Escuela Superior Politécnica del Litoral.

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO Y PROTOTIPO DE UNA RED COLABORATIVA USANDO UN SISTEMA DE ALERTAS TECNOLÓGICAS CON EL FIN DE APLACAR EL SECUESTRO EXPRESS CON RETIRO DE CAJEROS AUTOMATICOS"

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN SISTEMAS INFORMACIÓN

Presentada por:

BRENDA VANESSA CARRILLO ARGUELLO
MARÍA FERNANDA ESPINOZA INFANTE
MARTHA LUCIA TACURI MOROCHO

Guayaquil – Ecuador

2011

AGRADECIMIENTO

A Dios,
Por ser nuestro guía en el camino y
darnos fortaleza para seguir cumpliendo cada
una de nuestras metas.

A nuestra Familia,
Por su apoyo incondicional y sus consejos en cada
una de las etapas de nuestra vida.
.

DEDICATORIA

A nuestra familia y amigos,
por la confianza y el apoyo incondicional.

TRIBUNAL DE SUSTENTACION

Ing. Alfonso Aranda.
PROFESOR DEL SEMINARIO

Ing. Washington Medina.
PROFESOR DELEGADO DEL DECANO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Grado, nos corresponde exclusivamente y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

Brenda Vanessa Carrillo Arguello

María Fernanda Espinoza Infante

Martha Lucía Tacuri Morocho

RESUMEN

Este proyecto tiene como finalidad ofrecer un esquema de protección adicional a las entidades que cuentan con cajeros automáticos de tal forma que sus clientes no sean víctimas de personas inescrupulosas que afecten sus cuentas bancarias.

Esta idea surge con la necesidad de complementar el sistema actual de seguridad de los cajeros automáticos en cuanto al manejo de una sola clave para realizar sus transacciones.

Se plantea un esquema de manejo de dos tipos de claves diferentes para realizar las respectivas transacciones dependiendo de las diferentes circunstancias en las que se encuentre el usuario, la clave normal utilizada en el proceso normal de un cajero, la clave de auxilio utilizada cuando el delincuente exige retirar dinero de las cuentas personales a través de un cajero. [1]

---

[1] CLAVE DE AUXILIO: Es una clave adicional compuesta de cuatro dígitos creada para alertar a la Entidad de Seguridad sobre un posible Secuestro Express con retiro de cajero automático.

Para la elaboración de este prototipo se creará un ambiente en el cual intervengan todas las entidades involucradas en una transacción bancaria y el mecanismo de auxilio que se pretende involucrar.

Dicha señal de alerta puede ser generada en dos situaciones: si la víctima ingresa la clave de auxilio en el cajero, o si la entidad de seguridad recibe una llamada indicando que existe un secuestro express con modalidad de retiro obligado de dinero en proceso, en ésta segunda situación se deberá verificar la veracidad de dicha llamada por medio de la cédula de Identidad y realizando una pregunta al azar a través del cajero para corroborar que en efecto dicho usuario es víctima del delito antes mencionado y que no se trata de una llamada falsa usada por personas malintencionadas para hacer daño ya sea a la persona o a la Institución.

Por lo tanto este trabajo sienta las bases para incentivar a las entidades financieras en el aporte a soluciones que mejoren su seguridad y la de sus clientes brindándoles confianza y seguridad.

ÍNDICE GENERAL

ABREVIATURAS

Las abreviaturas que se utilizan en este trabajo son las siguientes:

TTL	TRANSPORT LAYER SECURITY.
SSL	SECURITY SOCKET LAYER.
HTTP	Hyper Text Transfer Protocol.
XML	Extensible Markup Language (Lenguaje de Marcas Extensible).
CSCG	Corporación para la Seguridad Ciudadana de Guayaquil.
SCM	Services Control Manager.
SSLeay	Implementación libre del Protocolo Secure Sockets Layer de Netscape.
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
OPEN SSH	OPEN SECURE SHELL.
SPX	Sequenced Packet Exchange (Intercambio de Paquetes Secuenciales).
NetBEUI	Protocolo utilizado en las antiguas redes.
NetBIOS	Engloba un conjunto de protocolos de niveles de sesión.
IPX	Internet Packet Exchange.
SMTP	Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo).
IETF	Internet Engineering Task Force.
SSH	Secure Shell (Interprete de Comandos Seguros).

SAS	Security Alarm System.
W3C	World Wide Web Consortium (Consorcio de la Web o Telaraña Mundial).

ÍNDICE DE FIGURAS

INDICE DE TABLAS

Pág.

ANEXOS

Anexo A Código de Verificación de claves.

Anexo B Código de Recepción y Envío de Información**.**

Anexo C Código de Ingreso de Denuncia.

Anexo D Código de Envío de Información al Banred**.**

Anexo E Código para grabar Acciones Tomadas**.**

Anexo F Lista de Precios Hosting**.**

Anexo G Pantalla Principal del Cajero**.**

Anexo H Pantalla Principal del Módulo perteneciente a la Corporación "Ingreso de Usuario".

Anexo I Pantalla Principal del Módulo perteneciente a la Corporación "Recepción de los Datos de la Alarma**".**

Anexo J Pantalla Principal del Módulo perteneciente a la Corporación "Registro de Denuncia"**.**

Anexo K Pantalla Principal del Módulo perteneciente a la Corporación "Denuncias"**.**

INTRODUCCIÓN

Actualmente en nuestro país se han incrementado los asaltos bajo la modalidad de Secuestros Express, siendo Guayaquil una de las ciudades más afectadas por este problema debido a muchos factores como la falta de empleo, el incremento del costo en la canasta familiar, decadencia de valores morales, etc.

El secuestro express generalmente se ejecuta sin seguimiento previo, como ocurre en los otros secuestros; uno de los objetivos principales de las personas que incurren en dicho delito es el de exigir retiros en cajeros automáticos de todas las cuentas personales de las víctimas muchas veces estas personas son retenidas más de un día para poder retirar todo el dinero de sus cuentas bancarias.

Estudios realizados sobre las denuncias de delitos contra las personas han demostrado que en promedio se realiza un secuestro express cada 9 horas, cabe recalcar que esta cifra se ha mantenido durante los últimos meses bajo la misma modalidad (utilizando la conocida red de taxi amigos dentro de la urbe o el de ser interceptado por otro/s vehículo/s y secuestrado), motivo por el cual el presente trabajo brindará la posibilidad a las personas que son víctimas de tal delito de retirar dinero de sus cuentas personales bajo un monto mínimo de tal

manera que los ahorros de sus cuentas bancarias no sean afectados en gran medida.

También se contará con la ayuda de las fuerzas policiales para que dicho delito no quede impune debido a que la comunicación será fiable entre la Institución Bancaria y la Entidad de Seguridad.

CAPÍTULO I

1. Planteamiento del Problema

En este capítulo definimos el problema identificado, en el cual nos basamos para el desarrollo de este proyecto, además se describen los objetivos y el alcance.

1.1 ESTRUCTURA DEL DOCUMENTO

En el capítulo 2 se describen los fundamentos teóricos usados en nuestro proyecto.

El capítulo 3 se realiza el análisis y el diseño de toda la solución a implementar para el desarrollo del proyecto. **En el capítulo 4**, se realiza una descripción detallada de los pasos seguidos para la implementación del proyecto basado en tecnologías de seguridad. Finalmente, **En el capítulo 5** se realiza el análisis FODA, el de Factibilidad y de Materialización del proyecto en el marco de la solución a la problemática planteada, así como también se especifican las conclusiones y recomendaciones de este trabajo.

