera el proceso de sincronización queda comprometido a manejar algoritmos de encriptación.

Por experiencia puedo decir que cualquier herramienta tecnológica, para uso exclusivo de trabajo, será objeto de estudio por los ciertos usuarios finales con la intención de sacarle provecho y utilizarlo para propósitos personales. Algunos de estos usuarios tendrán éxito modificando la herramienta y le darán un mal uso generando tiempos de ocio. Por esto es necesario el monitoreo de las actividades para “seguirles la pista” y evaluarlos, es decir hacer auditoría.

Otros terminarán dañándola. Y para reducir el riesgo de los daños que pueden ocasionar los malos usuarios se decidió utilizar una herramienta que restrinja las funcionalidades del Sistema Operativo en donde se ejecuta SICOP y otra para ocultar el código fuente.

CAPÍTULO 1

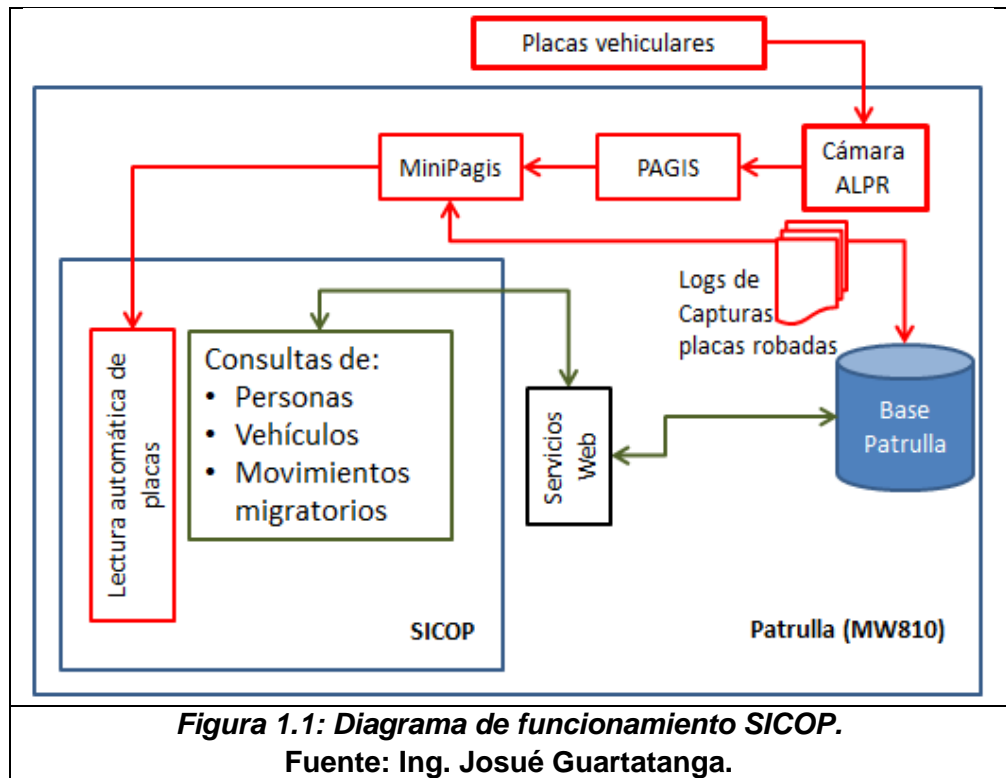
GENERALIDADES.

1.1. Descripción del problema

El Gobierno Nacional del Ecuador, la Policía Nacional, y CNT han solicitado un Sistema Inteligente de Consultas Policiales llamado SICOP instalado sobre una plataforma de equipos de cómputo de última tecnología, "Motorola", con el cual se van a equipar patrullas a nivel nacional. Con este sistema los uniformados va a poder realizar diversas actividades de control utilizando diferentes criterios para: Consultas de Personas; Consultas de vehículos y Consultas de Movimientos Migratorios. El SICOP nos va permitir realizar las siguientes actividades:

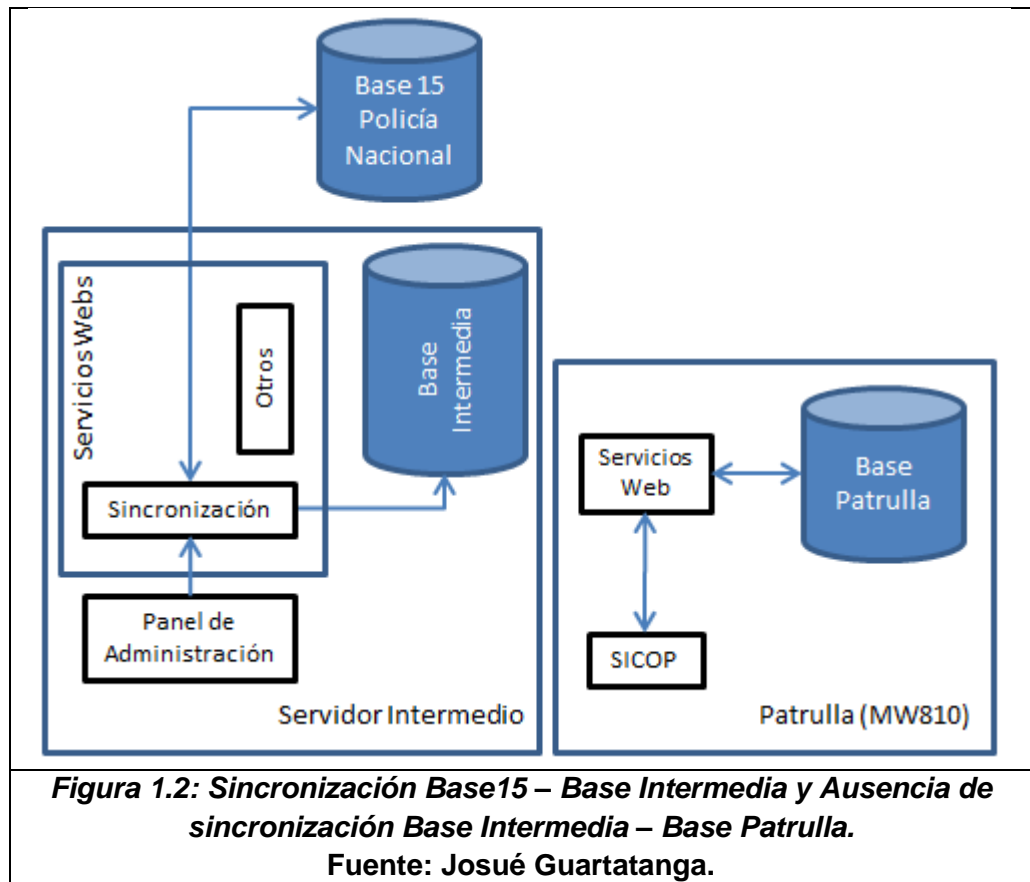
- Consultas de Personas por: número de cédula; licencia; pasaporte; nombre y apellidos para ecuatorianos y extranjeros que hayan ingresado legalmente al país.
- Consultas de Vehículos por número de: placa, motor o chasis.
- Consultas de Movimientos Migratorios por su número de cédula o pasaporte para ecuatorianos y extranjeros que hayan ingresado legalmente al país.
- Por cada dato consultado se realiza un proceso de verificación de antecedentes, órdenes de captura o restricciones de cualquier índole para así proceder de la mejor manera de acuerdo a las situaciones que se puedan presentar.
- Así mismo las patrullas cuentan con una cámara externa que de forma automática verifica todas las placas de los vehículos. En el caso de que la cámara detecte la placa de un vehículo reportado como robado el sistema emite una alerta sonora para que el Policía pueda tomar las acciones apropiadas de acuerdo a la situación.

El siguiente gráfico muestra el diagrama del funcionamiento de SICOP (Ver Figura 1.1)



La base de datos (Base Patrulla) que utiliza SICOP para desplegar las consultas tiene registros filtrados provenientes de la base de datos de la Policía Nacional (Base 15). El filtro se encuentra en el Servicio Web del Servidor Intermedio que se utiliza para la sincronización de la Base 15 a la Base Intermedia. (Ver Figura 1.2)

No existe sincronización desde la Base Intermedia hacia la Base Patrulla. Los registros que hay en la Base Patrulla fueron insertados a través de un script que se obtuvo de la Base Intermedia.



Dado el funcionamiento de SICOP y de la Sincronización de la Base Intermedia, a continuación se detallan los problemas potenciales que se encontraron en:

- LA PRIVACIDAD DE LOS DATOS.

La Base Patrulla, tiene información privada sin encriptar.

Se consideró como información privada los siguientes datos:

- ✓ La cédula de identidad, nombres y apellidos del ciudadano; la placa, motor, chasis y las restricciones del vehículo.
- ✓ El usuario y la clave de acceso de los Policías al SICOP.

Aunque la Policía nacional estableció políticas para el relevo de las patrullas con el fin de proteger los datos, estos no están exentos de delincuentes informáticos que desean obtener información y acceso al sistema que les permita realizar algún acto que perjudique o exponga al ciudadano comprometiéndolo a riesgo o abusos para sacar provecho.

Si existiera la sincronización Base Patrulla – Base Intermedia y viceversa; con tan solo insertar o modificar directamente los registros de usuario y clave de acceso a SICOP, se puede tener acceso al sistema desde cualquier patrulla.

- LA INTEGRIDAD DE LOS DATOS.

La Base Patrulla quedará desactualizada cuando registros actualizados o nuevos ingresen a la Base Intermedia; ya que no existe proceso de sincronización Base Intermedia – Base Patrulla.

El ciudadano podría salir perjudicado cuando lo detienen para investigación o a su vez el personal de la Policía podría ser demandado por detenciones no debidas.

La seguridad ciudadana saldría perjudicada si el personal de la Policía no detiene a quien debe.

La Base Intermedia quedará desactualizada cuando nuevos registros de lecturas de placas robadas, capturadas por SICOP, ingresen a la Base Patrulla; ya que no existe proceso de sincronización Base Patrulla –

Base Intermedia. El análisis de estos datos es de mucha importancia para el proceso de recuperación de vehículos.

Si existiera la sincronización Base Patrulla – Base Intermedia; con tan solo modificar directamente los registros de lecturas de placas robadas en la Base Patrulla, se puede contaminar los registros del servidor intermedio generando resultados erróneos para el proceso de recuperación de vehículos.

- LA GESTIÓN DE AUDITORÍA PARA LOS USUARIOS DE SICOP.

SICOP no genera bitácoras de los eventos que realizó el policía para su posterior auditoría. Actualmente, cualquier sistema informático, debe mantener un registro de actividades de los usuarios. Sin éstos no se podrá evaluar la eficacia y eficiencia del policía en sus labores. Dichas evaluaciones son necesarias para la toma de decisiones en la gestión del personal policial.

- LA SEGURIDAD EN CONTRA DE DAÑOS HACIA SICOP.

Al estar todas las funcionalidades del Sistema Operativo disponibles para el usuario (personal policial), el Software podría ser:

- ✓ Relegado a segundo plano por otras aplicaciones que generan tiempos de ocio.
- ✓ Manipulado con mala intención dejándolo con errores e incluso inoperable.

- ✓ Afectado por programas externos (virus) que se cargan con dispositivos de almacenamiento externos.

1.2. Solución propuesta.

- Implementar un proceso para encriptar los datos relevantes de la Base Patrulla. Este proceso se lo realizará una sola vez.
- Implementar el proceso de sincronización Base Intermedia – Base Patrulla utilizando 2 algoritmos de encriptación:
 - ✓ Un algoritmo para procesar la información privada de los ciudadanos con el que podamos encriptar y desencriptar.
 - ✓ Un algoritmo para procesar la información privada del Policía con el que se autentica con SICOP con el que podamos solo encriptar.
- Implementar un proceso de registros eventos del manejo de SICOP para la gestión de auditoría.
- Ejecutar SICOP de manera exclusiva y personalizada; y restringir ciertas funcionalidades del Sistema Operativo que no afecten el funcionamiento de SICOP.

BENEFICIO DE LA SOLUCIÓN:

- Privacidad a la información sensible.
- Consistencia en los datos consultados de la base local, ubicada en la patrulla con respecto a la base intermedia.
- Seguridad contra daños al Sistema Operativo y al Software.
- Mejora la productividad en el trabajo del personal de la Policía.

CAPÍTULO 2

METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN

2.1. Implementación del proceso de encriptación para datos relevantes de la Base Patrulla.

Para la tabla de personas se implementó un script que utiliza el algoritmo de cifrado simétrico AES [1]. (Ver Figura 2.1)

```

update [redacted] set
  documento= aes_encrypt(documento, [redacted]),
  nombre1=   aes_encrypt(nombre1 , [redacted]),
  nombre2=   aes_encrypt(nombre2 , [redacted]),
  apellido1= aes_encrypt(apellido1, [redacted]),
  apellido2= aes_encrypt(apellido2, [redacted])

```

Figura 2.1: Porción de código del Script que encripta los datos de la tabla de personas

Fuente: Josué Guartatanga.

Para la tabla de vehículos se implementó un script que utiliza el algoritmo de cifrado simétrico AES [1]. (Ver Figura 2.2)

```

update [redacted] set
  placa= aes_encrypt(placa , [redacted]),
  motor= aes_encrypt(motor , [redacted]),
  chasis= aes_encrypt(chasis , [redacted]),
  restric= aes_encrypt(restric, [redacted])

```

Figura 2.2: Porción de código del Script que encripta los datos de la tabla de vehículos

Fuente: Josué Guartatanga.

Además se desarrolló el proceso que desencripta para la correcta presentación de los datos en SICOP.

Se creó un servicio web de consulta genérica que utiliza una tabla (Ver Figura 2.3) donde se guardan las consultas utilizadas en SICOP. Dependiendo del identificador enviado al servicio web, se realizará entonces la consulta deseada.

id_seleccion	nombre	etiquetacampo	tabla	query
7	consulta nombre	Tipo,Document...		select tipo,aes_decrypt(...
8	consulta nombre para vehiculo	Cdg,Tipo,Estad...		select tipo,aes_decrypt(...
20	consulta de vehiculos (placa)	Cdg,Placa,Mod...		select cdg,aes_decrypt(...
21	consulta de Vehiculo (motor)	Cdg,Placa,Mod...		select cdg,aes_decrypt(...
22	consulta de vehiculos (chasis)	Cdg,Placa,Mod...		select cdg,aes_decrypt(...



Parámetro del servicio web de consulta genérica
Consultas disponibles

Figura 2.3: Tabla de registros de qryes para la consulta manual
Fuente: Josué Guartatanga.

La consulta con el identificador 7 es la siguiente (Ver Figura 2.4)

```

select  tipo,aes_decrypt(documento,[redacted]),
        cdg,aes_decrypt(nombre1,[redacted]),
        aes_decrypt(nombre2,[redacted]),
        aes_decrypt(apellido1,[redacted]),
        aes_decrypt(apellido2,[redacted]),
        estadociv,paiscb1,fechanac,sexo
from    [redacted] where documento=aes_encrypt(

```

Figura 2.4: Consulta de personas mediante la cédula de identidad
Fuente: Josué Guartatanga.

La consulta con el identificador 8 es la siguiente (Ver Figura 2.5)

```

select  tipo,aes_decrypt(documento,[redacted]),
        fechaexp,fechacad,cdg,
        aes_decrypt(nombre1,[redacted]),
        aes_decrypt(nombre2,[redacted]),
        aes_decrypt(apellido1,[redacted]),
        aes_decrypt(apellido2,[redacted]),
        estadociv,paiscb1,fechanac,sexo
from    [redacted] where cdg=

```

Figura 2.5: Consulta del dueño del vehículo mediante el identificador de la persona
Fuente: Josué Guartatanga.

La consulta con el identificador 20 es la siguiente (Ver Figura 2.6)

```

select  cdg, aes_decrypt(placa, [redacted]),
        modelo, marca, aes_decrypt(motor, [redacted]),
        aes_decrypt(chasis, [redacted]), clasevehi,
        tipovehi, color1, persona,
        aes_decrypt(restric, [redacted]), activado
from    [redacted] where placa=aes_encrypt(

```

Figura 2.6: Consulta del vehículo mediante el número de placa
Fuente: Josué Guartatanga.

La consulta con el identificador 21 es la siguiente (Ver Figura 2.7)

```

select  cdg, aes_decrypt(placa, [redacted]),
        modelo, marca, aes_decrypt(motor, [redacted]),
        aes_decrypt(chasis, [redacted]), clasevehi,
        tipovehi, color1, persona,
        aes_decrypt(restric, [redacted]), activado
from    [redacted] where motor=aes_encrypt(

```

Figura 2.7: Consulta del vehículo mediante el número de motor
Fuente: Josué Guartatanga.