1.2 DEFINICIÓN DEL PROBLEMA

La inseguridad al momento de utilizar un cajero automático es el diario vivir para todos los usuarios que necesitan realizar transacciones, tales como consultas de saldos, retiro en efectivo, etc. Muchos individuos inescrupulosos aprovechan la vulnerabilidad de los usuarios para sustraerle todo el dinero que posean en sus cuentas bancarias, con el tan conocido estilo de robo “Secuestro Express”, donde la víctima debe ingresar su clave personal en el cajero automático y sacar un monto máximo por día, en muchos casos no son liberados hasta vaciar totalmente sus cuentas, además que ningún ente de seguridad se percata del delito hasta que es denunciado por la víctima. Es por esto que surge la necesidad de integrar un sistema que al acontecer este tipo de delito, se dé un aviso de alerta a una entidad de Seguridad.

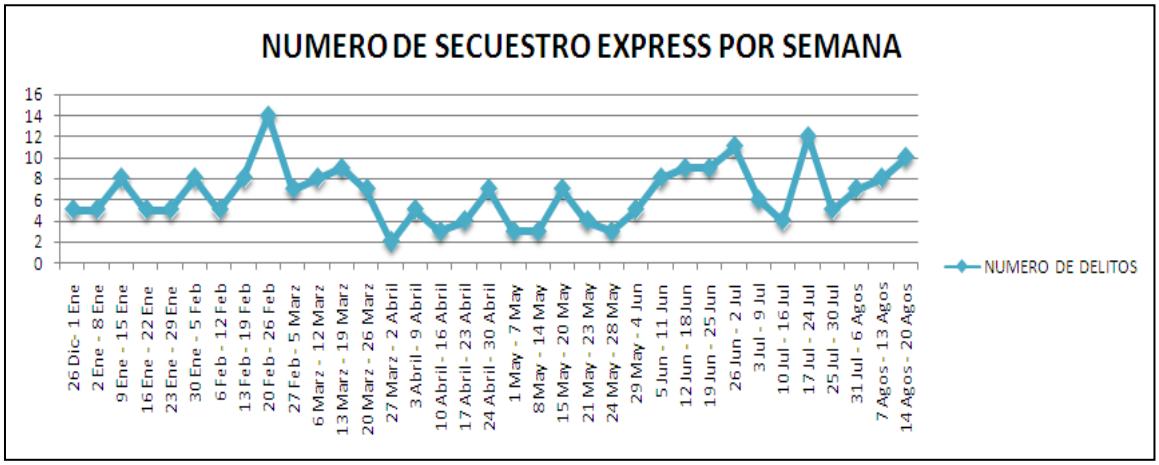


Figura 1 *Secuestro Express por semana durante el año 2010.* ***Fuente:*** *www.icm.espol.edu.ec/delitos.*

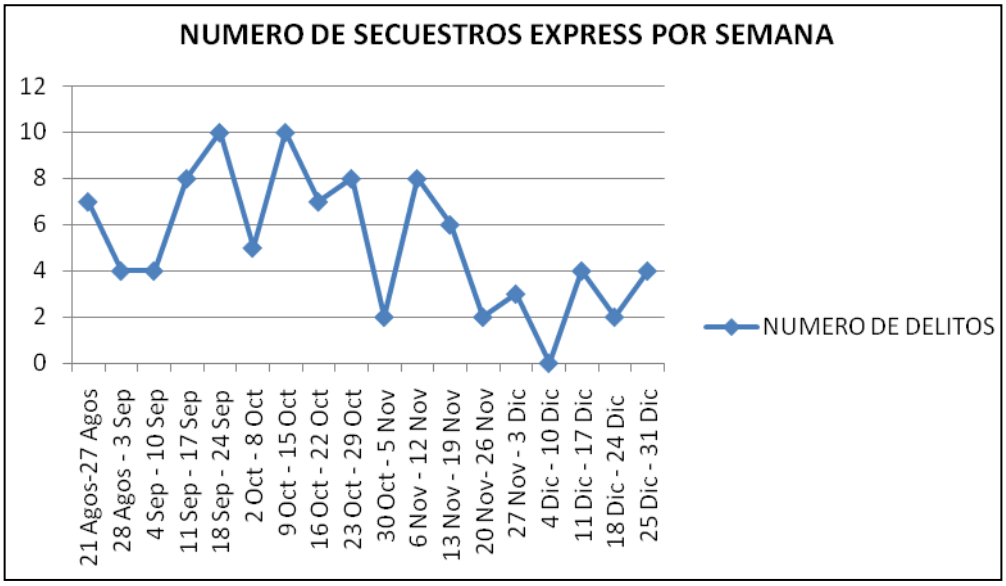


Figura 1.1 *Secuestro Express por semana durante el año 2010, desde Agosto hasta finales del año*

Fuente: www.icm.espol.edu.ec/delitos.

1.3 OBJETIVOS

En esta sección se plantean el alcance y los objetivos, tanto generales como específicos que tiene el proyecto.

1.3.1 Objetivo General

El presente trabajo tiene como objetivo plantear una solución para las instituciones que brindan el servicio de cajeros automáticos con el afán de minimizar los secuestros express con modalidad de retiro obligado de dinero.

1.3.2 Objetivos Específicos

Para llegar al objetivo general se plantearon los siguientes objetivos específicos:

- Diseñar una red colaborativa entre una Entidad Financiera y una Entidad de Seguridad.
- Elaborar análisis FODA.
- Implementar un proceso para el envío y recepción de alertas.
- Generar reportes y gráficos estadísticos.

1.3.3 Alcance

Debido a que las Entidades Bancarias ofrecen sus servicios de cajero automático a nivel nacional, nuestro sistema será capaz de adaptarse aquellos requerimientos y necesidades que el Banco amerite, cabe recalcar que la Entidad de Seguridad con la que vamos a realizar nuestro proyecto la CSCG (Corporación para la Seguridad Ciudadana de Guayaquil), es solo a nivel de la ciudad de Guayaquil, es por esa razón que nuestro sistema esta creado de tal forma que puede trabajar con las diferentes Entidades que proveen seguridad en todo el país.

CAPÍTULO 2

2. Marco Teórico

2.1 WEB SERVICE

Se denomina así a un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones, donde los equipos envían parámetros al servidor (que es donde está alojado el web Service) y éste responderá la petición. Son muy prácticos debido a que son independientes de las aplicaciones.

2.1.1 Requisitos de un Web Service

2.1.1.1 Interoperabilidad: Un servicio remoto debe permitir su utilización por clientes de otras plataformas.

2.1.1.2 Amigabilidad con Internet: La solución debe poder funcionar para soportar clientes que accedan a los servicios remotos desde internet.

2.1.1.3 Interfaces fuertemente "tipadas"[1]: No debería haber ambigüedad acerca del tipo de datos enviados y recibidos desde un servicio remoto. [2]

---

[2] Tipadas: el tipo de objeto que debe contener es conocido en tiempo de compilación, por lo que el propio compilador es capaz de emitir un mensaje de error en caso de asignar un tipo incorrecto.

2.1.1.4 Posibilidad de aprovechar los estándares de Internet existentes: La implementación del servicio remoto debería aprovechar estándares de Internet existentes tanto como sea posible y evitar reinventar soluciones a problema que ya se han resuelto.

2.1.1.5 Soporte para cualquier lenguaje: La solución no debería ligarse a un lenguaje de programación en particular, un cliente debería ser capaz de implementar un nuevo servicio Web existente independientemente del lenguaje de programación en el que se haya escrito.

2.1.1.6 Soporte para cualquier infraestructura de componente distribuida: No se debería requerir el comprar, instalar o mantener una infraestructura de objetos distribuidos, solo construir un nuevo servicio remoto utilizando un servicio existente. Los protocolos subyacentes deberían proporcionar un nivel base de comunicación entre infraestructura de objetos distribuidos existentes tales como DCOM y CORBA.

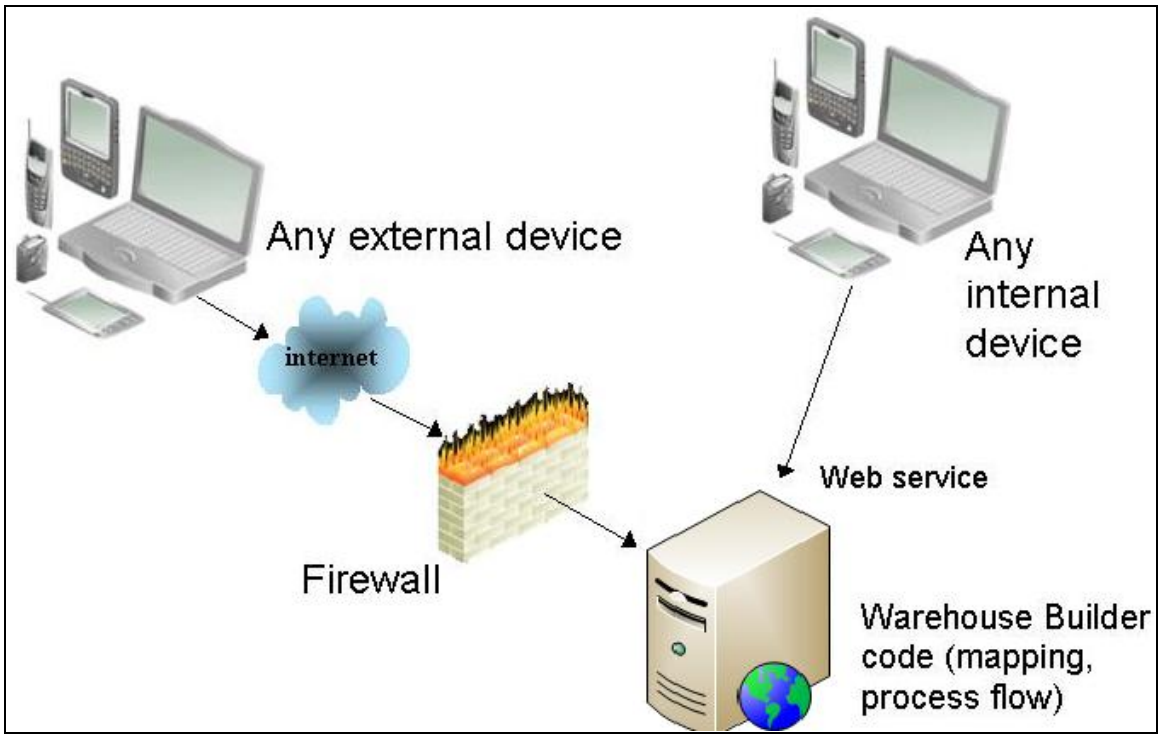


Figura 2 *Diseño Web Service.*

Fuente: *Autores.*

2.1.2 Bloques Constructivos

2.1.2.1 Descubrimiento

La aplicación cliente que requiere acceder a la funcionalidad que expone un Servicio Web necesita una forma de resolver la ubicación de servicio remoto. Se logra mediante un proceso llamado, **descubrimiento** (discovery). El descubrimiento se puede proporcionar mediante un directorio centralizado así

como por otros métodos como **ad hoc (**no hay un nodo central, todos los dispositivos están en igualdad de condiciones**)**.

2.1.2.2 Descripción

Una vez que se ha resuelto el extremo de un servicio Web dado, el cliente necesita suficiente información para interactuar adecuadamente con el mismo. La descripción de un servicio Web implica meta datos estructurados sobre la interfaz que intenta utilizar la aplicación cliente así como documentación escrita sobre el servicio Web incluyendo ejemplo de uso. Un componente DCOM expone meta datos estructurados sobre sus interfaces mediante una biblioteca de tipo (typelib). Los meta datos dentro de una typelib de componente se guardan en un formato binario propietario a los que se accede mediante una interfaz de programación de aplicación (API) propietaria.

2.1.2.3 Formato del mensaje

Para el intercambio de datos, el cliente y el servidor tienen que estar de acuerdo en un mecanismo común de codificación y formato de mensaje.
El uso de un mecanismo estándar de codificar los datos asegura que los datos que codifica el cliente los interpretará correctamente el servidor. En DCOM los mensajes que se envían entre un cliente y un servidor tienen un formato definido por el protocolo DCOM Object RPC (ORPC).

2.1.2.3.1 Soap

Es un protocolo que define cómo realizar la comunicación entre cliente y servidor, es decir cómo debemos codificar las llamadas a los métodos de un Web Service, y cómo debe el Web Service codificar el resultado para que nosotros lo podamos interpretar. Estos mensajes son los que transportarán los protocolos de transporte, por lo general, **HTTP**.

2.1.2.3.2 Encriptación de mensajes SOAP

Los mensajes que utiliza un Web Service para comunicarse entre dos entidades son mensajes SOAP[3] en XML, estos mensajes basados en la descripción XML tienen la característica de tener sus propias definiciones de tipos de datos y manejar la información a través de tags. Cuando nos referimos a encriptar estamos hablando de cambiar la presentación de la información de tal forma que no sea entendible para una persona que pueda leer este mensaje en caso de que lo intercepte en medio de una comunicación.

[3] SOAP al principio significaba Simple Object Access Protocol, luego fue Service Oriented Architecture Protocol, pero actualmente es simplemente SOAP