La consulta con el identificador 22 es la siguiente (Ver Figura 2.8)

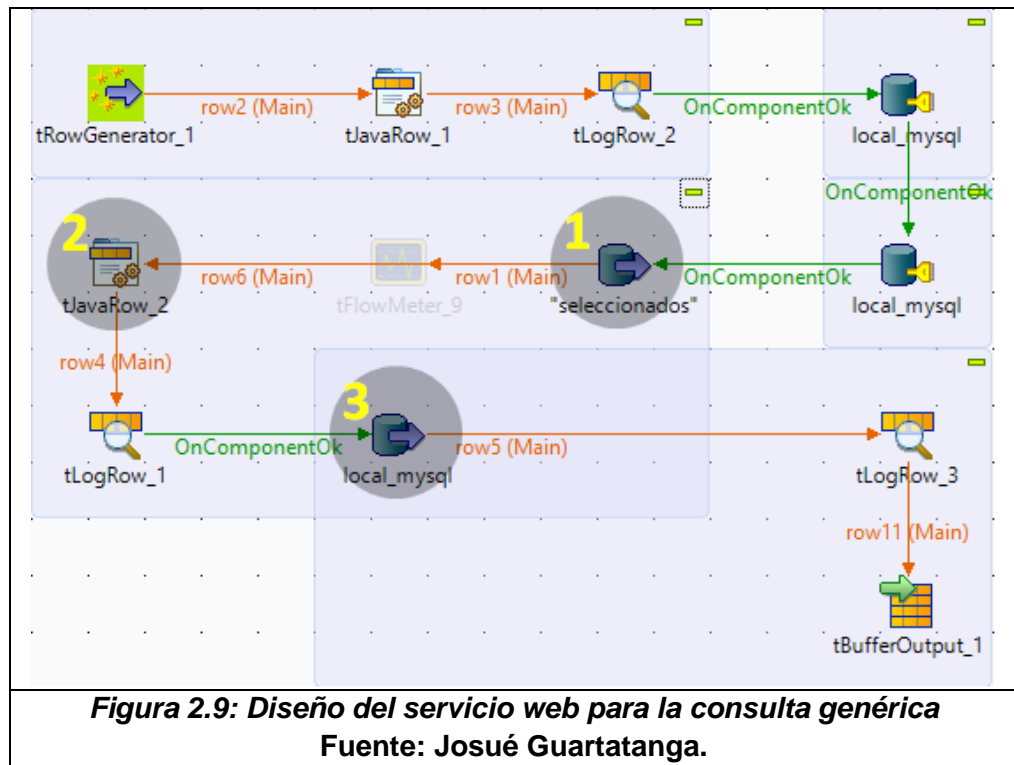
```

select  cdg, aes_decrypt(placa, [redacted]),
        modelo, marca, aes_decrypt(motor, [redacted]),
        aes_decrypt(chasis, [redacted]), clasevehi,
        tipovehi, color1, persona,
        aes_decrypt(restric, [redacted]), activado
from    [redacted] where chasis=aes_encrypt(

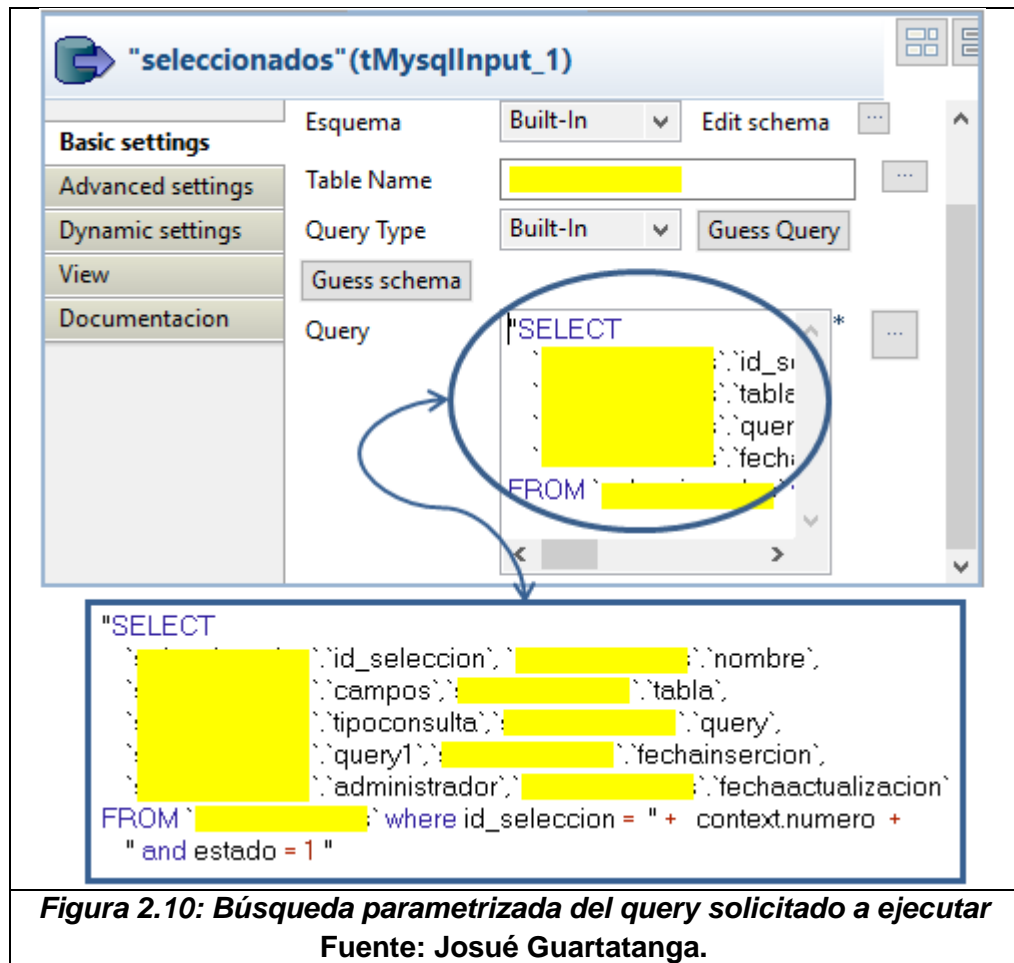
```

Figura 2.8: Consulta del vehículo mediante el número de chasis
Fuente: Josué Guartatanga.

El diseño del servicio web de la consulta genérica es el siguiente (Ver Figura 2.9). Se lo realizó con ayuda de la herramienta Talend Open Studio – Data Integration [2].



En el elemento marcado con 1 se realiza la consulta, según el parámetro de entrada, en la tabla donde están los queries de las consultas (Ver Figura 2.10).



En el elemento marcado con 2 se arma el query añadiendo el parámetro de búsqueda solicitado en SICOP (Ver Figura 2.11).

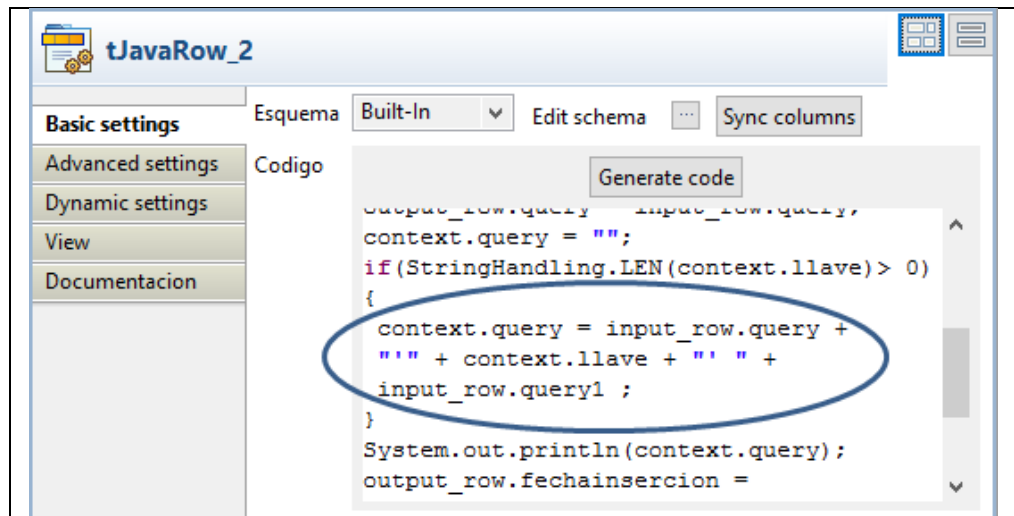


Figura 2.11: Consulta completada mediante el parámetro de búsqueda "llave"

Fuente: Josué Guartatanga.

En el elemento marcado con 3 se ejecuta el query que se obtuvo de 1 y 2 para obtener el registro deseado desde SICOP (Ver Figura 2.12).

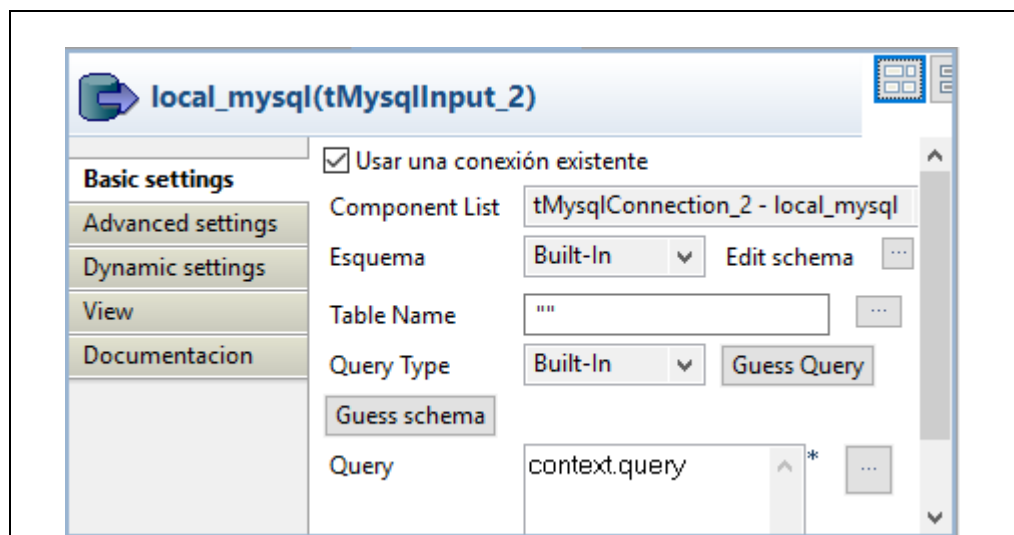
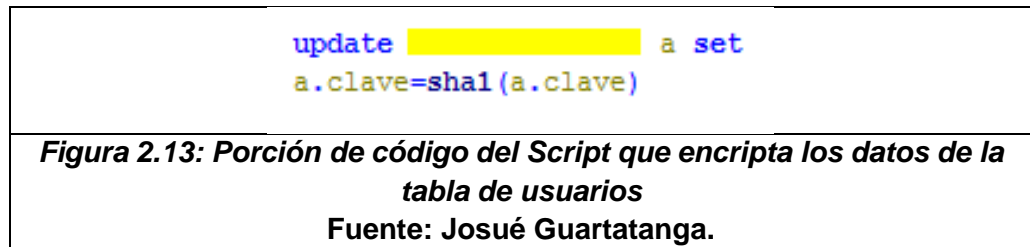


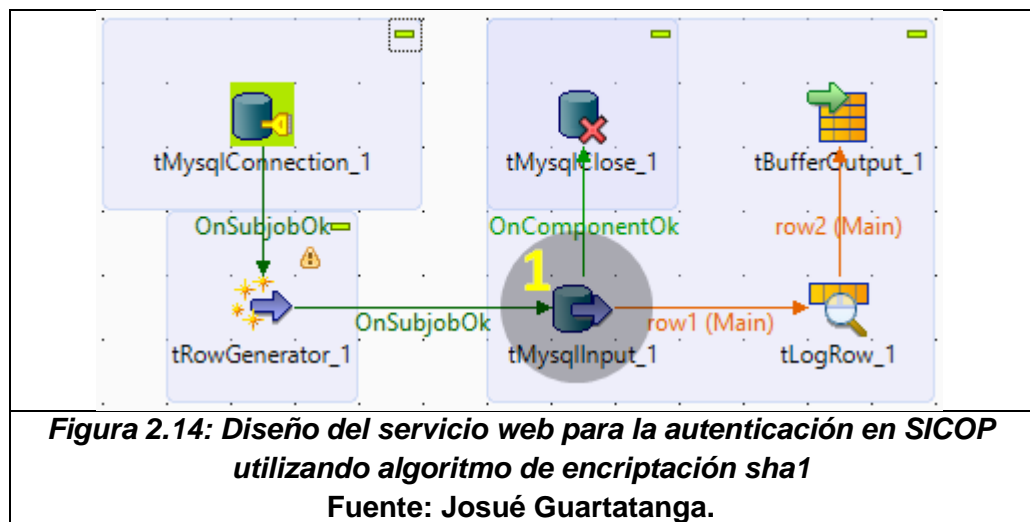
Figura 2.12: Ejecución de la consulta completa almacenada en la variable "query"

Fuente: Josué Guartatanga.

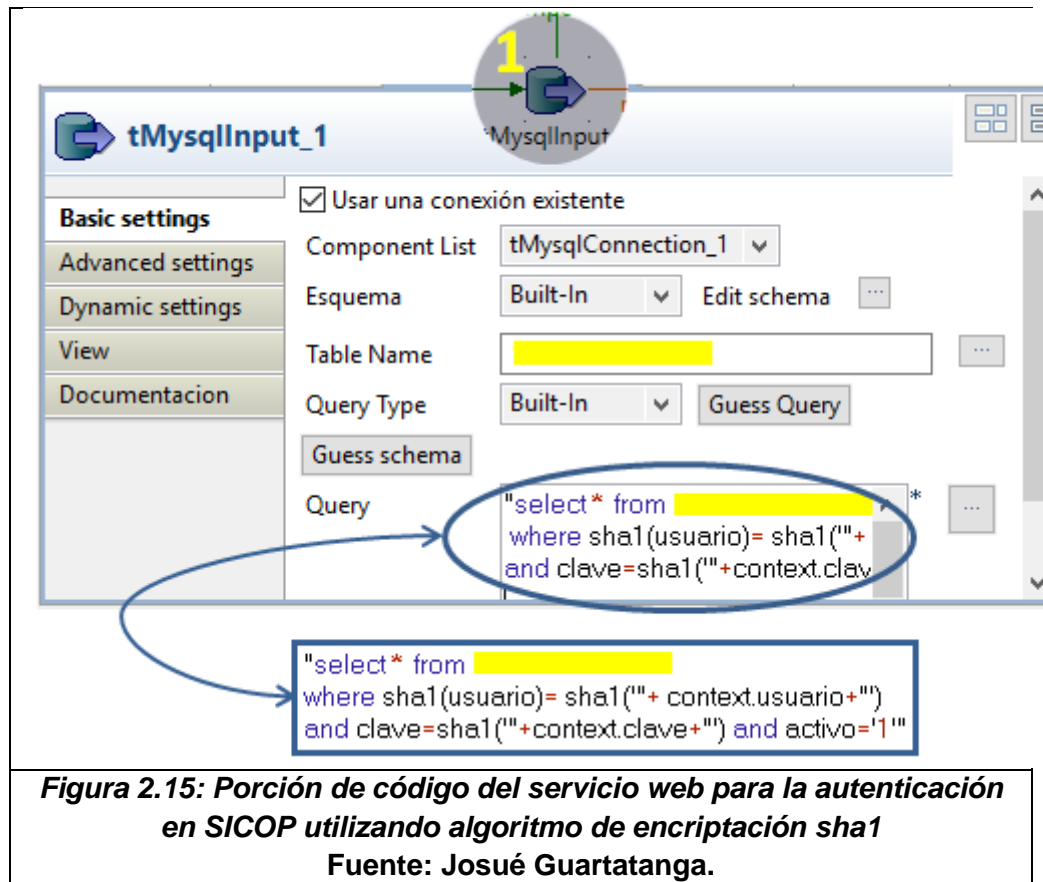
Para la tabla de usuarios se implementó un script que utiliza el algoritmo de cifrado asimétrico SHA [3]. (Ver Figura 2.13)



Además se desarrolló el proceso que permite la autenticación en SICOP. (Ver Figura 2.14)

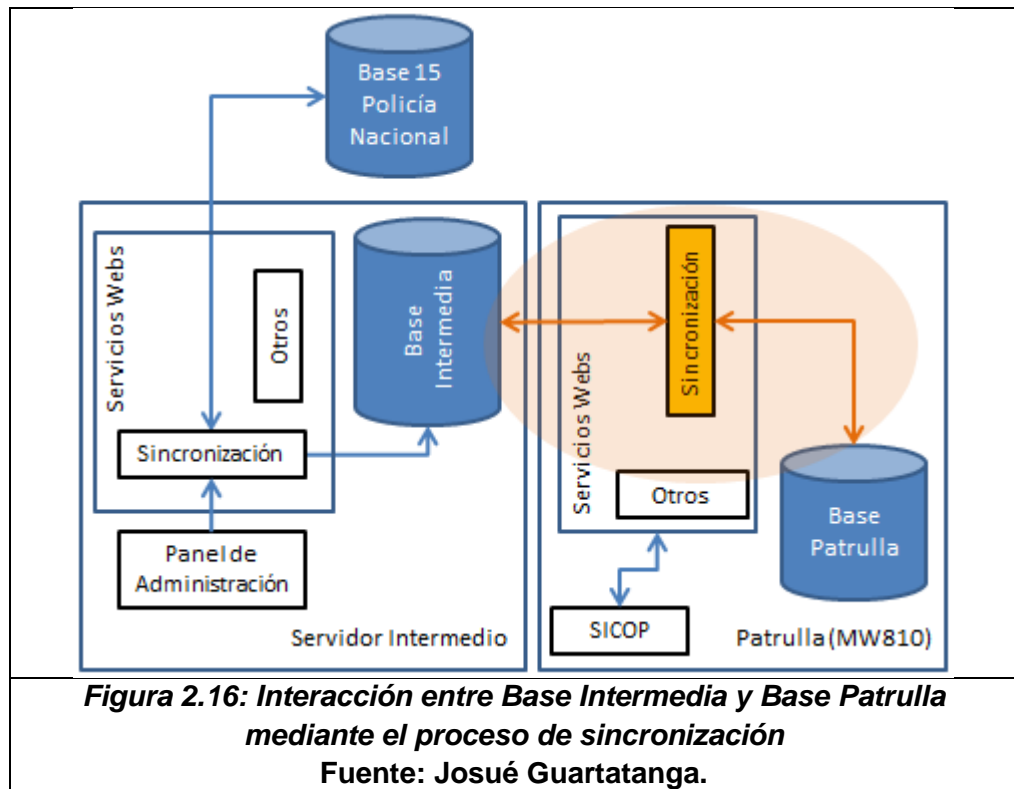


En el elemento marcado con 1 se recibe como parámetro de entrada el usuario y la clave ingresada por el agente policial. De la clave que se obtiene un hash, utilizando sha1, y la compara con los hashes que están en la tabla de usuarios. Si existe el usuario con el respectivo hash de la clave, permite el ingreso. (Ver Figura 2.15).



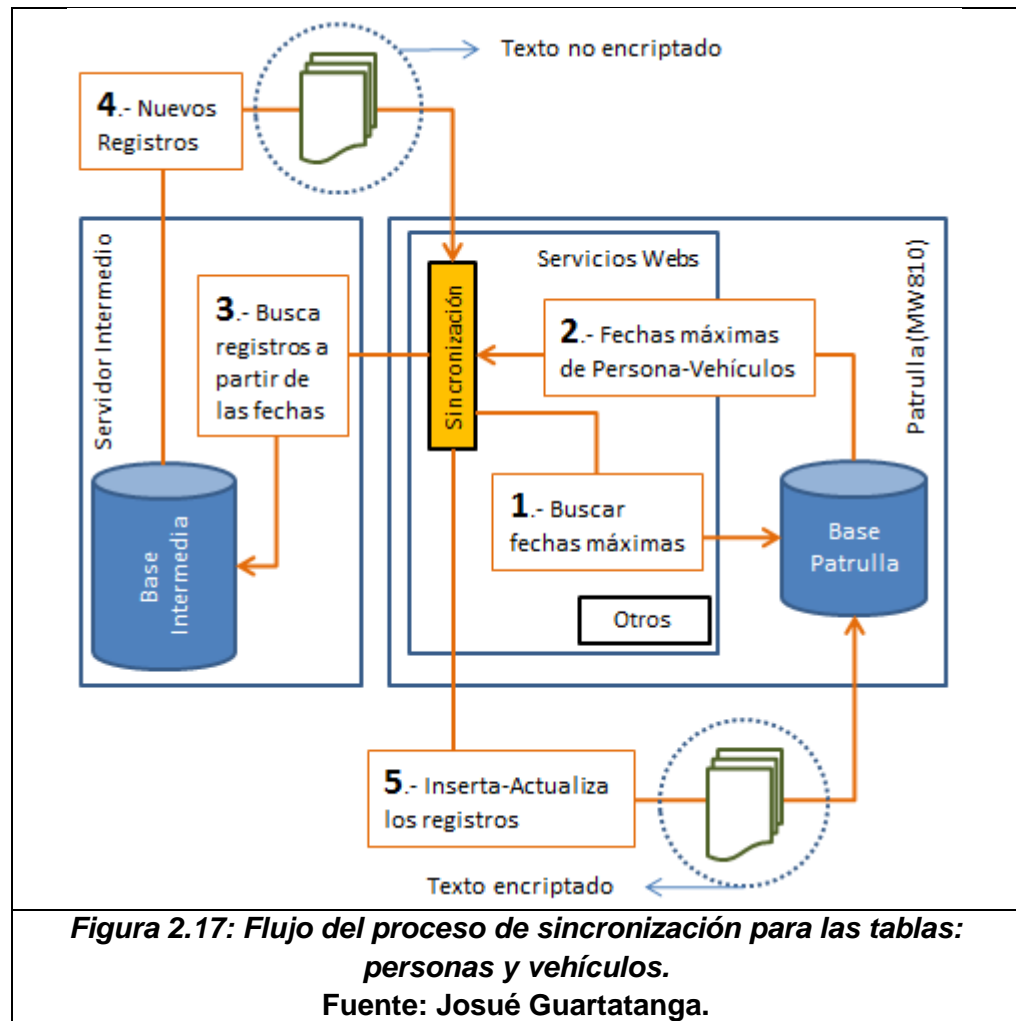
2.2. Implementación del proceso de sincronización de datos para ciertas tablas de la Base Patrulla.

El proceso de sincronización consiste en la actualización de los registros de las tablas de: “personas”, “vehículos”, “movimientos migratorios”, “detenciones”, “órdenes de captura” e “impedimentos de salida” de la Base Patrulla, teniendo como fuente de datos la Base Intermedia.

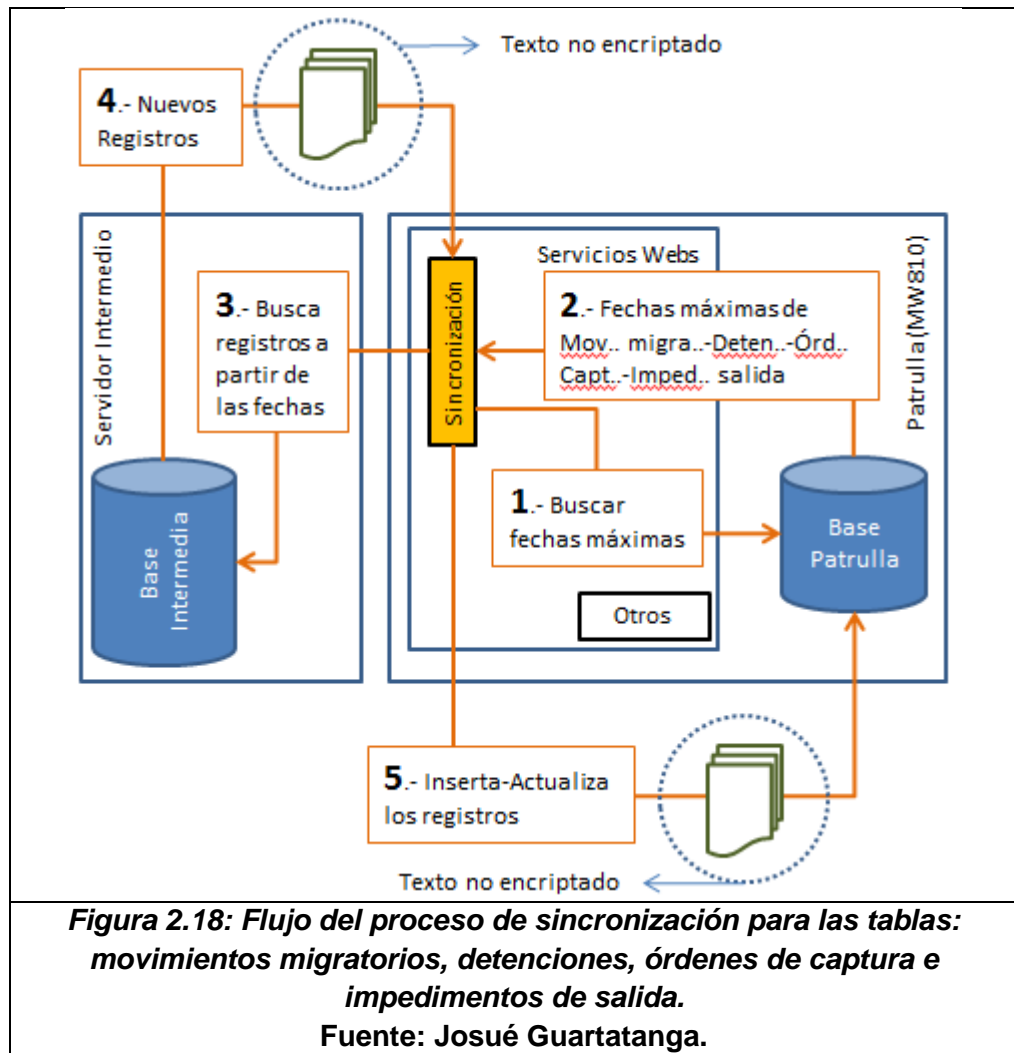


El proceso utiliza un servicio web local que busca la fecha máxima (timestamp) de los registros de las tablas de la Base Patrulla que servirán como fechas de inicio en la búsqueda de los nuevos registros de la Base Intermedia (Ver Figura 2.16).

Los datos considerados como información privada que vienen de la Base Intermedia se encriptarán antes actualizar las tablas de “personas” y “vehículos” de la Base Patrulla (Ver Figura 2.17).



Los datos no considerados como información privada que vienen de la Base Intermedia para actualizar las tablas: “movimientos migratorios”, “detenciones”, “órdenes de captura” e “impedimentos de salida” de la Base Patrulla no serán necesarios de encriptar (Ver Figura 2.18).



Los servicios web se realizaron con ayuda de la herramienta Talend Open Studio – Data Integration [2] en la que se implementó 6 tareas de sincronización. Estas tareas se exportaron como Axis WebService (WAR) para deployarlos en el servidor de aplicaciones GlassFish 3.1.2 [4].

El diseño general de los 6 servicios webs para la sincronización de las 6 tablas es el siguiente (Ver Figura 2.19). Sólo varían en las vistas de la Base Intermedia a las que se consultan y las tablas de la Base Patrulla a las que se actualizan.



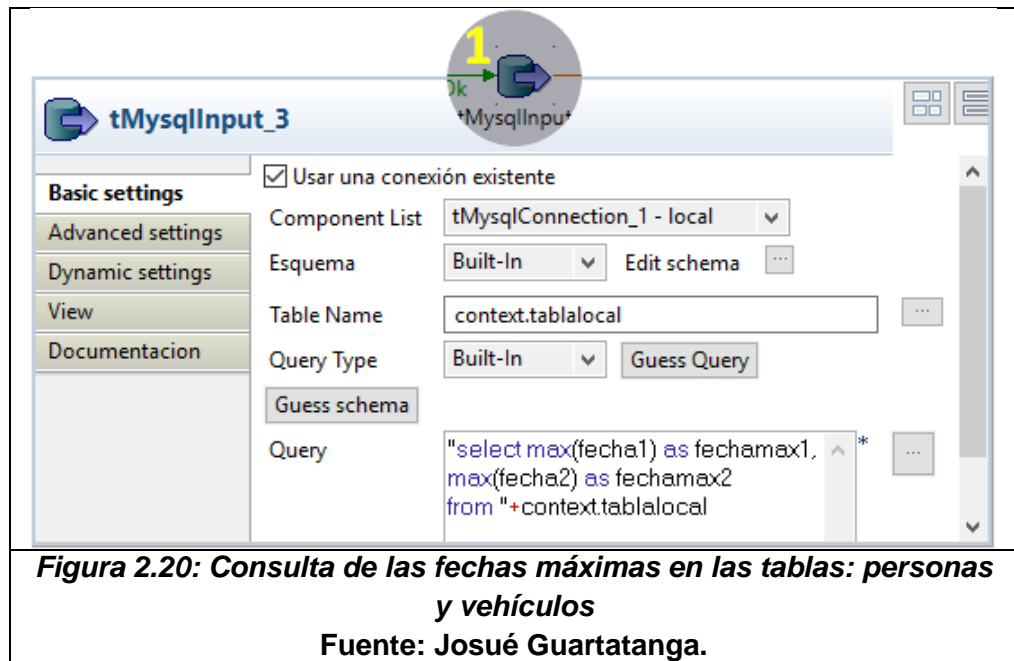
Los parámetros de entrada para que funcione cada servicio web son:

- base.- El nombre de la base de datos del servidor intermedio a la que se quiere conectar.
- tabla.- El nombre de la tabla en el servidor intermedio de la que se desea extraer los registros para actualización. Realmente es una vista.
- tablalocal.- El nombre de la tabla de la patrulla a la que se desea actualizar
- fechalimit.- Es la fecha hasta donde se desea extraer los registros de la tabla en el servidor intermedio.
- particion.- Es un número que sirve para dividir el proceso de sincronización en partes. Esto depende del cuán desactualizada esté la base de datos de la patrulla

En el elemento marcado con 1 se obtiene la fecha máxima de la tabla T de la Base Patrulla (Ver Figura 2.20).

En el elemento marcado con 2 se obtendrán los registros de la vista W de la Base Intermedia a partir de la fecha máxima obtenida en 1 (Ver Figuras 2.21 – 2.26).

En el elemento marcado con 3 se guardan y actualizan [5] los registros en la tabla T de la Base Patrulla que se obtuvieron en el elemento marcado con 2 (Ver Figs. 2.27 – 2.29).



The screenshot shows the configuration window for 'tMysqlInput_2'. The 'Query' field contains a SQL query with several date-related conditions. A blue circle highlights the conditions in the 'Query' field, and a blue arrow points from this circle to a callout box containing the full SQL query.

Query (highlighted in the screenshot):

```
and fecha2 > "" + context.fechamax2 + ""
and fecha2 < "" + context.fechalimit + ""
or fecha1 > "" + context.fechamax1 + ""
and fecha1 < "" + context.fechalimit + ""
```

Full SQL Query (shown in the callout box):

```
"select
  cdg, cdg_doc,tipo,documento,fechaexp,fechacad,
  nombre1,nombre2,apellido1,apellido2,estadociv,
  paiscb1,fechanac,sexo,falso,fecha1,fecha2
from [redacted] where cdg is not null and cdg_doc is not null
and fecha2 > "" + context.fechamax2 + ""
and fecha2 < "" + context.fechalimit + ""
or fecha1 > "" + context.fechamax1 + ""
and fecha1 < "" + context.fechalimit + ""
"
```

Figura 2.21: Consulta de los nuevos registros de la vista de personas de la Base Intermedia
Fuente: Josué Guartatanga.