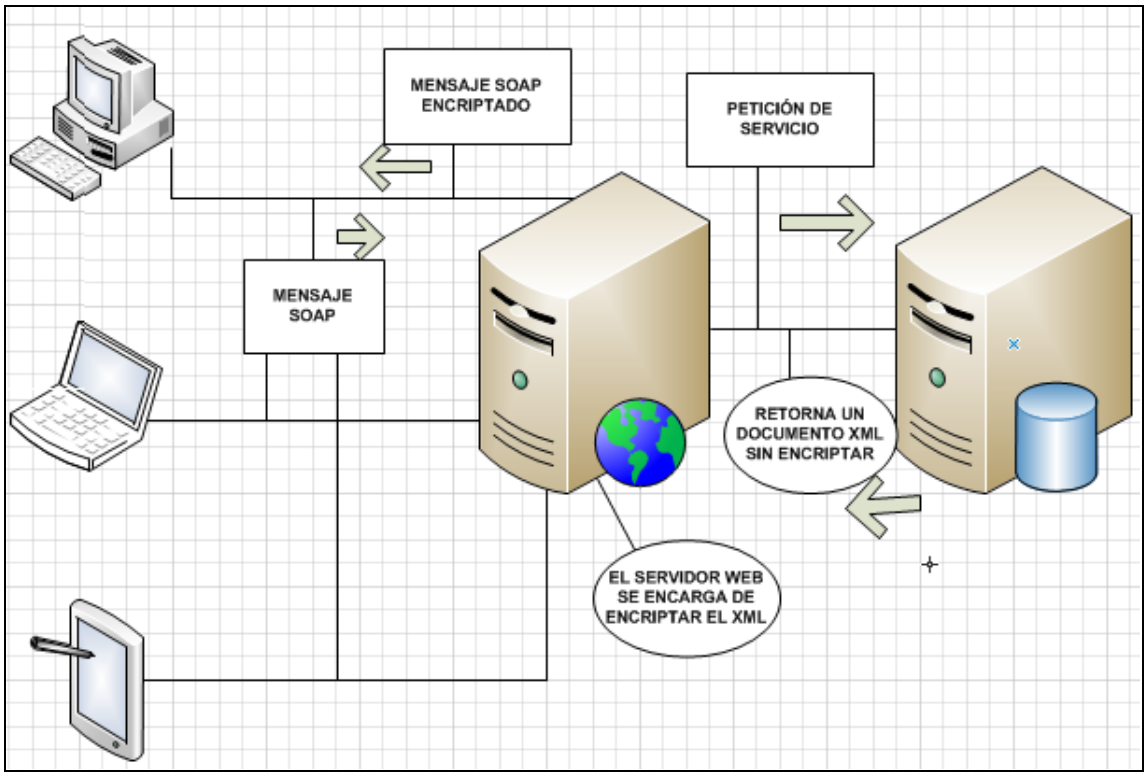


Figura 2.1 *Flujo de los mensajes en una comunicación segura.*

Fuente: *Autores.*

2.1.2.4 Codificación

Los datos que se trasmiten entre el cliente y el servidor necesitan codificarse en un cuerpo de mensaje. DCOM utiliza un esquema de codificación binaria para serializar los datos de los parámetros que se intercambian entre el cliente y el servidor.

2.1.2.4.1 Encriptación del XML

El protocolo de encriptación para un archivo XML dice que una parte del mensaje se puede encriptar cuando se hace uso de este proceso, el algoritmo de encriptación se encarga de tomar parte del mensaje y reemplazar la parte del mensaje y cambiarlo por el resultado del algoritmo.

2.1.2.4.2 Tipos de encriptación

Los tipos de encriptación se dividen en dos:

- **Simétricas:** Este tipo de encriptación se hace con el uso de llaves simétricas, esto quiere decir que el cliente y el servidor se comunican con una llave compartida que viaja a través de un mensaje seguro, este tipo de comunicación se aplica por ejemplo en Kerberos, el cual haciendo uso de un servidor de autenticación que recibe la solicitud de un cliente A haciendo la petición de querer comunicarse con el cliente B, genera una llave simétrica entre A - B y con esta llave ambos clientes entran a una comunicación segura.
- **Asimétricas:** este tipo de encriptación se basa en el uso de llaves privadas y públicas se usa para la comunicación a través del Internet.

  Por ejemplo SSL se basa en el uso de este tipo de encriptación, la llave pública se utiliza para encriptar el mensaje, pero esta no se puede utilizar

para desencriptar para esto se hace uso de la llave privada la cual solo la conoce cada poseedor.

2.1.2.5 Transporte

Una vez que se ha dado formato al mensaje y se han serializado los datos en el cuerpo del mensaje, se debe transferir entre el cliente y el servidor utilizando algún protocolo de transporte. DCOM dispone de varios protocolos propietarios como TCP, SPX, NetBEUI y NetBIOS sobre IPX.

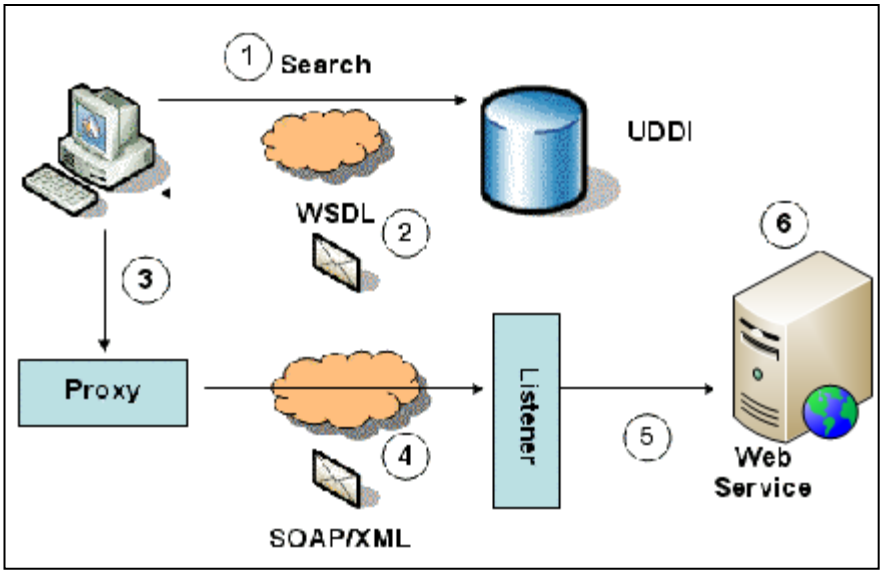


Figura 2.2 *Procesos y Tecnología de los Servicios Web*

Fuente: *http://www.moisesdaniel.com/es/wri/wsepsu.htm*

2.1.3 Ventajas de los servicios web

Aportan interoperabilidad entre aplicaciones de software independientemente de sus propiedades o de las plataformas sobre las que se instalen. Los servicios Web fomentan los estándares y protocolos basados en texto, que hacen más fácil acceder a su contenido y entender su funcionamiento. Al apoyarse en HTTP, los servicios Web pueden aprovecharse de los sistemas de seguridad firewall sin necesidad de cambiar las reglas de filtrado.

Permiten que servicios y software de diferentes compañías ubicadas en diferentes lugares geográficos puedan ser combinados fácilmente para proveer servicios integrados.

Permiten la interoperabilidad entre plataformas de distintos fabricantes por medio de protocolos estándar y abiertos. Las especificaciones son gestionadas por una organización abierta, la W3C, por tanto no hay secretismos por intereses particulares de fabricantes concretos y se garantiza la plena interoperabilidad entre aplicaciones.

En la ***Figura 2.3*** podemos apreciar como se realiza la interacción entre diferentes clientes, los servidores Web y sus distintas herramientas accesando todos a los distintos Servicios Web.

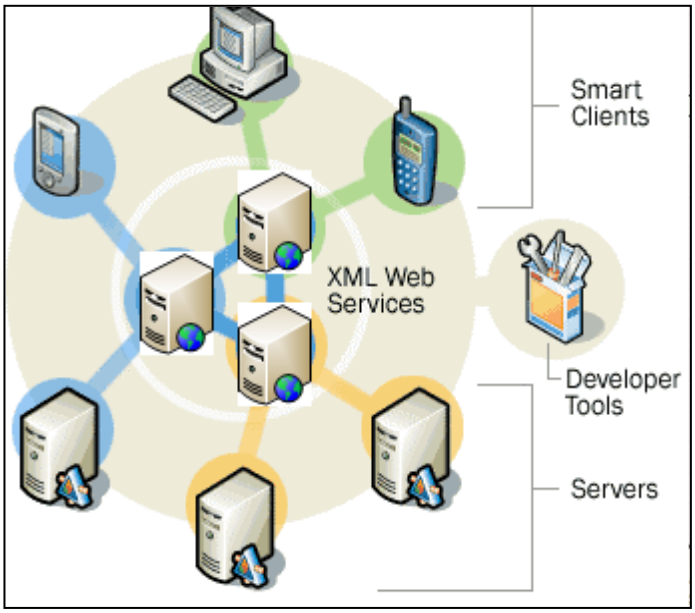


Figura 2.3 *Representación de la interacción entre varios servicios Web y diferentes clientes.*

Fuente: *http://www.moisesdaniel.com/es/wri/wsepsu.htm*

2.2 PUNTOS DÉBILES DE LOS WEB SERVCE

En los actuales momentos existen muchos desarrollos de web Service tanto empresariales como individuales, pero todavía existen muchas preguntas por responder y por lo tanto muchos puntos débiles que fortalecer.

2.2.1 Seguridad/Privacidad

Se debe asegurar que los usuarios solo tengan acceso a roles específicos, previniendo el acceso de personas no autorizadas. Este problema no lo aborda

SOAP puntualmente, ya que se han desarrollado herramientas adicionales para asegurar esto, como el uso de certificados digitales.

2.2.2 Enrutamiento/Confiabilidad/Transaccionalidad

Se deben desarrollar métodos que permitan monitorear el paso de mensajes y se pueda garantizar que en el caso de que una transacción falle, esta se pueda devolver (rollback[4]). Hasta que esto pueda ser posible, la capacidad de un Web Service es limitada.

2.2.3 Manejo Transaccional

Este es uno de los puntos con mayor importancia cuando se habla de un Web Service, ya que al no mantener un estado ni poder manejar sesiones, es imposible saber como manejar una transacción distribuida y como deshacerla en el caso de que un error ocurra. Muchas empresas desarrolladoras han abordado este tema, y han desarrollado herramientas pero W3C, no ha demostrado iniciativa en desarrollar un estándar para el desarrollo de un manejador transaccional, lo que implica que cada desarrollo es diferente y por lo tanto específico a la solución.

---

[4] Rollback: Revertir una transacción. Por ejemplo, en una Base de Datos, una transacción se compone de una o más operaciones. Cuando se quiere revertir el resultado de dichas operaciones (de una transacción), entonces se ejecuta el comando Rollback.

2.3 PROTOCOLO SEGURO: TLS

Para intentar corregir las deficiencias en SSL se buscó un nuevo protocolo que permitiera transacciones seguras por internet, sobre todo teniendo en cuenta que SSL es propiedad de la empresa Netscape. El resultado de esta búsqueda fue el protocolo TLS, el cual permite una compatibilidad total con SSL.

TLS es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor. Encripta la comunicación entre servidor y cliente mediante el uso de llaves y algoritmos de encriptación.

2.3.1 TLS: Sus fases

Posee tres fases:

2.3.1.1 Negociación: Criptografía de clave pública para cifrado simétrico con funciones hash.

2.3.1.2 Autenticación y Claves: Los extremos se autentican mediante certificados digitales e intercambian las claves para el cifrado, según la negociación.

2.3.1.3 Transmisión Segura: los extremos pueden iniciar el tráfico de información cifrada y auténtica.

2.3.2 Objetivos del Protocolo TLS

Los objetivos del protocolo son varios:

2.3.2.1 Seguridad criptográfica. El protocolo se debe emplear para establecer una conexión segura entre dos partes.

2.3.2.2 Interoperabilidad. Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.

2.3.2.3 Extensibilidad. El protocolo permite la incorporación de nuevos algoritmos criptográficos.

2.3.2.4 Eficiencia. El protocolo incluye un esquema de caché de sesiones para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

2.3.3 Funcionamiento Protocolo TLS

El protocolo está dividido en dos niveles:

- Protocolo de registro TLS (*TLS Record Protocol*).
- Protocolo de mutuo acuerdo TLS (*TLS Handshake Protocol*).

El de más bajo nivel es el ***Protocolo de Registro***, que se implementa sobre un protocolo de transporte fiable como el TCP. El protocolo proporciona seguridad en la conexión con dos propiedades fundamentales:

2.3.3.1 La conexión es privada. Para encriptar los datos se usan algoritmos de cifrado simétrico. Las claves se generan para cada conexión y se basan en un secreto negociado por otro protocolo (como el de mutuo acuerdo). El protocolo también se puede usar sin encriptación.

2.3.3.2 La conexión es fiable. El transporte de mensajes incluye una verificación de integridad.

El *Protocolo de mutuo acuerdo,* proporciona seguridad en la conexión con tres propiedades básicas:

- La identidad del interlocutor puede ser autentificada usando criptografía de clave pública. Esta autentificación puede ser opcional, pero generalmente es necesaria al menos para uno de los interlocutores.
- La negociación de un secreto compartido es segura.
- La negociación es fiable, nadie puede modificar la negociación sin ser detectado por los interlocutores.

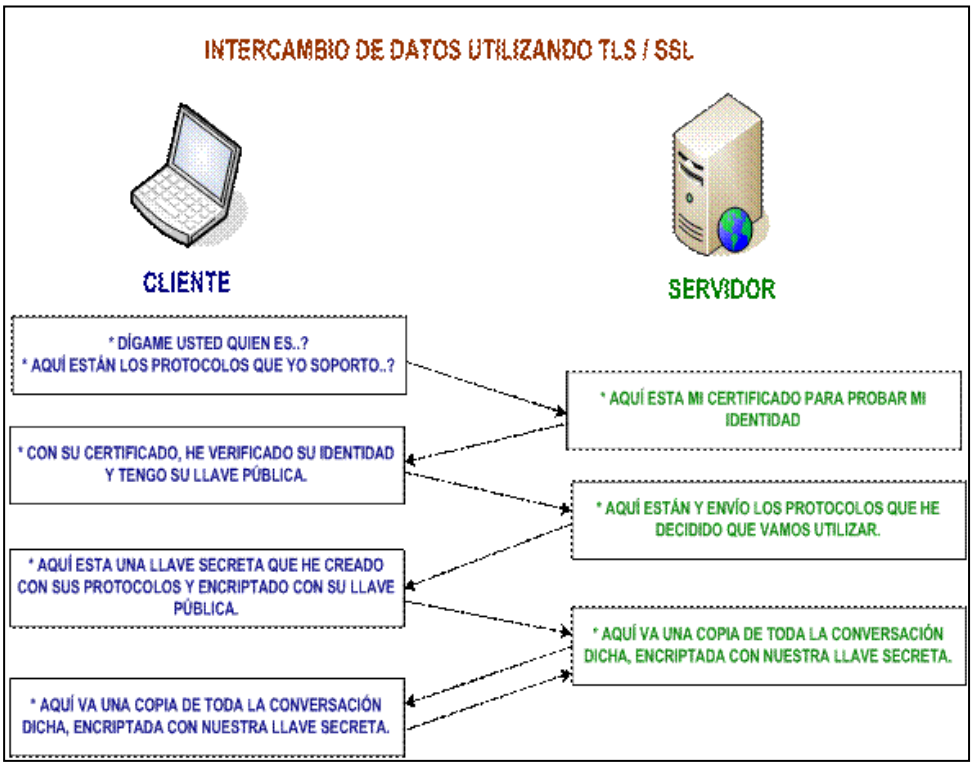


Figura 2.4 *Intercambio de datos usando TLS/SSL.*

Fuente:

2.3.4 Aplicaciones

HTTP sobre SSL/TLS es HTTPS, ofrece seguridad a páginas WWW para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

SSH utiliza SSL/TLS por debajo. SMTP y NNTP pueden operar también de manera segura sobre SSL/TLS.