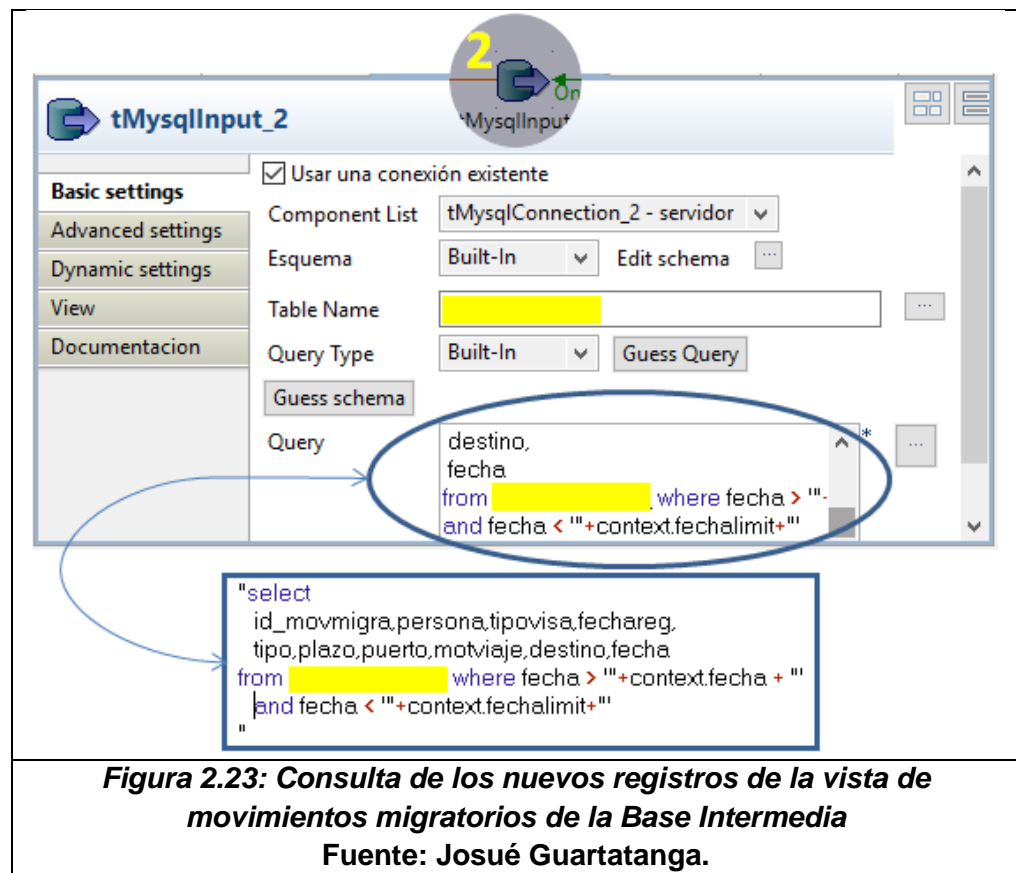
The screenshot shows the configuration window for 'tMysqlInput_2'. The 'Query' field contains the following SQL query:

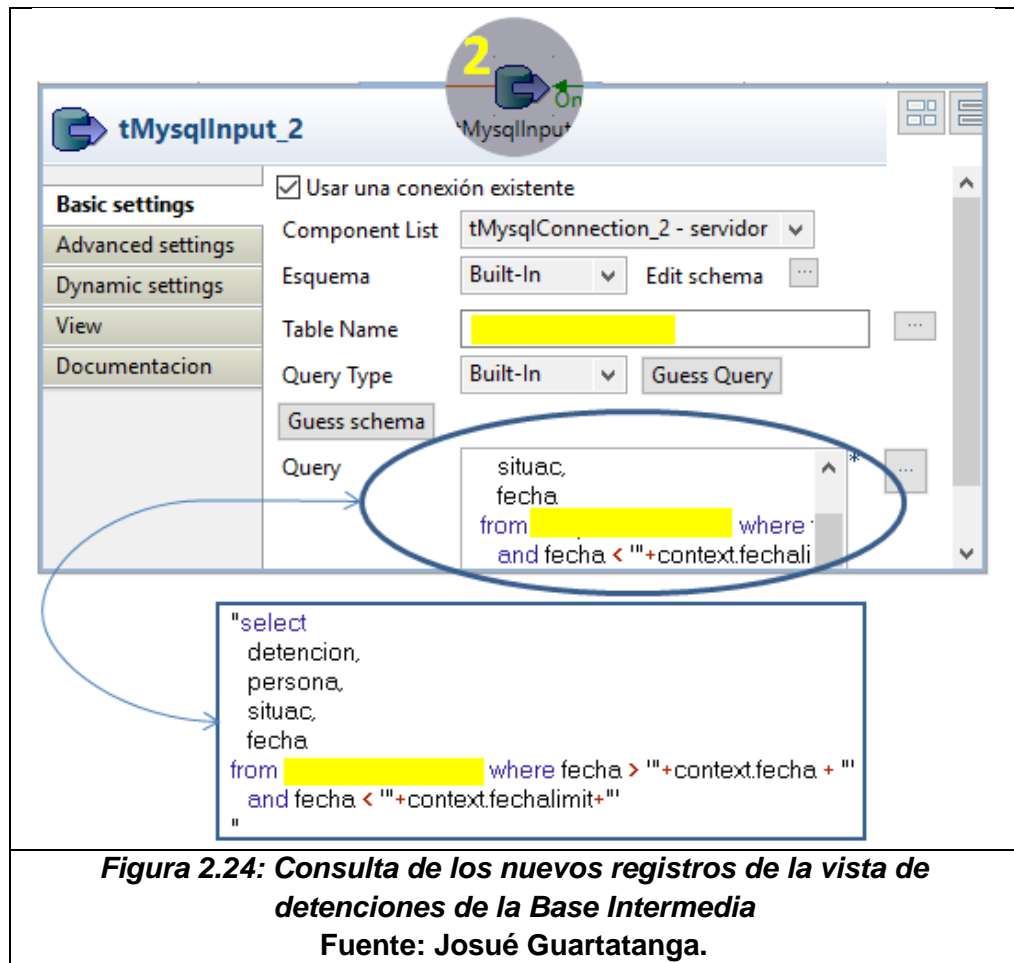
```
and fecha2 > "" + context.fechamax2 + ""
and fecha2 < "" + context.fechalimit + ""
or fecha1 > "" + context.fechamax1 + ""
and fecha1 < "" + context.fechalimit + ""
```

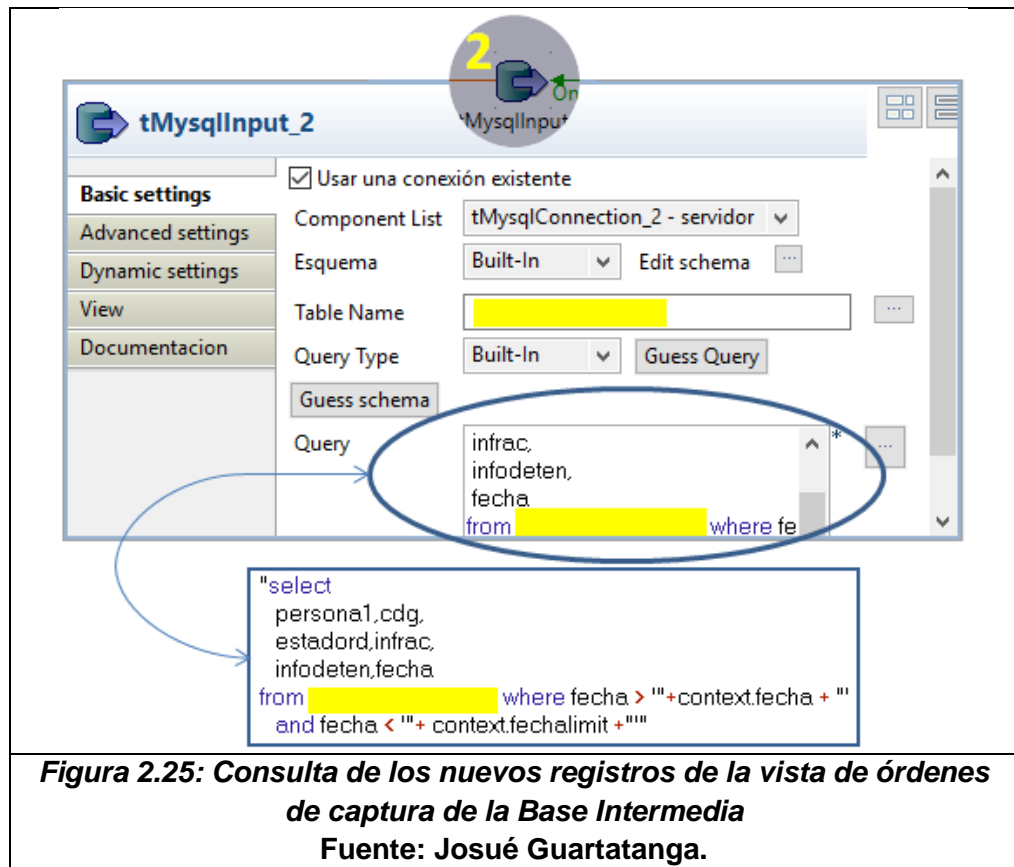
Below the configuration window, a separate text box displays the full SQL query:

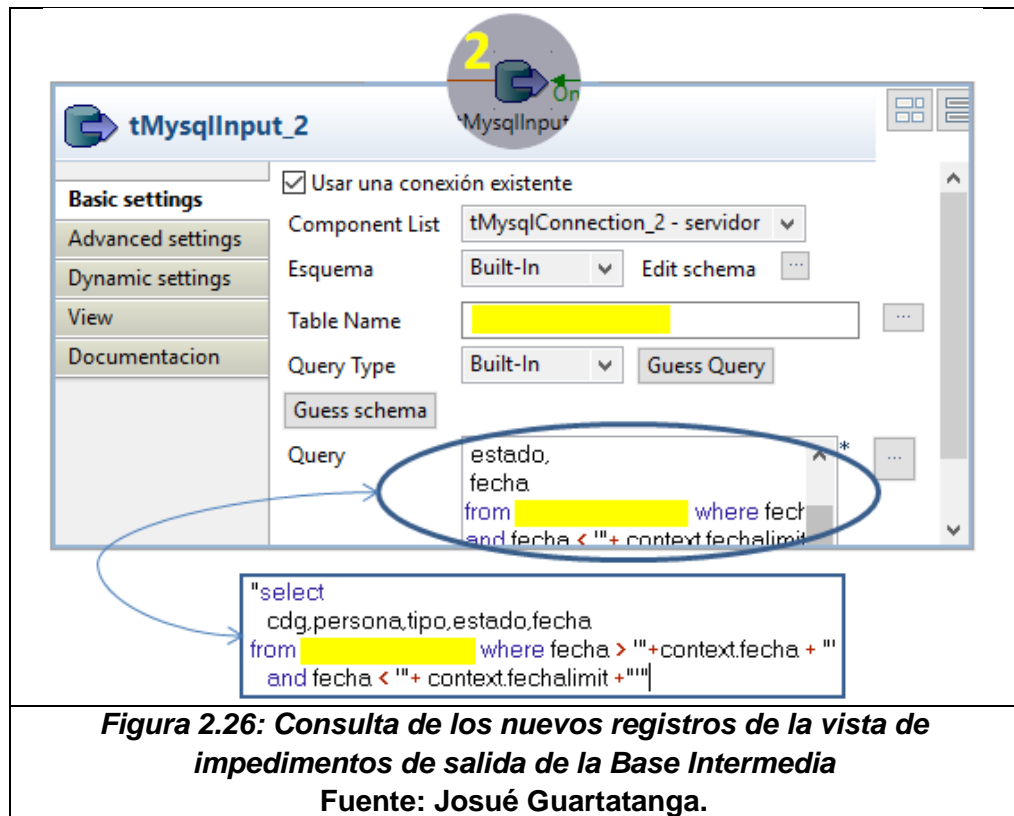
```
"select
cdg,placa,motor,chasis,modelo,marca,clasevehi,tipovehi,
aniofab,color1,color2,persona,cdg_res,restric,activado,
fecha1,fecha2
from [redacted] where cdg is not null
and fecha2 > "" + context.fechamax2 + ""
and fecha2 < "" + context.fechalimit + ""
or fecha1 > "" + context.fechamax1 + ""
and fecha1 < "" + context.fechalimit + ""
"
```

Figura 2.22: Consulta de los nuevos registros de la vista de vehículos de la Base Intermedia
Fuente: Josué Guartatanga.









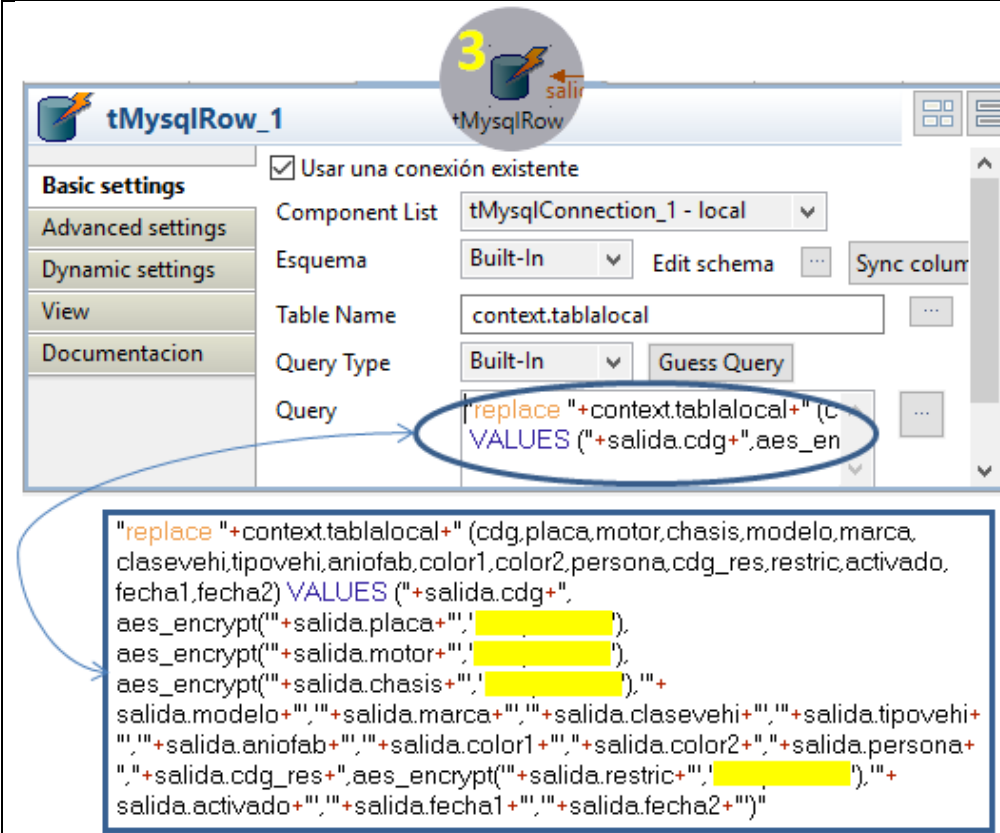
The screenshot shows the tMySQLRow_1 application interface. The 'Query' field contains the following SQL statement:

```
replace "+context.tablalocal+" (c
VALUES ("+salida.cdg_doc+", "+
```

The callout box contains the full query text:

```
"replace "+context.tablalocal+" (cdg_doc,tipo,documento,fechaexp,
fechacad,cdg.nombre1,nombre2,apellido1,apellido2,estadociv,
paiscb1,fechanac,sexo,falso,fecha1,fecha2)
VALUES ("+salida.cdg_doc+", "+salida.tipo+",
aes_encrypt(""+salida.documento+", '...', ''), "+
salida.fechaexp+", "+salida.fechacad+", "+salida.cdg+",
aes_encrypt(""+salida.nombre1+", '...', ''),
aes_encrypt(""+salida.nombre2+", '...', ''),
aes_encrypt(""+salida.apellido1+", '...', ''),
aes_encrypt(""+salida.apellido2+", '...', ''), "+
salida.estadociv+", "+salida.paiscb1+", "+
salida.fechanac+", "+salida.sexo+", "+salida.falso+", "+
salida.fecha1+", "+salida.fecha2+"")"
```

Figura 2.27: Actualización de la tabla personas de la Base Patrulla con datos encriptados
Fuente: Josué Quartatanga.



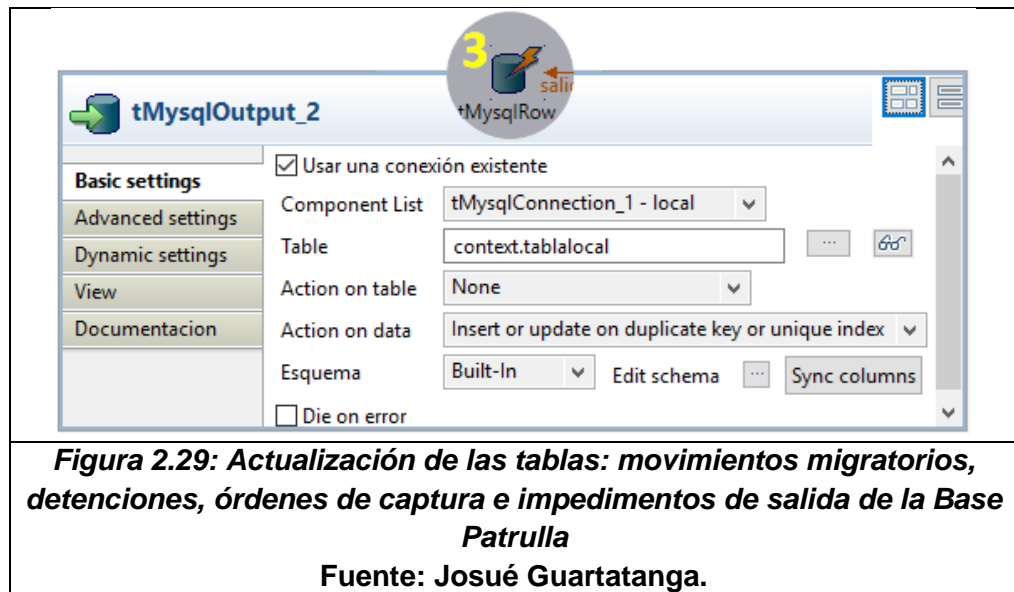
The screenshot shows the tMySQLRow_1 application window. The 'Query' field contains the following SQL statement:

```
replace "+context.tablalocal+" (
VALUES ("+salida.cdg+", aes_en
```

The full query shown in the expanded view is:

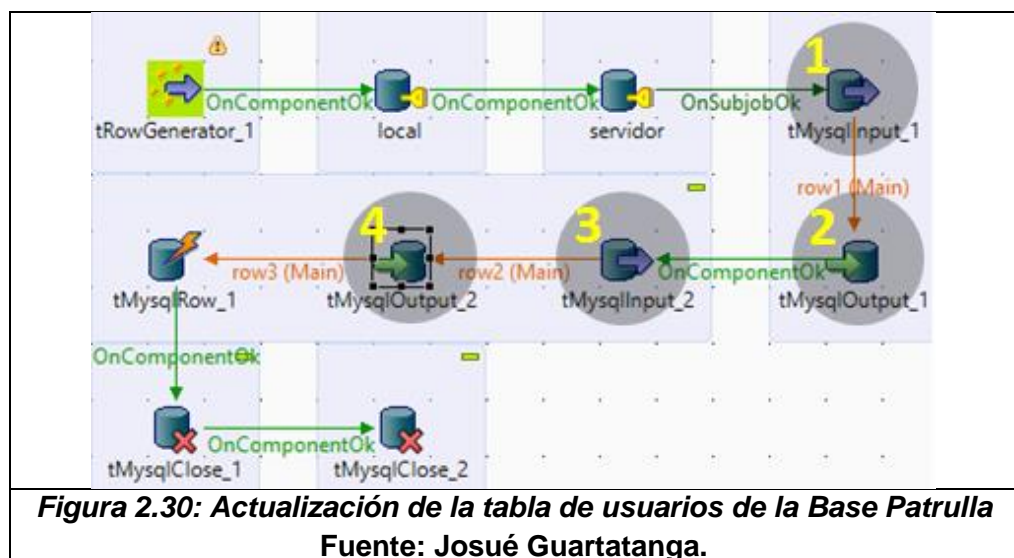
```
"replace "+context.tablalocal+" (cdg,placa,motor,chasis,modelo,marca,
clasevehi,tipovehi,aniofab,color1,color2,persona,cdg_res,restric,activado,
fecha1,fecha2) VALUES ("+salida.cdg+",
aes_encrypt(""+salida.placa+"','"),
aes_encrypt(""+salida.motor+"','"),
aes_encrypt(""+salida.chasis+"','"),""+
salida.modelo+"','"+salida.marca+"','"+salida.clasevehi+"','"+salida.tipovehi+
'"+salida.aniofab+"','"+salida.color1+"','"+salida.color2+"','"+salida.persona+
'"+salida.cdg_res+",aes_encrypt(""+salida.restric+"','"),""+
salida.activado+"','"+salida.fecha1+"','"+salida.fecha2+"")"
```

Figura 2.28: Actualización de la tabla vehículos de la Base Patrulla con datos encriptados
Fuente: Josué Guartatanga.