2.3.5 Implementaciones.

Existen diferentes implementaciones, como por ejemplo:

Open SSL: una implementación de código abierto, la más utilizada. Es un proyecto desarrollado por la comunidad Open Source para libre descarga y está basado en SSLeay. Ayudan al sistema a implementar el SSL/TLS ofreciéndole un robusto paquete de herramientas de administración y librerías de criptografía que pueden ser usadas para OpenSSH y navegadores web (acceso seguro a HTTPS).

GnuTLS: una implementación de código abierto con licencia compatible con GPL.

JSSE: una implementación realizada en el Java incluida en el Java Runtime Environment.

2.4 UNA ENTIDAD - DOS CLAVES

Es un término que consiste en que el ID de un usuario puede tener dos claves.

2.5 EXPANDIBILIDAD

Nuestro sistema puede ser utilizado en:

- Seguridad en cajas fuertes con claves digitales.

- Seguridad en casa, empresas y negocios.
- Seguridad de alertas digitales en vehículos.
- Seguridad sobre una red GPRS en el servicio de Transporte Público.

CAPÍTULO 3

3. ANÁLISIS Y DISEÑO

3.1 ANÁLISIS DE INTEGRACIÓN DE RED COLABORATIVA[5]

Para formar una red colaborativa es necesaria la intervención del Sistema bancario con la CSCG (Corporación para la Seguridad Ciudadana de Guayaquil, es una entidad creada en derecho privado y sin fines de lucro, que participa en acción social y cívica que opera en la ciudad de Guayaquil), esto se realizará a través de nuestro módulo SAS (Security Alarm System).

En la ***Figura 3*** hemos detallado el funcionamiento de un cajero en el momento en que el usuario digita la clave (normal o auxilio) y el proceso que se debe realizar. i el usuario digita la clave de auxilio el servidor del banco verifica la información y genera el proceso del monto mínimo.

---

[5] RED COLABORATIVA: Se refiere a la conexión para la transferencia de información entre la Institución Bancaria y la CSCG conectada a través de una red INTERNET.

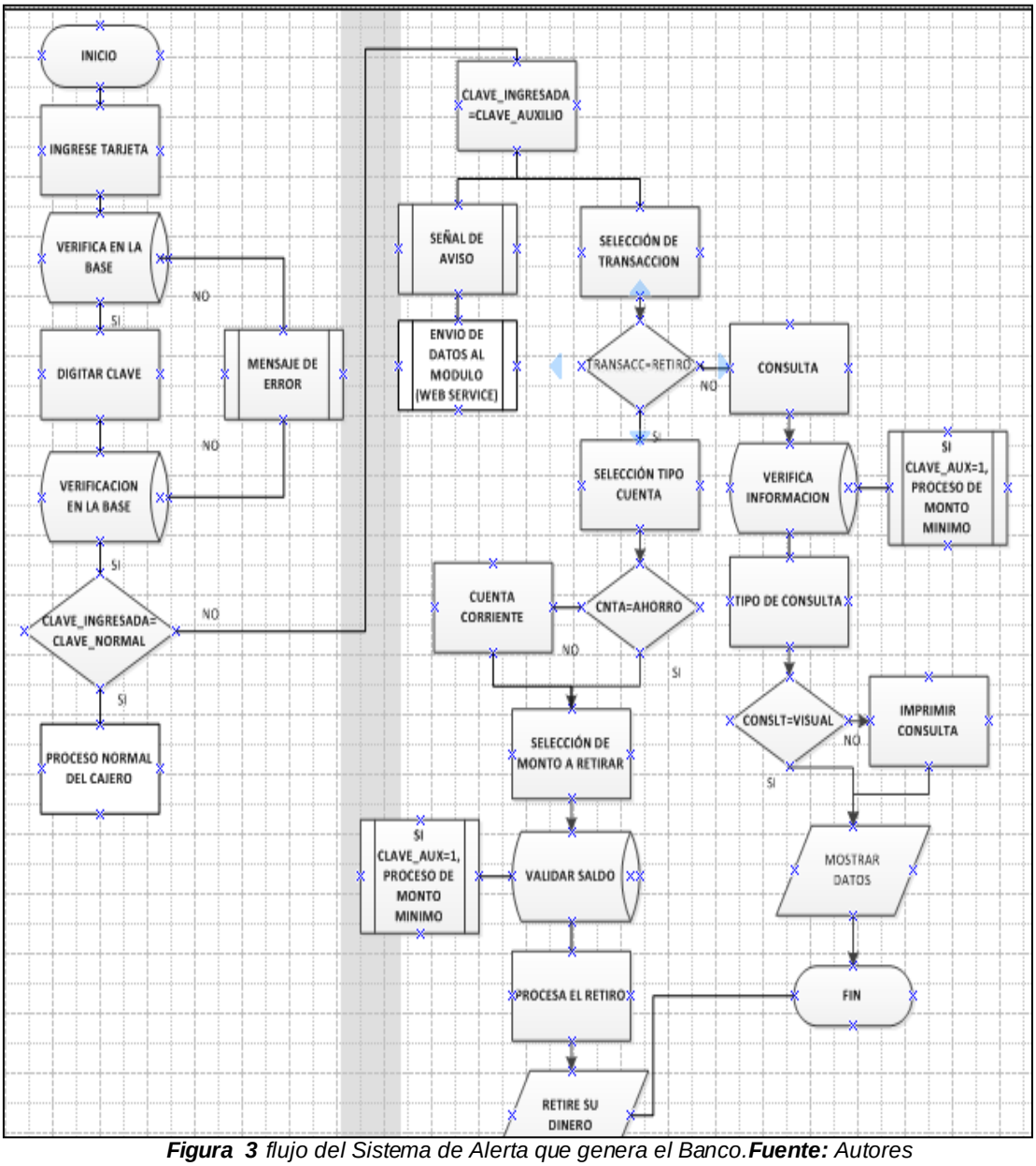


Figura 3 *flujo del Sistema de Alerta que genera el Banco.* ***Fuente:*** *Autores*

Si la clave de auxilio ha sido confirmada, del lado de la CSCG se envía la información de dicha alerta como se muestra en la ***Figura 3.1,*** aquí el receptor

recibe los datos, despacha el incidente (suceso ocurrido) dando aviso a la policía y registrando las acciones que ha debido tomar.