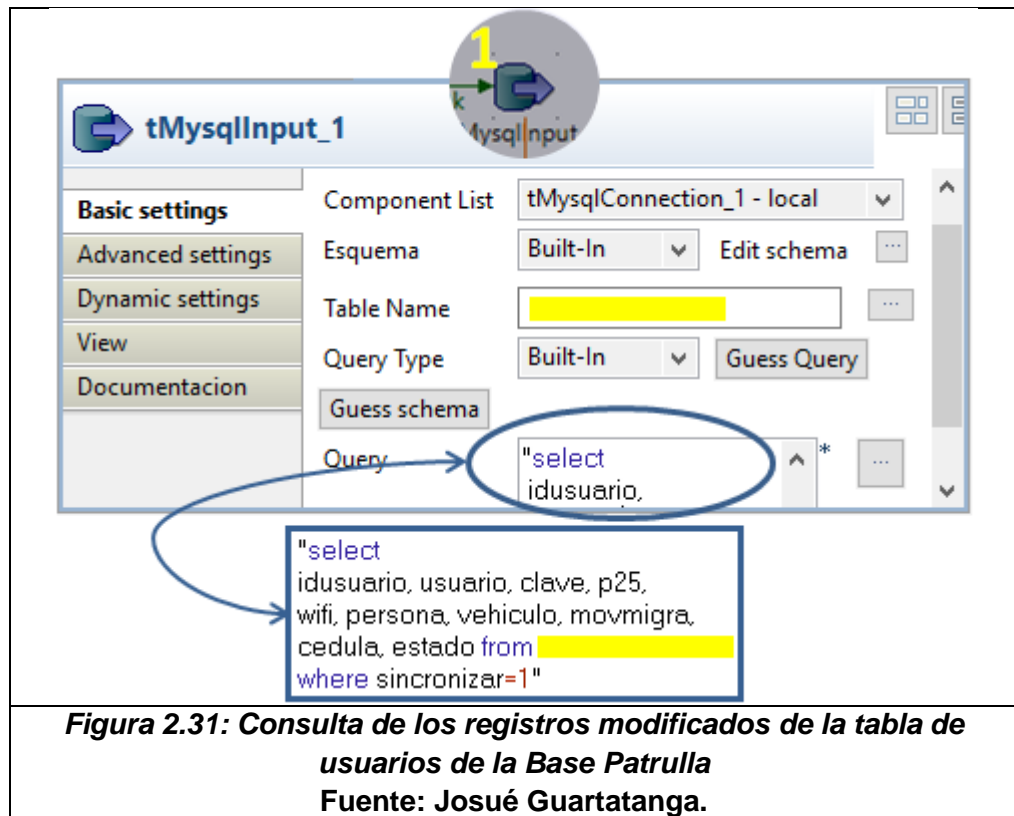


El proceso de sincronización también consiste en la actualización de la tabla de usuarios en donde se almacenan las credenciales para el acceso a SICOP teniendo como fuente de datos la Base Intermedia.

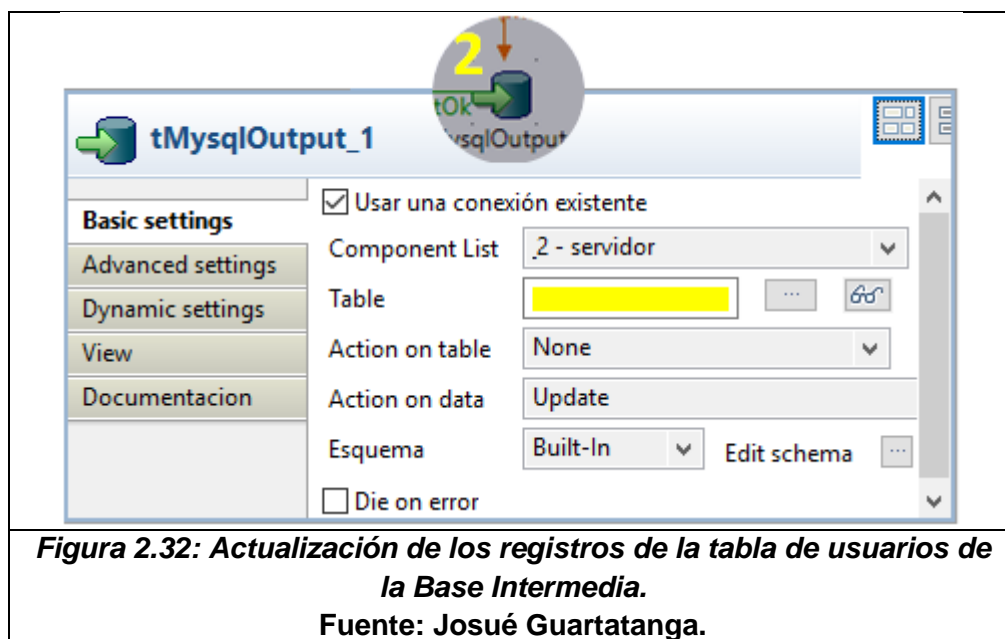
El diseño del servicio web para la sincronización de la tabla de usuario es el siguiente (Ver Figura 2.30).



En el elemento marcado con 1 se obtienen todos los registros que se actualizaron desde SICOP, ya que se permite a los usuarios cambiar la contraseña cuando lo requieran. Estos registros se identifican con el valor del campo sincronizar=1 (Ver Figura 2.31).



En el elemento marcado con 2 se insertan a la Base Intermedia todos los registros que se obtuvieron de 1. (Ver Figura 2.32).



En los elementos marcados con 3 y 4 ocurre el proceso inverso. Se obtienen los usuarios creados en la Base Intermedia y viajarán a la tabla de usuarios de la Base Patrulla.

Este proceso de sincronización de usuarios finaliza actualizando el valor del campo sincronizar=0 de los registros que ya fueron sincronizados.

2.3. Implementación para reportes de auditoría en Servidor Intermedio.

En el proceso de sincronización de la base de datos de cada patrulla se desea registrar en la tabla de log de sincronización lo siguiente:

- El usuario.- Quien realiza la sincronización.
- El nombre de la máquina de la patrulla.- A cada máquina (MW810) que se encuentra en la patrulla se le dio un nombre compuesto por: El

chasis, la placa y la zona a la que pertenece. Este dato está parametrizado.

- El nombre de la tabla.- La tabla que se está actualizando. Este dato está parametrizado.
- La fecha o fechas máximas de la tabla.- Las fechas que sirven para la búsqueda de nuevos registros en la base intermedia. Estos datos están parametrizados.
- La cantidad de registros que se procesa.- El número de registros que pasan a la tabla de la base patrulla. Este dato se lo obtendrá en el proceso.
- La partición de la sincronización.- Según la cantidad de días de desactualización de la tabla, la sincronización se divide en partes. La cantidad de días se cuenta a partir de la fecha máxima de la tabla hasta la fecha actual. Este dato está parametrizado.
- La fecha y hora en que se realizó.- Esto se configuró poniendo un campo de timestamp en la tabla de logs para auditoría.

Se añadió a cada servicio web del proceso sincronización los siguientes parámetros de entrada para completar los datos de registro de auditoría:

- maquina.- Nombre de la máquina de la patrulla
- usuario.- El nombre de usuario que realiza la sincronización
- lati.- Latitud provista por el gps de la patrulla
- longi.- Longitud provista por el gps de la patrulla

Para poder grabar cada registro que pase a la base de datos de la patrulla fue necesario incorporar tres elementos importantes en el diseño del proceso de sincronización, marcados con los literales A, B y C. Quedando finalmente el diseño del proceso de sincronización de la siguiente manera (Ver Figura 2.33).

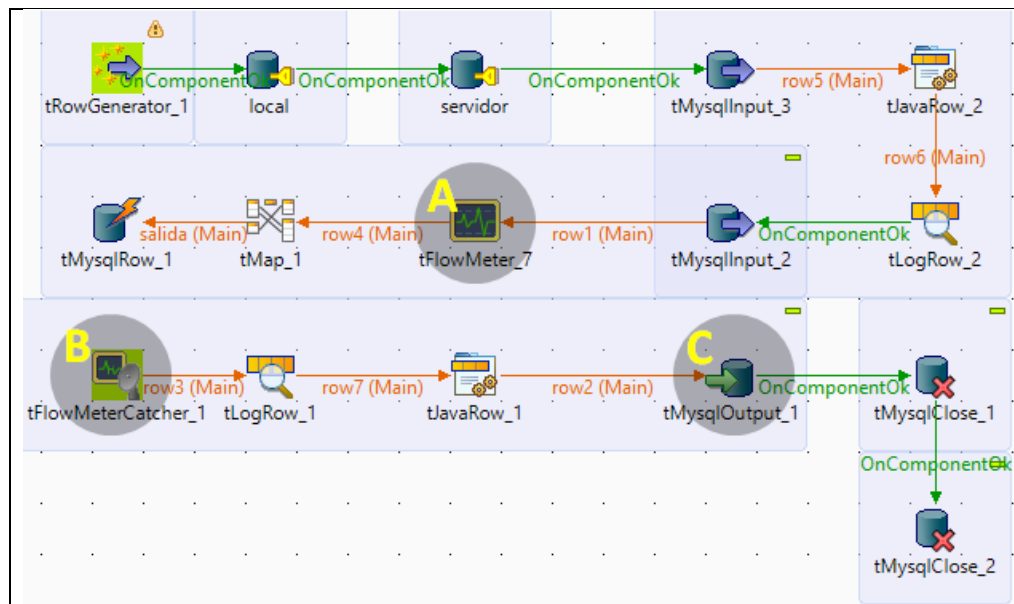


Figura 2.33: Diseño final de los servicios web del proceso de sincronización para registrar datos de auditoría

Fuente: Josué Guartatanga.

En el elemento marcado con A se registran las métricas del flujo de información, entre ellas está el número de registros que pasaron.

El elemento marcado con B escucha al elemento marcado con A proveyendo un estandarizado registro de log como salida (Ver Figura 2.34).

Schema of tFlowMeterCatcher_1

tFlowMeterCatcher_1

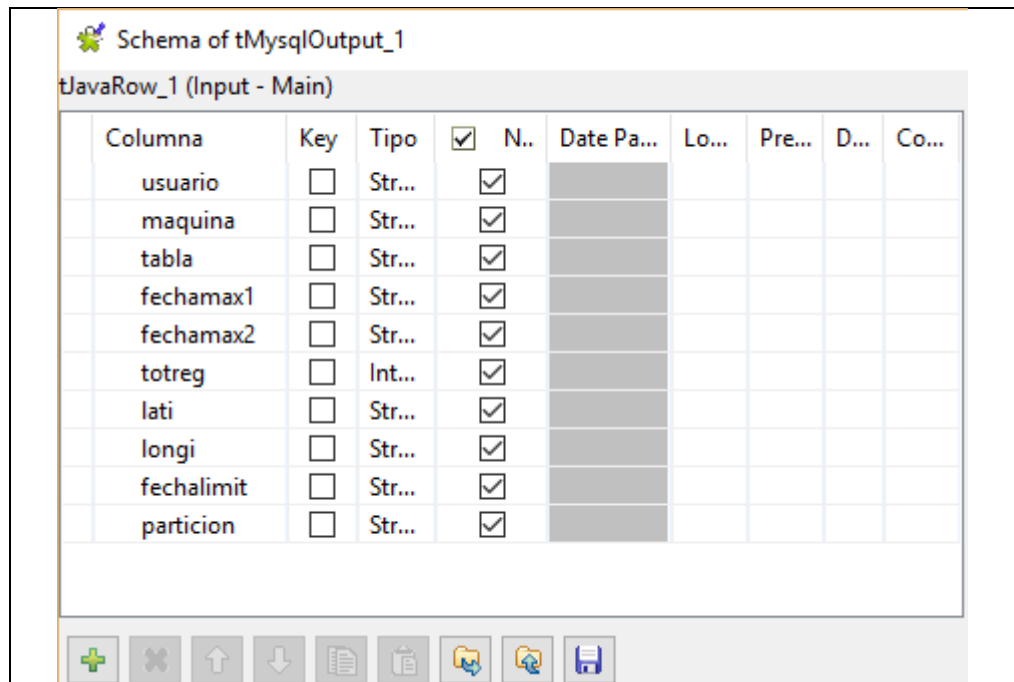
Columna	Key	Tipo	<input checked="" type="checkbox"/>	N..	Date Patt...	Lon...	Prec...	De...	Co...
moment	<input type="checkbox"/>	Date	<input checked="" type="checkbox"/>		"yyyy-M...		0		
pid	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			20	0		
father_pid	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			20	0		
root_pid	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			20	0		
system_pid	<input type="checkbox"/>	Long	<input checked="" type="checkbox"/>			8	0		
project	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			50	0		
job	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			50	0		
job_repositor...	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			255	0		
job_version	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			255	0		
context	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			50	0		
origin	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			255	0		
label	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			255	0		
count	<input type="checkbox"/>	Inte...	<input checked="" type="checkbox"/>			3	0		
reference	<input type="checkbox"/>	Inte...	<input checked="" type="checkbox"/>			3	0		
thresholds	<input type="checkbox"/>	String	<input checked="" type="checkbox"/>			255	0		

Dato necesario para auditoría

Aceptar Cancelar

Figura 2.34: Datos de salida del elemento que escucha las métricas de flujo (tFlowMeterCatcher)
Fuente: Josué Guartatanga.

En el elemento marcado con C se guardan los registros en la tabla de Logs de sincronización para auditoría de la base patrulla (Ver Figura 2.35).



Schema of tMysqlOutput_1

tJavaRow_1 (Input - Main)

Columna	Key	Tipo	<input checked="" type="checkbox"/> N..	Date Pa...	Lo...	Pre...	D...	Co...
usuario	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
maquina	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
tabla	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
fechamax1	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
fechamax2	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
totreg	<input type="checkbox"/>	Int...	<input checked="" type="checkbox"/>					
lati	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
longi	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
fechalimit	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					
particion	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>					

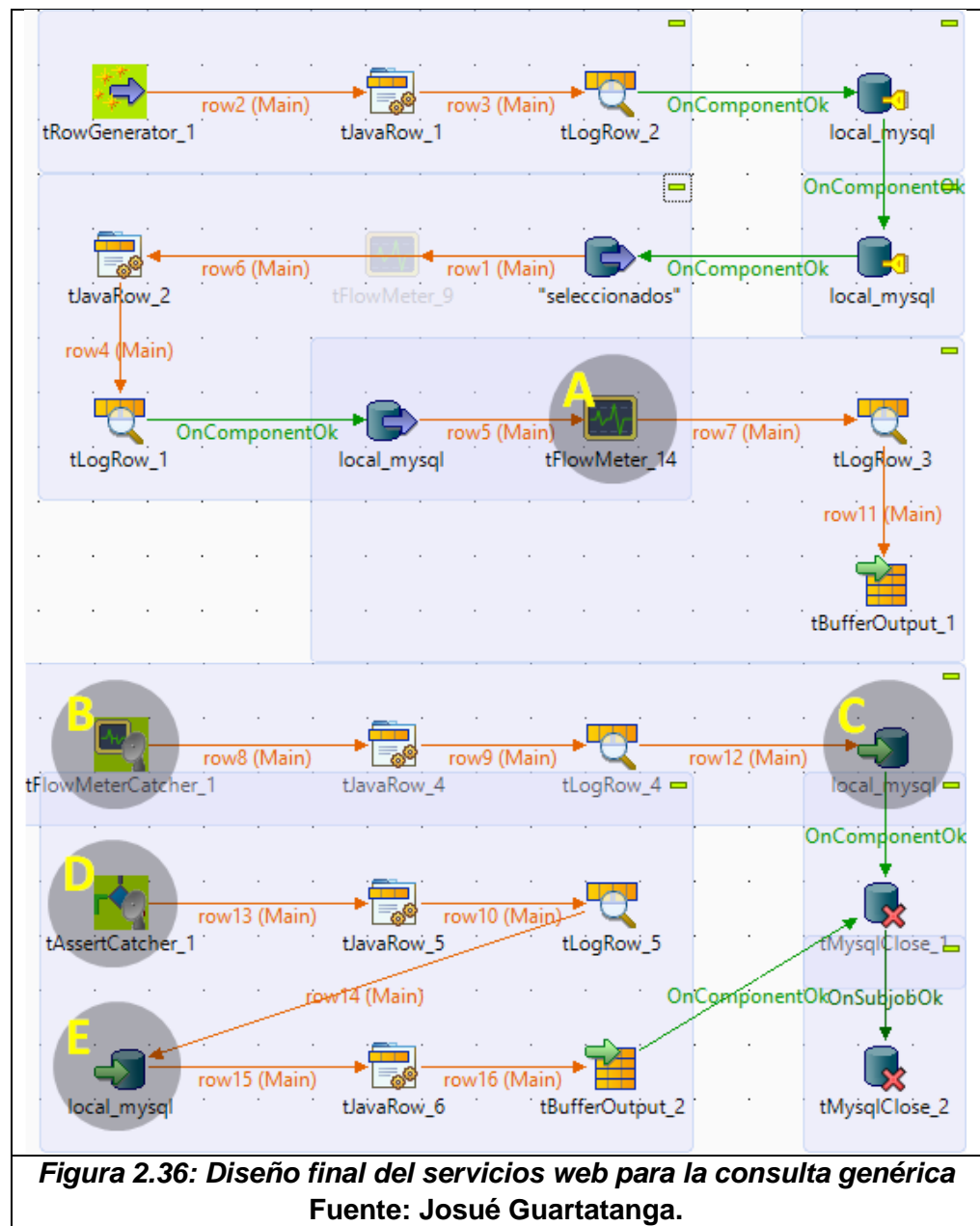
Figura 2.35: Datos de entrada del elemento que guarda los registros de sincronización para auditoría (tMysqlOutput)
Fuente: Josué Guartatanga.

La consulta manual deberá registrar en la tabla de log de operaciones lo siguiente:

- El usuario.- Quien realiza la consulta.
- El tipo de consulta.- Existen tres tipos de consulta que son:
 - Consulta de personas: por cédula o pasaporte
 - Consulta de vehículos: por placa, chasis o motor
 - Consulta de movimientos migratorios: por cédula o pasaporte
 El tipo de consulta es identificado por el id del registro de la tabla donde se guardan las consultas utilizadas.
- La fecha y hora en que se realizó.- Esto se configuró poniendo un campo de timestamp en la tabla de logs para auditoría.

- lati.- Latitud provista por el gps de la patrulla.
- longi.- Longitud provista por el gps de la patrulla.

Para poder guardar registros para auditoría de las consultas manuales en SICOP, fue necesario incorporar 5 elementos importantes en el diseño del servicio web de consulta genérica, marcados con los literales A, B, C, D y E. Quedando finalmente el diseño del servicio web de la consulta genérica de la siguiente manera (Ver Figura 2.36).



En el elemento marcado con A se registran las métricas del flujo de información.

El elemento marcado con B escucha al elemento marcado con A proporcionando un estandarizado registro de log como salida.

En el elemento marcado con C se guardan los registros para auditoría (Ver Figura 2.37).

Schema of local_mysql

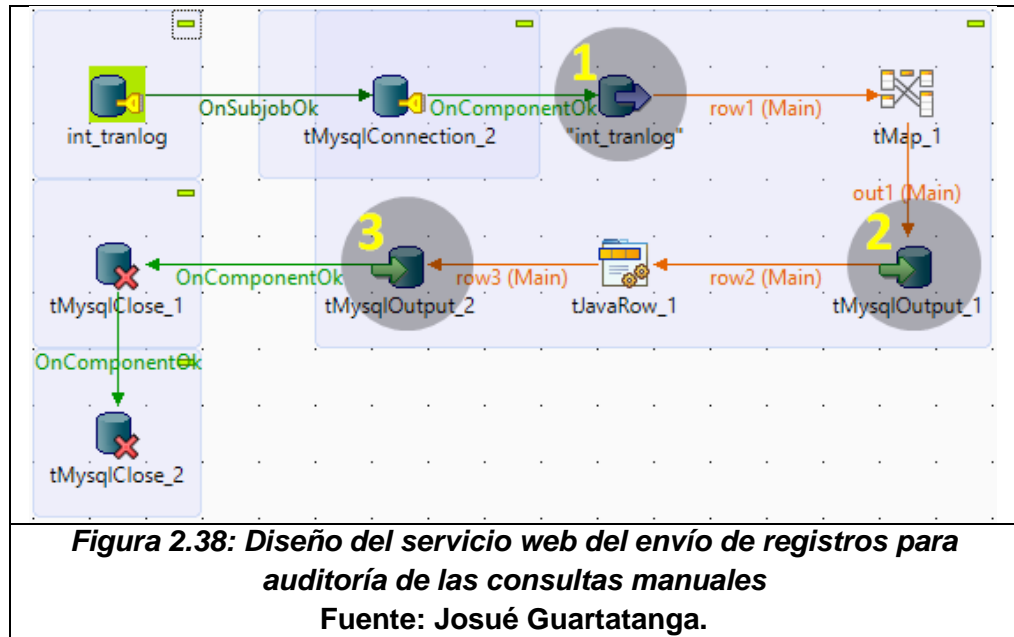
tLogRow_4 (Input - Main)

Columna	Key	Tipo	<input checked="" type="checkbox"/>	N..	Date Pa...	Lo...	Pre...	D...	Co...
moment	<input type="checkbox"/>	Date	<input checked="" type="checkbox"/>		"yyy-...		0		
pid	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			20	0		
father_pid	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			20	0		
root_pid	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			20	0		
system_pid	<input type="checkbox"/>	Lo...	<input checked="" type="checkbox"/>			8	0		
project	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			50	0		
job	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			50	0		
job_reposi...	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			255	0		
job_version	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			255	0		
context	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			50	0		
origin	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			255	0		
label	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			255	0		
count	<input type="checkbox"/>	Int...	<input checked="" type="checkbox"/>			3	0		
reference	<input type="checkbox"/>	Int...	<input checked="" type="checkbox"/>			3	0		
thresholds	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			255	0		
usuario	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			50			
origen	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			5			
lati	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>						
longi	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			20			
sql	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			2			
llave	<input type="checkbox"/>	Str...	<input checked="" type="checkbox"/>			25			

Datos necesario para auditoría

Figura 2.37: Datos de entrada del elemento que guarda los registros de consulta para auditoría (tMysqlOutput)
Fuente: Josué Guartatanga.

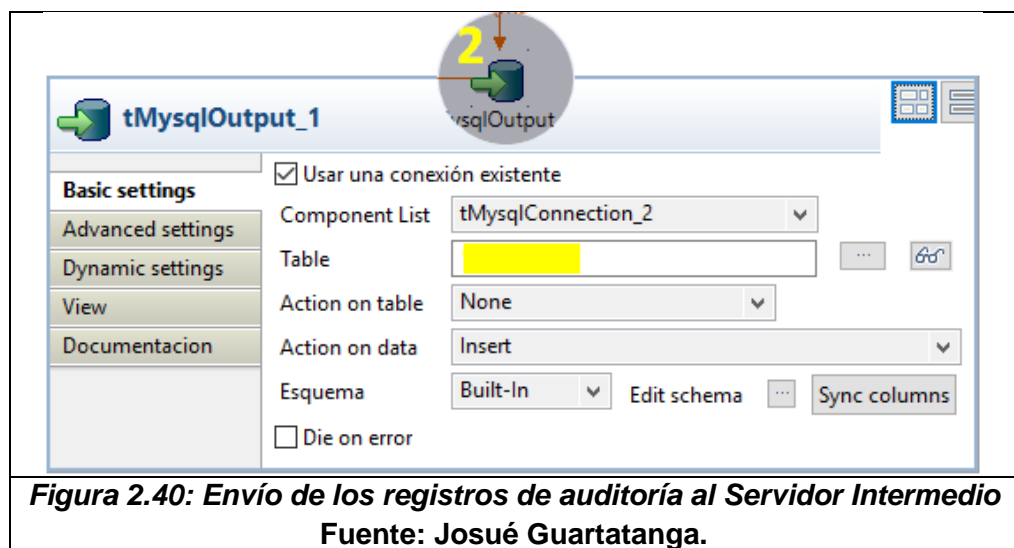
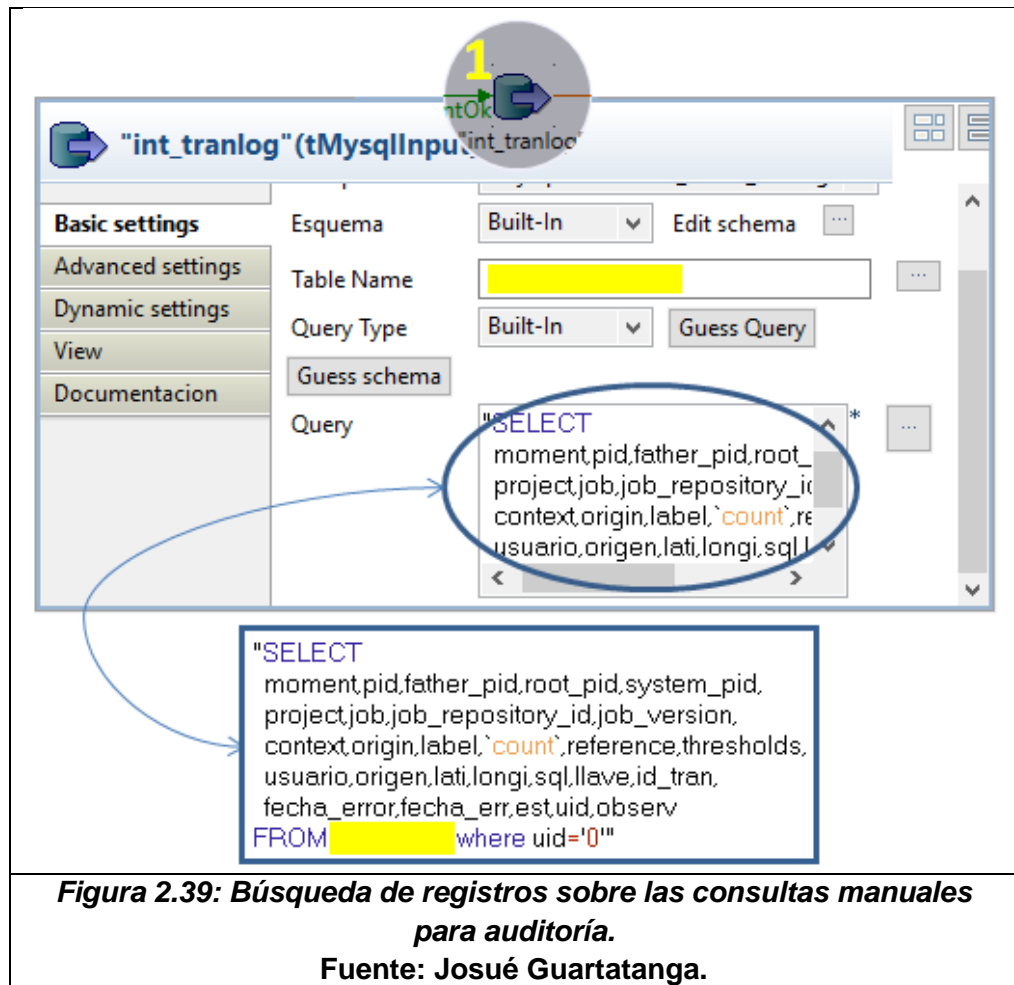
Los registros para auditorías de las consultas manuales que están en local se enviarán al Servidor Intermedio para su posterior análisis de auditoría mediante el siguiente servicio web (Ver Figura 2.38).

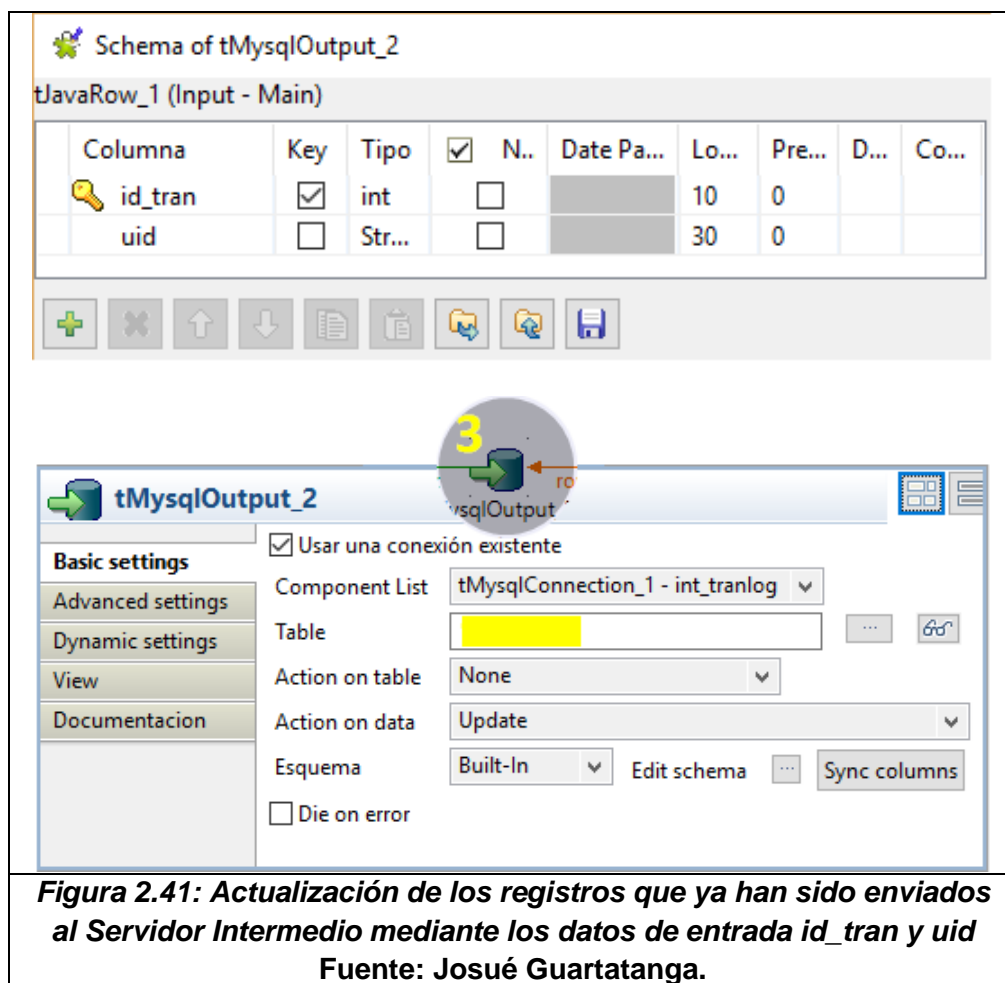


En el elemento marcado con 1 se realiza la consulta de los registros de auditoría que se enviarán al Servidor Intermedio, aquellos cuyo campo uid sea cero (Ver Figura 2.39).

En el elemento marcado con 2 se realiza la inserción de los registros de auditoría en el Servidor Intermedio (Ver Figura 2.40).

En el elemento marcado con 3 se realiza la actualización de los registros que ya pasaron al Servidor Intermedio, actualizando el campo uid a otro valor (Ver Figura 2.41).





El hit de captura de un vehículo robado deberá registrar en el log de alpr lo siguiente:

- El usuario.- Quien opera SICOP.
- La placa del vehículo.- La placa está en la tabla de vehículos con la restricción activa de robado.
- La latitud y longitud.- La geolocalización de la patrulla al momento de capturar la placa de un vehículo reportado como robado.
- La fecha y hora en que se realizó.