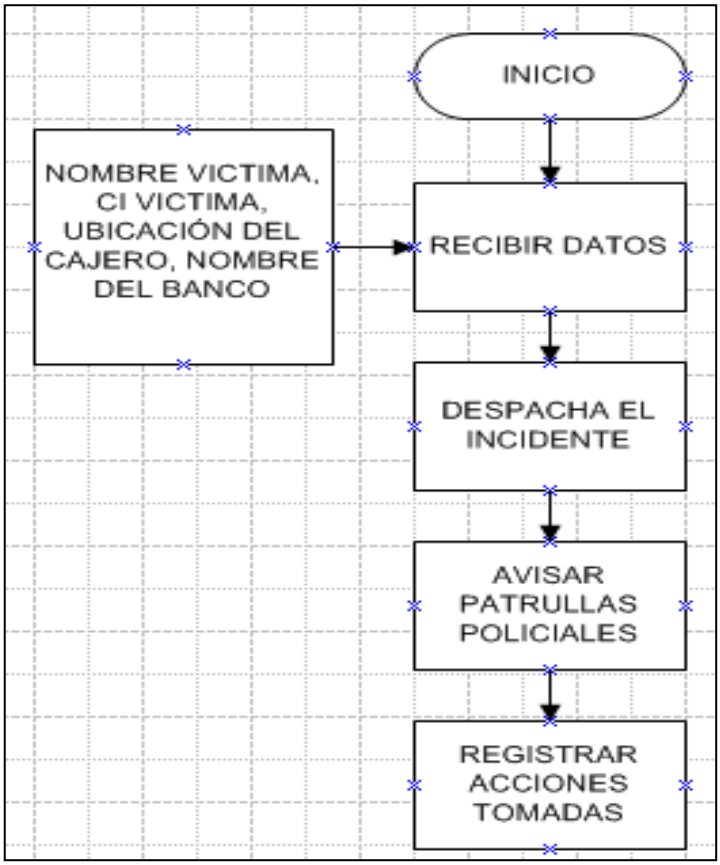


Figura 3.1 *flujo del Sistema de Alerta que genera el Banco (lado de la CSCG).*

Fuente: *Autores*

Si la CSCG es la que recibe la llamada el usuario deberá registrar la información necesaria en nuestro sistema,, si sabe la cedula de identidad de la victima será mas fácil para el Banco identificar quien es el cliente y tomar las respectivas

medidas, sino se la sabe nuestro sistema permite guardar los datos para futuros reportes.

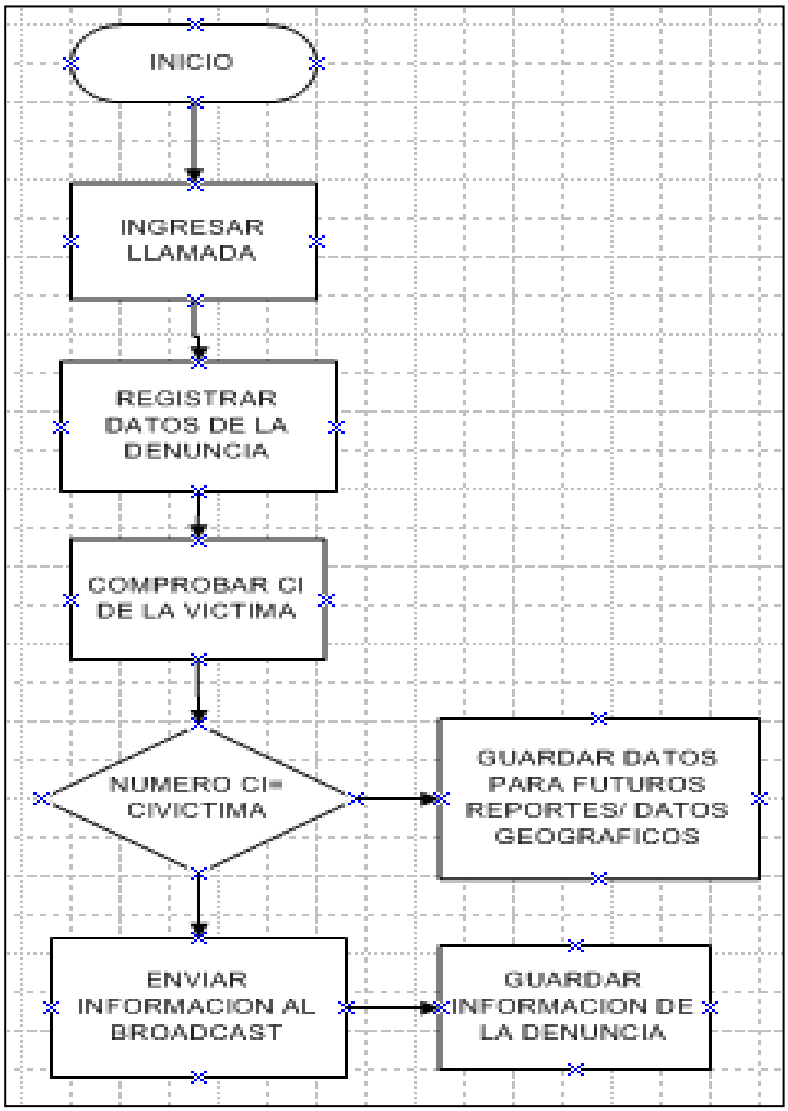


Figura 3.2 *flujo del Sistema de Alerta que genera la CSCG..*

Fuente: *Autores*

Cuando el Banco recibe los datos de la victima que han sido enviados por la CSCG, verifica en que Bancos posee cuentas, nuestro sistema da la opción de

realizar una pregunta aleatoria que solo la sabe el usuario, para comprobar la veracidad de la llamada realizada a la CSCG, para poder realizar el respectivo proceso según la situación.

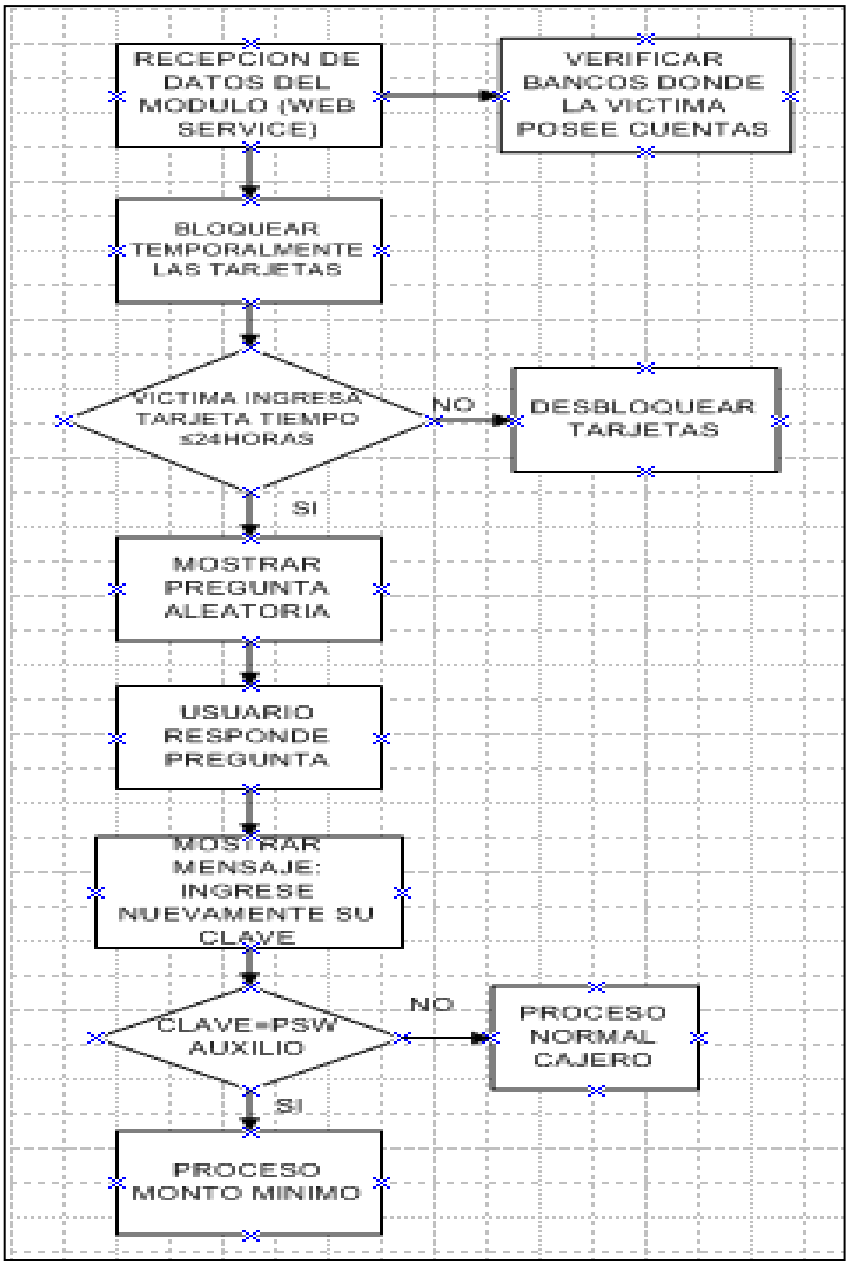


Figura 3.3 *flujo del Sistema de Alerta que genera la CSCG(del lado del Banco)..*