Este proceso se desarrolló en visual C#.Net debido a la facilidad de interactuar con el puerto serial de la cámara ALPR.

Parte del código del registro del hit se presenta a continuación (Ver Figura 2.42).

```
MySQLCommand cmd = new MySQLCommand();
MySQLDataReader r = null;
try
{
    cnx.Open();
    cmd.Connection = cnx;
    cmd.CommandText =
        "insert into [REDACTED] (" +
        "usuario,lati,longi,placa,mac) values ('" +
        usuario + "','" + lati + "','" + longi + "','" +
        placa + "','" + mac + "')";
    cmd.ExecuteNonQuery();
}
catch (Exception e)
{
    cnx.Close();
    return 0;
}
```

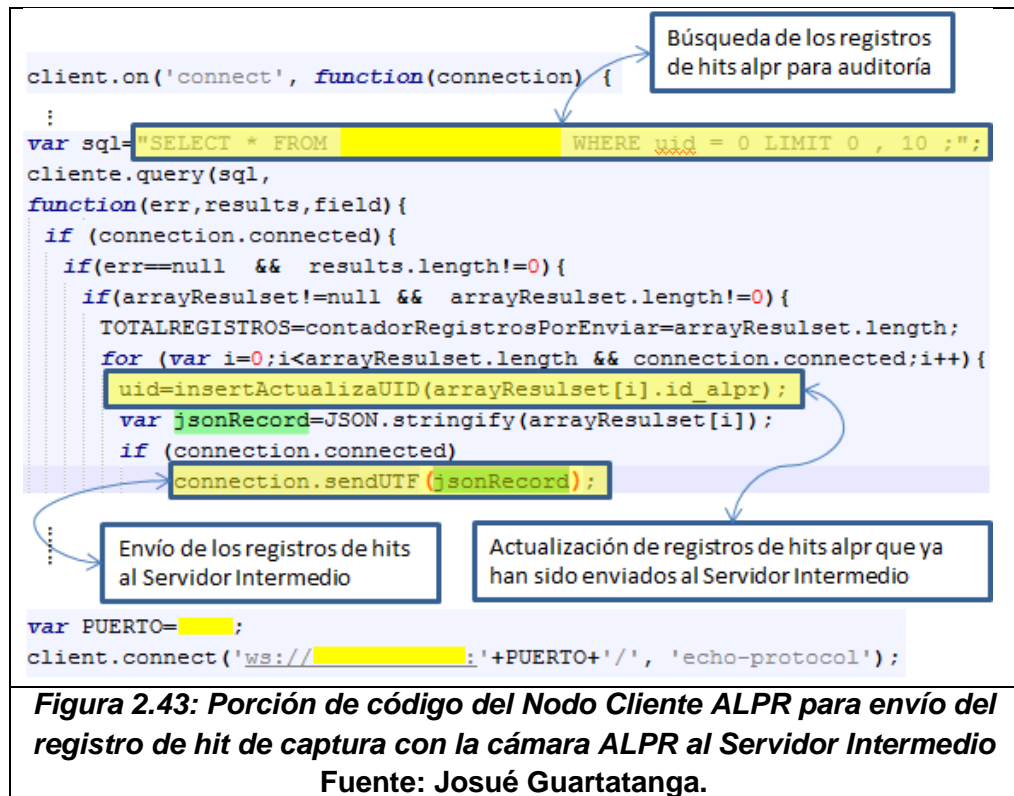
Figura 2.42: Porción de código C#.Net del registro de hit de captura con la cámara ALPR de un vehículo robado a la base patrulla

Fuente: Josué Guartatanga.

Los registros de hit de captura que están en la Base Patrulla se enviarán, mediante un “Nodo Cliente ALPR”, al Servidor Intermedio para su posterior análisis de auditoría (Ver Figura 2.43).

En el Servidor Intermedio corre un “Nodo Servidor ALPR” que recibe el registro hit y lo inserta en la Base Intermedia (Ver Figura 2.44).

Estos nodos fueron realizados en Node.js utilizando websokets para su respectiva comunicación en un determinado puerto.



```

var PORT=;
server.listen(PORT, function() {
  console.log((new Date()) +
    ' Server is listening on port '+PORT+' ');
});
wsServer.on('request', function(request){
  if (!originIsAllowed(request.origin)){
    request.reject(); return;
  }
  var connection = request.accept('echo-protocol', request.origin);
  console.log((new Date()) + ' Connection accepted. ');
  connection.on('message', function(message) {
    if (message.type === 'utf8') {
      console.log('Received Message: ' + message.utf8Data);
      var objRecord=eval('(' +message.utf8Data+') ');
      if(objRecord!=null){
        if(objRecord.numero_registros!=null){
          :
        }
        else{
          var sql2="INSERT INTO int_tranlog_alpr "+
            "( `usuario`, `timestamp`, `lati`, "+
            "`longi`, `placa`, `mac`) VALUES (?, ?, ?, ?, ?, ?)";
          cliente.query(sql2, [objRecord.usuario,objRecord.timestamp,
            objRecord.lati,objRecord.longi,
            objRecord.placa,objRecord.mac],
            function(errorInsert, results, field) {
              console.log(errorInsert);
            });
        }
      }
    }
  });
}
}

```

Recibe le registro hit

Inserta registro hit en Servidor Intermedio

Figura 2.44: Porción de código del Nodo Servidor ALPR para recibir los registros de hit de captura con la cámara ALPR e insertarlos a la Base Intermedia

Fuente: Josué Guartatanga.

2.4. Implementación de seguridad en: El Sistema Operativo por restricción de funcionalidades; El Código fuente de SICOP.

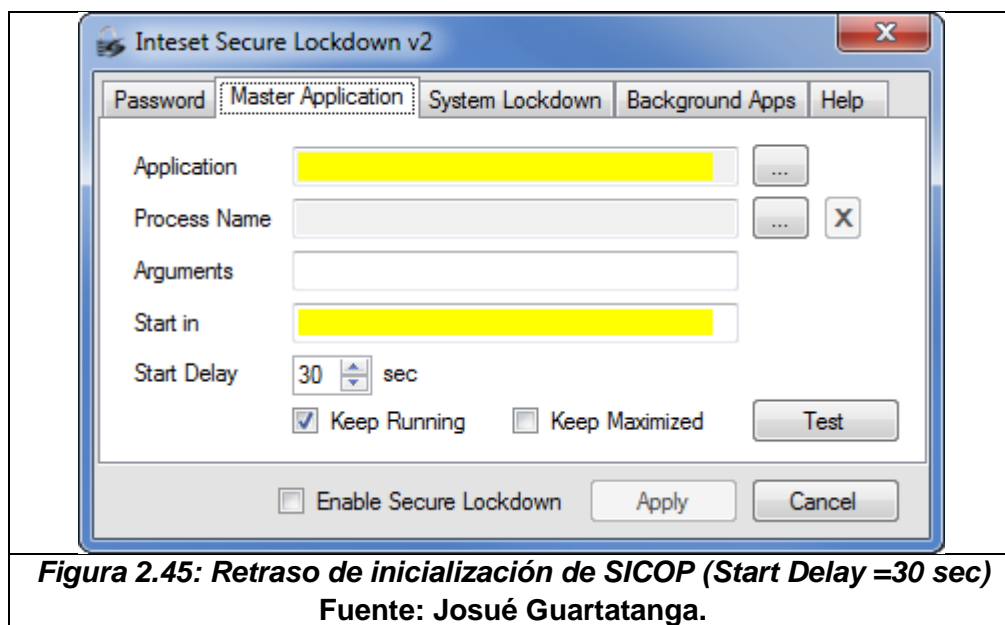
Debido a que el Sistema operativo estará expuesto para el uso del agente policial se bloqueó ciertas funcionalidades para protegerlo.

La solución que se encontró es la instalación de una aplicación kiosko para el Sistema Operativo que: proporciona seguridad al disuadir a los usuarios a realizar ataques maliciosos; previene el mal uso de las funciones que ofrece el Sistema Operativo y limita a los usuarios a realizar actividades específicas de manera que el dispositivo (MW810) se pueda utilizar para una determinada tarea.

Se escogió Secure Lockdown [6] como kiosko del Sistema Operativo debido al precio conveniente y a las capacidades que ofrece que son suficientes para limitar funcionalidad del Sistema Operativo.

SICOP viene con otras herramientas necesarias para su funcionamiento que serán necesarios que se ejecuten antes de iniciarse.

Debido a experiencia, mediante prueba y error, se configuro en el kiosko para que SICOP se ejecute en 30 segundos (Ver Figura 2.45)



Mediante el kiosko se impidió: El acceso a las unidades locales o dispositivos mediante cuadros de diálogos de acceso a archivos o aplicaciones de ABRIR o GUARDAR; La reproducción automática al insertar un medio externo, como una unidad flash USB; Ciertas teclas del sistema: Key, Alt-Tab, Alt-Shift-Tab, Alt-Esc, Alt-Shift-Esc, Ctrl-Alt-Esc, Ctrl-Esc, Alt-F4, F1, and F3; Mostrar el escritorio de Windows y ejecuta el Lockdown seguro como el Shell de Windows; El acceso a diversas características de Windows a través de comandos de voz; La ayuda y el soporte para que no tengan acceso a aplicaciones externas o sitios web dentro de la pantalla de ayuda; La instalación de aplicaciones; El acceso a los dispositivos de almacenamiento USB extraíbles, como discos duros y unidades flash; La conexión de nuevos dispositivos USB a registrarse en el Sistema Operativo. Los que ya están conectados seguirán trabajando en su respectivo puerto; La opción de arranque en modo seguro; La secuencia de teclas Ctrl+Alt+Spr para impedir

el bloqueo, cambio de usuario, cerrar sesión, ver el administrador de tareas o apagar el Sistema Operativo (Ver Figura 2.46).

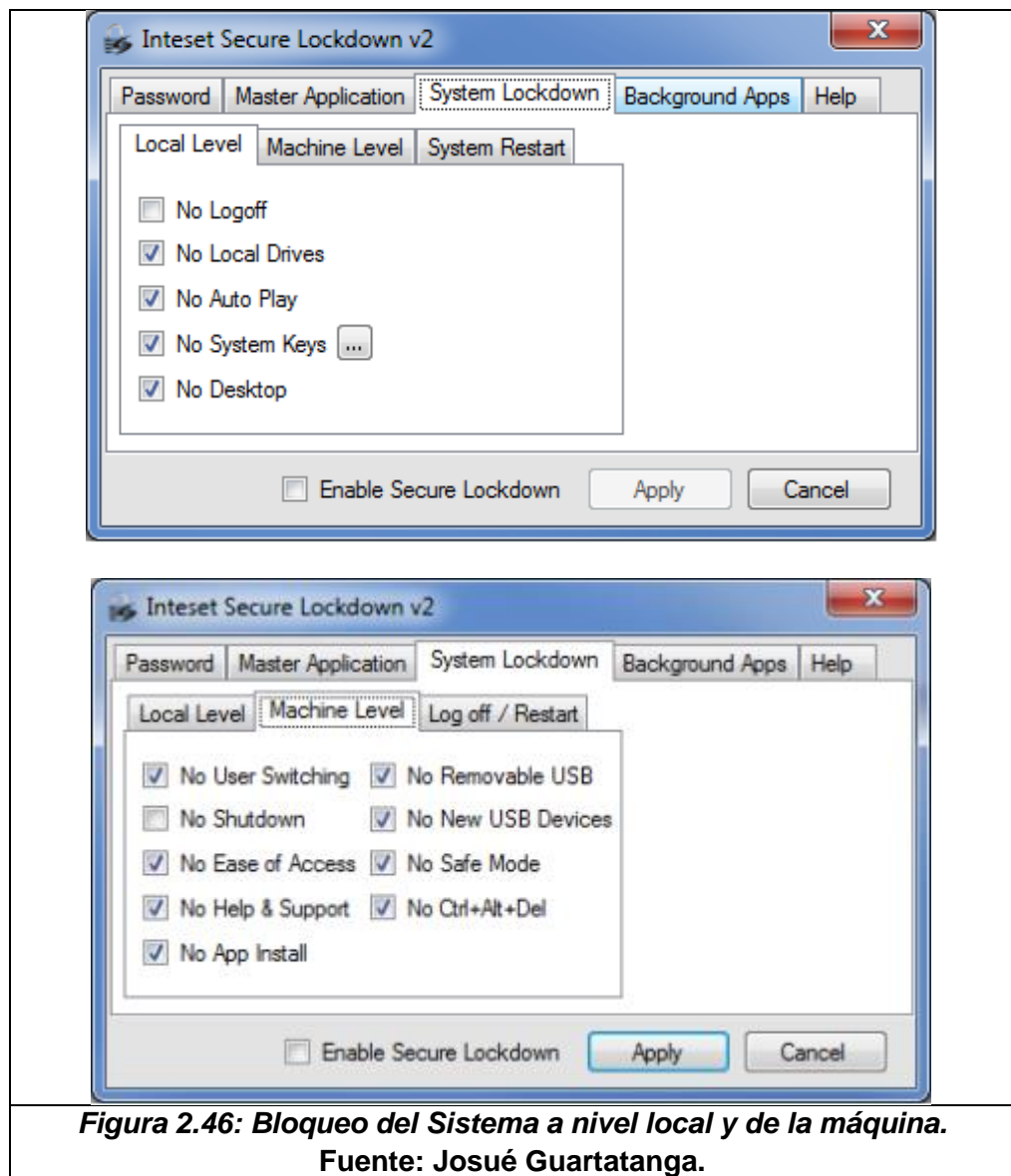


Figura 2.46: Bloqueo del Sistema a nivel local y de la máquina.
Fuente: Josué Guartatanga.

Para proteger el código de SICOP se utilizó un ofuscador, el cual realiza cambios no destructivos a la fuente con la finalidad de que sea difícil de entender. El ofuscador que se utilizó es Javascript Obfuscator [7].

CAPÍTULO 3

ANÁLISIS DE RESULTADOS.

3.1. Confidencialidad de los datos en la Base Patrulla.

Dado que los datos de importancia están encriptados en la base patrulla, los usuarios expertos no podrán tener acceso a ellos (Ver Figura 3.1), sino desde la aplicación SICOP, ya que no cuentan con el usuario y clave para entrar a la base, ni la llave para desencriptar.

De esta manera solo el personal policial que tenga credenciales para ingresar a SICOP podrá leer los datos (Ver Figura 3.2).

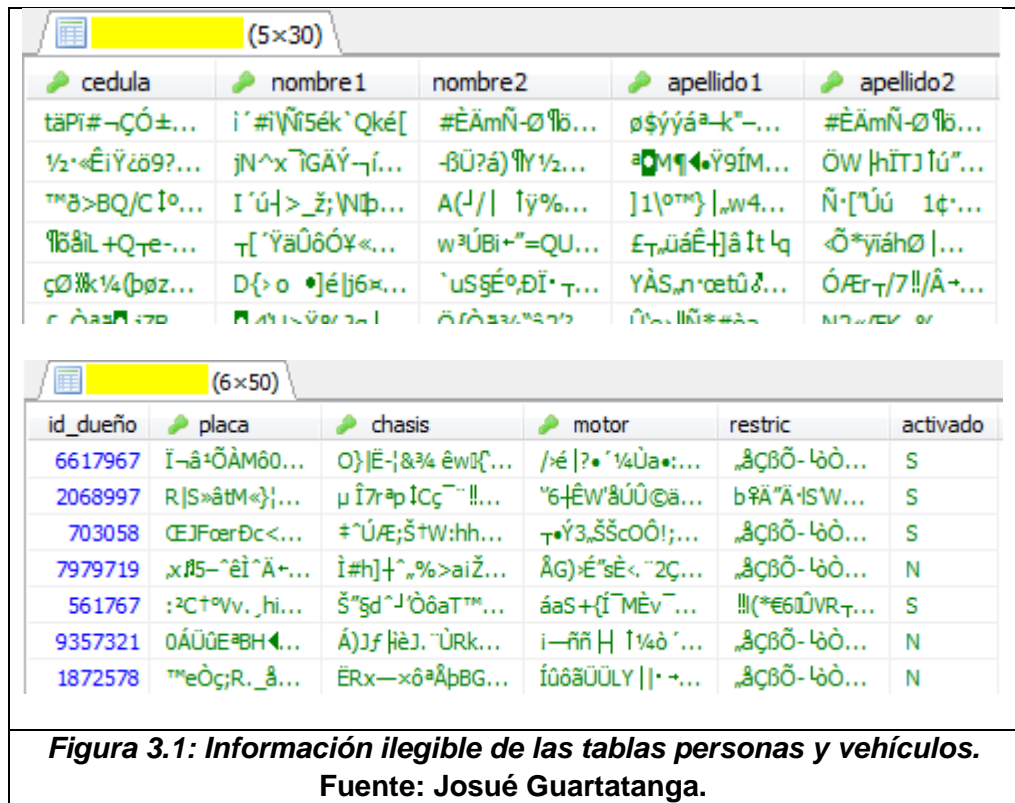


Figura 3.1: Información ilegible de las tablas personas y vehículos.
 Fuente: Josué Guartatanga.

The figure displays two screenshots of the 'Consola Interactiva Policial' interface. The top screenshot shows a search for a person using the document number 0916352537. The bottom screenshot shows a search for a vehicle using the license plate pxu0304. Both screenshots show the search criteria, the resulting data fields, and the status of the search.

Screenshot 1: Datos de consulta (Personas)

Datos de la Persona	
Tipo:	CEDULA
Documento:	0916352537
Nombre1:	JOSUE
Nombre2:	JEFFERSON
Apellido1:	GUARTATANGA
Apellido2:	ROBAYO
Estado civil:	SOLTERO
Lugar:	ECUADOR
Nacimiento:	ECUADOR
Fecha Nacimiento:	1984
Genero:	MASCULINO
Orden de Captura:	NO
Antecedentes:	NO

Screenshot 2: Datos de consulta (Vehiculos)

Datos Vehiculo	
Placa:	PXU0304
Modelo:	COLORADO
Marca:	CHEVROLET
Motor:	1GCDT136568134284
Chasis:	1GCDT136568134284
Clasevehi:	CAMIONETA
Tipovehi:	DOBLE CABINA
Color1:	ROJO
Restricción:	RESERVA DE DOMINIO
Rest. Vigente:	NO
Propietario:	JOHN RICHARD WELLS VALLEJO

Both screenshots include a footer with the text: FTJE1714863147 00:52:19 30/12/2015 © OCRW Todos los derechos reservados.

Figura 3.2: Información legible de las tablas personas y vehículos en SICOP.

Fuente: Josué Guartatanga.

3.2. Integridad y disponibilidad de los datos mediante procesos de sincronización Base Intermedia – Base Patrulla y Base Patrulla – Base Intermedia.

Para el ejemplo BASE INTERMEDIA- BASE PATRULLA escogeremos un registro de vehículo que está en la base intermedia pero no en la base patrulla.

El registro que escogimos fue el de la placa=GJL0284

Este vehículo con placa= GJL0284 tiene 4 restricciones. En la vista de vehículos de la base intermedia con cdg_res=1260844 tiene restricción de robado como se muestra en la siguiente imagen (Ver Figura 3.3).

cdg	placa	tipovehi	cdg_res	restric	activado	fecha1	fecha2
926589	GJL0284	(NULL)	283505	NO IDENTIFICADO(Y) SISTEMA COBOL	S	2013-04-03	2013-06-15
926589	GJL0284	(NULL)	1260844	ROBADO	S	2015-04-18	2013-06-15
1894054	GJL0284	STATION WAGON	760917	PRENDA COMERCIAL	S	2013-04-03	2013-04-03
1894054	GJL0284	STATION WAGON	760918	PRENDA COMERCIAL	S	2013-04-03	2013-04-03

Figura 3.3: Registro con restricción robado que está en la base intermedia y no en la base patrulla
Fuente: Josué Guartatanga.

En la base patrulla de la MW810 no se encuentra la restricción de robado (Ver Figura 3.4)







+ Policia Nacional del Ecuador	- Datos de consulta
+ Personas 	Chasis: MIG
- Vehiculos 	Clasevehi: --- Tipovehi: --- Color1: ---
Consulta por: <input type="text" value="Placa"/>  <input type="text" value="GJL0284"/>  <input type="button" value="Consultar"/>	Restricción: NO IDENTIFICADO(Y) SISTEMA COBOL Rest. Vigente: SI Restricción: PRENDA COMERCIAL Rest. Vigente: SI Restricción: PRENDA COMERCIAL Rest. Vigente: SI Restricción: NO IDENTIFICADO(Y) SISTEMA COBOL Rest. Vigente: SI Sin propietario / Datos en
+ Movimientos Migratorios 	
+ Armas 	

Figura 3.4: Registro de vehículo sin restricción de robo en SICOP por desactualización de la base patrulla
Fuente: Josué Guartatanga.

Se procedió a sincronizar la base patrulla desde SICOP y el resultado fue que el registro viajó a la tabla de vehículos de la base patrulla (Ver Figura 3.5).







+ Policia Nacional del Ecuador	- Datos de consulta
+ Personas 	Restricción: NO IDENTIFICADO(Y) SISTEMA COBOL
- Vehículos 	Rest. Vigente: SI
Consulta por: <input type="text" value="Placa"/>  <input type="text" value="GJL0284"/>  <input type="button" value="Consultar"/>	Restricción: PRENDA COMERCIAL
+ Movimientos Migratorios 	Rest. Vigente: SI
+ Armas 	Restricción: PRENDA COMERCIAL
	Rest. Vigente: SI
	Restricción: NO IDENTIFICADO(Y) SISTEMA COBOL
	Rest. Vigente: SI
	Restricción: ROBADO
	Rest. Vigente: SI
	Propietario: Sin propietario (Datos en revisión)

Figura 3.5: Registro de vehículo con restricción de robado en SICOP después de la sincronización

Fuente: Josué Guartatanga.

Para el ejemplo de sincronización BASE PATRULLA - BASE INTERMEDIA presentamos los registros de auditoría después de la sincronización. De esta manera se puede notar quien realizó la sincronización, la cantidad de registros por tabla que se procesaron, la máquina, la fecha y hora en que se realizó la sincronización y la geolocalización (Ver Figura 3.6).

id_sincro	usuario	maquina	tabla	fechamaxpat	fechamaxpat2	totreg	lati	lo...	timestamp
19750	ADMIN	ADMINISTRACION	Mov. migratorios	2015-04-07 ...	(NULL)	1765269	2015-08-20 15
19749	ADMIN	ADMINISTRACION	Personas	2015-07-27 ...	2015-07-27 ...	98873	2015-08-20 15
19748	ADMIN	ADMINISTRACION	Vehiculos	2015-08-10 ...	2015-08-09 ...	1790	2015-08-20 12
19747	ADMIN	ADMINISTRACION	Imp. salida	2015-07-16 ...	(NULL)	7004	2015-08-20 12
19746	ADMIN	ADMINISTRACION	Detenciones	2015-07-16 ...	(NULL)	2719	2015-08-20 12
19745	ADMIN	ADMINISTRACION	Ord. Captura	2015-07-16 ...	(NULL)	1991	2015-08-20 12

Figura 3.6: Registros de auditoría de sincronización Base Patrulla – Base Intermedia
Fuente: Josué Guartatanga.

Las capturas de los hits que se registran en la Base Patrulla, se guardan también en el Base Intermedia cuando se realice la sincronización (Ver Figura 3.7).

as en total								Siguiente
usuario	timestamp	lati	longi	placa	mac	uid		
1 sop...	2014-07-23 15:04:53	-0.178251666824023	-78.4942600001891	PCF0925	PCJ4821	20...		
2 sop...	2014-07-23 19:29:53	-0.160264999667803	-78.4779416670402	PBO0750	PCJ4821	20...		
3 sop...	2014-07-24 08:49:55	-0.188246666888396	-78.5113483329614	PEO0872	PCJ4821	20...		
4 sop...	2014-07-24 09:57:54	-0.188241666555405	-78.5114650001129	PRS0436	PCJ4821	20...		
5 sop...	2014-07-24 10:30:41	-0.188256666560968	-78.5113983333111	PPO0597	PCJ4821	20...		
6 sop...	2014-07-24 15:11:04	-0.188361666599909	-78.5114050000906	TCW0249	PCJ4821	20...		
7 sop...	2014-07-24 22:13:13	-0.170350000013908	-78.4821916669607	PBF3611	PCJ4821	20...		
8 sop...	2014-07-24 22:19:39	-0.170350000013908	-78.4821999996901	PBO8477	PCJ4821	20...		
9 sop...	2014-07-25 08:46:33	-0.170331666618586	-78.4822066664696	PBO8477	PCJ4821	20...		
10 sop...	2014-07-25 09:00:29	-0.170331666618586	-78.4822066664696	PBO8477	PCJ4821	20...		
11 sop...	2014-08-06 15:00:02	-1.06346166630586	-78.603999999106	PVR0155	PPNN-PC	20...		
12 sop...	2014-08-06 15:22:38	-1.22925333380699	-78.6079099997878	POO0874	PPNN-PC	20...		

Figura 3.7: Registros de auditoría de capturas hits en el servidor intermedio
Fuente: Josué Guartatanga.

3.3. Integridad del Sistema Operativo y Confidencialidad del código fuente de SICOP.

Con la restricción de funcionalidades que ofrece el kiosko, el usuario no tuvo acceso a:

- Las unidades locales, evitando la navegación por las carpetas del Sistema Operativo o de SICOP.
- La reproducción automática cuando insertó una unidad flash USB.
- Las combinaciones de ciertas teclas del sistema: Key, Alt-Tab, Alt-Shift-Tab, Alt-Esc, Alt-Shift-Esc, Ctrl-Alt-Esc, Ctrl-Esc, Alt-F4, F1, and F3.
- Al escritorio del Sistema Operativo.
- A las características de Windows mediante de comandos de voz.
- La ayuda y el soporte para que no pueda ejecutar aplicaciones externas o ir a sitios web dentro de la pantalla de ayuda.
- La secuencia de teclas Ctrl+Alt+Spr para impedir el bloqueo, cambio de usuario, cerrar sesión, ver el administrador de tareas o apagar el Sistema Operativo.

Mediante el ofuscamiento con la herramienta Javascript Obfuscator se puede notar que el archivo de código fuente MonitorPatrulla.js antes de ser ofuscado su tamaño original era 103 KB y después de ofuscar quedó en 29 KB con una compresión de ratio del 28.34% (Ver Figura 3.8).

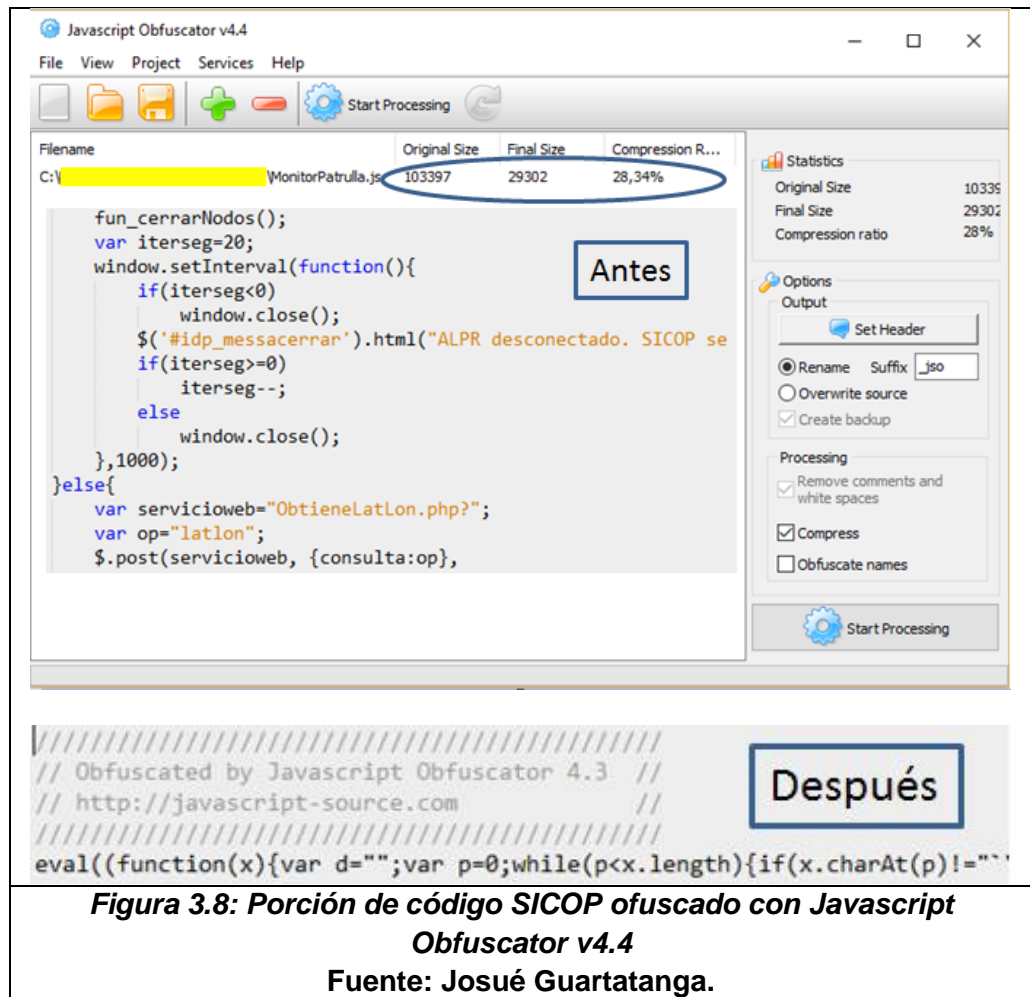


Figura 3.8: Porción de código SICOP ofuscado con Javascript Obfuscator v4.4

Fuente: Josué Guartatanga.

CONCLUSIONES Y RECOMENDACIONES.

CONCLUSIONES

1. El proceso de sincronización mantiene actualizada todas las tablas que SICOP necesita.
2. El proceso de encriptación de datos de las tablas de personas y vehículos ofrecen confidencialidad, evitando así que personas no autorizadas, que logren acceder a la Base Patrulla, pudieran robarla y sacar provecho.
3. El mantener registro de las actividades del agente y de los hits capturas de vehículos robados permiten evaluar el desempeño del personal policial.

4. La restricción de funcionalidades al Sistema Operativo en donde SICOP se ejecuta permitió que el agente policial rinda más en las horas laborables, reduciendo el tiempo de horas de ocio.

RECOMENDACIONES

1. Se recomienda optimizar la configuración del motor de base de datos para reducir tiempo al encriptar datos de tablas que están alrededor de los 5 Gb, para la tabla de personas y 1Gb para la tabla de vehículos.
2. Se recomienda particionar cualquier proceso que tome mucho tiempo. Por ejemplo en el caso del script de encriptación de las tablas de personas y vehículos se pudiera utilizar límites en el query, y de esta manera encriptar por bloques.
3. Para aumentar la complejidad al proceso de encriptación con el algoritmo AES, se puede utilizar como clave un hash de un texto secreto. Por ejemplo el hash puede ser con el algoritmo SHA1 en MySql.

BIBLIOGRAFÍA

- [1] Wikipedia, Advanced Encryption Standard, [En línea]. Available: https://es.wikipedia.org/wiki/Advanced_Encryption_Standard. [Último acceso: noviembre 2013].
- [2] Talend Open Studio, Data Integration, [En línea]. Available: <http://www.talend.com/>. [Último acceso: febrero 2013].
- [3] Wikipedia, Secure Hash Algorithm, [En línea]. Available: https://es.wikipedia.org/wiki/Secure_Hash_Algorithm. [Último acceso: noviembre 2013].
- [4] Glassfish, quick-start-guide: Deploying Applications by Using the Administration Console, [En línea]. Available: <https://glassfish.java.net/docs/4.0/quick-start-guide.pdf>. [Último acceso: marzo 2013].
- [5] MySQL, Reference Manual :: 13.2.8 REPLACE Syntax, [En línea]. Available: <http://dev.mysql.com/doc/refman/5.7/en/replace.html>. [Último acceso: diciembre 2013].
- [6] Inteset Systems, Windows Lockdown, [En línea]. Available: <http://shop.inteset.com/lock-down-windows-with-inteset-secure-lockdown>. [Último acceso: Febrero 2014].
- [7] Javascript-Source, Ofuscador de código javascript, [En línea]. Available: <http://www.javascript-source.com/>. [Último acceso: agosto 2013].
- [8] Blueliv, De cómo evadir las restricciones de seguridad establecidas en un kiosko, [En línea]. Available: <https://www.blueliv.com/research/de-como-evadir-las-restricciones-de-seguridad-establecidas-en-un-kiosko-2/>. [Último acceso: marzo 2014].
- [9] elhacker, Atajos de teclado en Windows, [En línea]. Available: <http://www.elhacker.net/atajos-teclado-windows-xp.html>. [Último acceso: marzo 2014].

GLOSARIO.

SICOP	Sistema Integral de Consultas Policiales.
C.N.T.	Corporación Nacional de telecomunicaciones.
Base 15	Base de datos de la Policía Nacional en la que consta los datos de: Las personas con sus detenciones y órdenes de captura; Los vehículos asociados a sus respectivos dueños; Los movimientos migratorios de ecuatorianos, y de los extranjeros que llegaron al país.
Base Intermedia	Es la base de datos resultante de la depuración de la Base 15 mediante un proceso de sincronización en donde se filtran registros con datos inconsistentes.
Base Intermedia – Base Patrulla	Tipo de sincronización que se ejecuta en SICOP donde registros de la Base Intermedia pasan a la Base Patrulla.
Base Patrulla – Base Intermedia	Tipo de sincronización que se ejecuta en SICOP donde registros de la Base Patrulla pasan a la Base Intermedia.