Fuente: *Autores*

3.2 ANÁLISIS DE LA SOLUCIÓN

3.2.1 Requerimientos Funcionales

Los requerimientos funcionales principales son:

3.2.1.1 Envió alarma a entidad de seguridad: Una vez que nuestro sistema recibe la alarma, nuestro módulo envía la información necesaria a la entidad competente para que ésta pueda actuar.

3.2.1.2 Información de usuarios se mantiene segura:_Debido a que se usan protocolos de seguridad no existe forma de que la información sea alterada.

3.2.1.3 Envió de señal de alerta a entidad Bancaria:_Una vez que nuestro sistema recibe los datos de un posible secuestro express con retiro de cajero automático, inmediatamente nuestro módulo envía la información necesaria a la entidad Bancaria para que esta actúe.

3.2.1.4 Envío de señal de alerta a Banred:_Una vez ingresados los datos de la víctima, se envía la información para saber en que Instituciones Bancarias

posee cuentas y proceder de una manera adecuada para evitar que se realice el retiro de su dinero.

3.2.2 Requerimientos no Funcionales

Los requerimientos no funcionales principales son:

3.2.2.1 Disponibilidad 24/7: Nuestro sistema se encontrará disponible 100% o muy cercano a esta disponibilidad las 24 horas del día, los 7 días de la semana incluyendo feriados.

3.2.2.2 Soporta varios usuarios interactuando con el sistema: Debido a que es un sistema diseñado para la seguridad en el retiro de cajeros, debe soportar que varios servidores de distintas entidades Bancarias se conecten a nuestro sistema.

3.2.2.3 Promedio de Mantenimiento 1 vez cada seis meses: para que no exista ningún inconveniente nuestro proyecto estará debidamente documentado y por lo menos cada seis meses se verificará que todo se encuentre funcionando en perfectas condiciones.

3.3 ESPECIFICACIÓN DEL SISTEMA

El sistema constará de dos situaciones:

- El sistema de auxilio que genera el Banco cuando se ingresa la clave de auxilio.

- El sistema de alerta que genera la Corporación para la Seguridad Ciudadana de Guayaquil cuando recibe una denuncia de un posible Secuestro Express.

La creación de estas dos situaciones surge de la necesidad de que cualquiera de las dos entidades (Banco y/o Corporación) puede enviar una señal de alerta.

3.4 DISEÑO DE LA SOLUCIÓN

3.4.1 Descripción del Diseño del Sistema de Auxilio que genera el Banco

El usuario digita la clave, ésta se verifica en el Servidor Central del Banco, si la clave ingresada por el usuario es la de auxilio se envía información (Ubicación del cajero, Entidad Bancaria a la que pertenece dicho cajero, Nombre de la víctima, CI de la víctima) a nuestro módulo, la entidad de seguridad recibirá las alertas las cuales se mostraran en su monitor con los datos necesarios y tomará las acciones debidas.

3.4.2 Descripción de módulos del Sistema de Alerta que genera el Banco

Este consiste de tres módulos:

3.4.2.1 Módulo Despachador: El Módulo Despachador cuando detecta una alerta se encarga de enviar la información (ubicación del cajero, usuario, nombre de la victima) al Módulo de Alarma

3.4.2.2 Módulo de Alarma: El Módulo de Alarma recepta los datos enviados por el Módulo Despachador.

3.4.2.3 Módulo Receptor: Se encarga de registrar las acciones tomadas por los receptores y de enviar ayuda al usuario víctima del Secuestro Express.

3.4.3 Diseño Integración de Red Colaborativa del Sistema de Alerta que genera el Banco

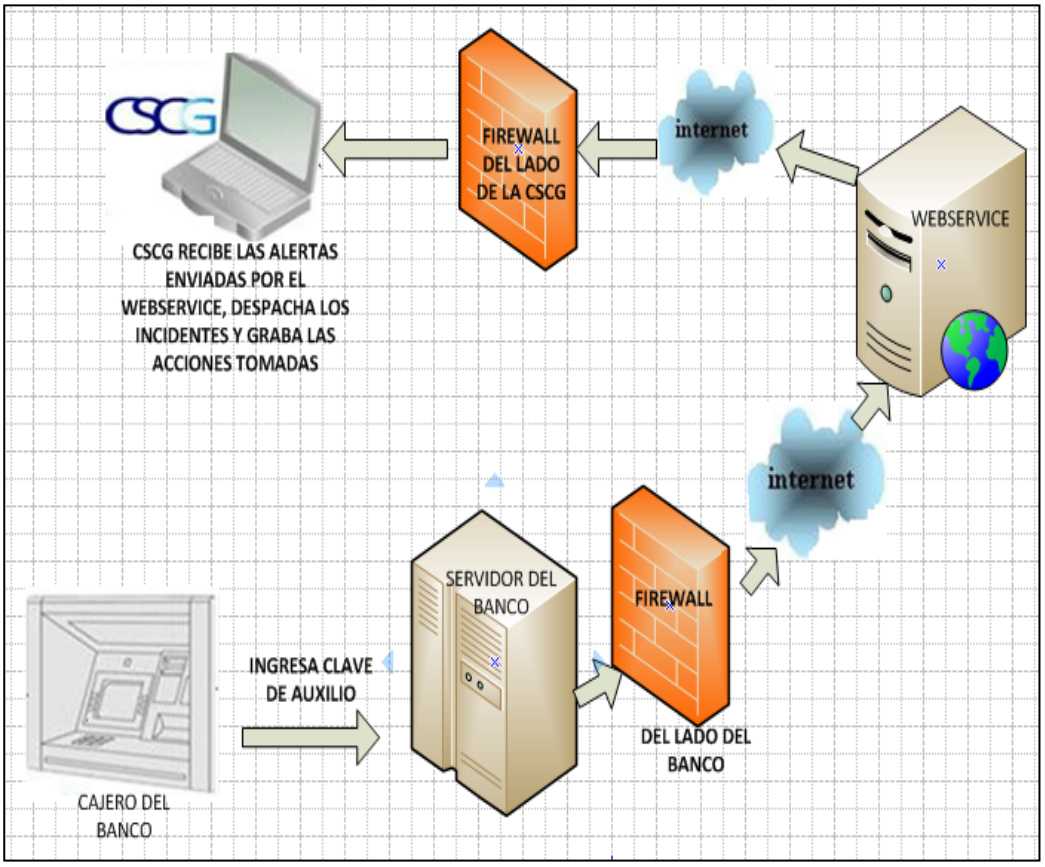


Figura 3.4 *Descripción del Diseño.*

Fuente: *Autores*

3.4.4 Diseño Módulo Despachador

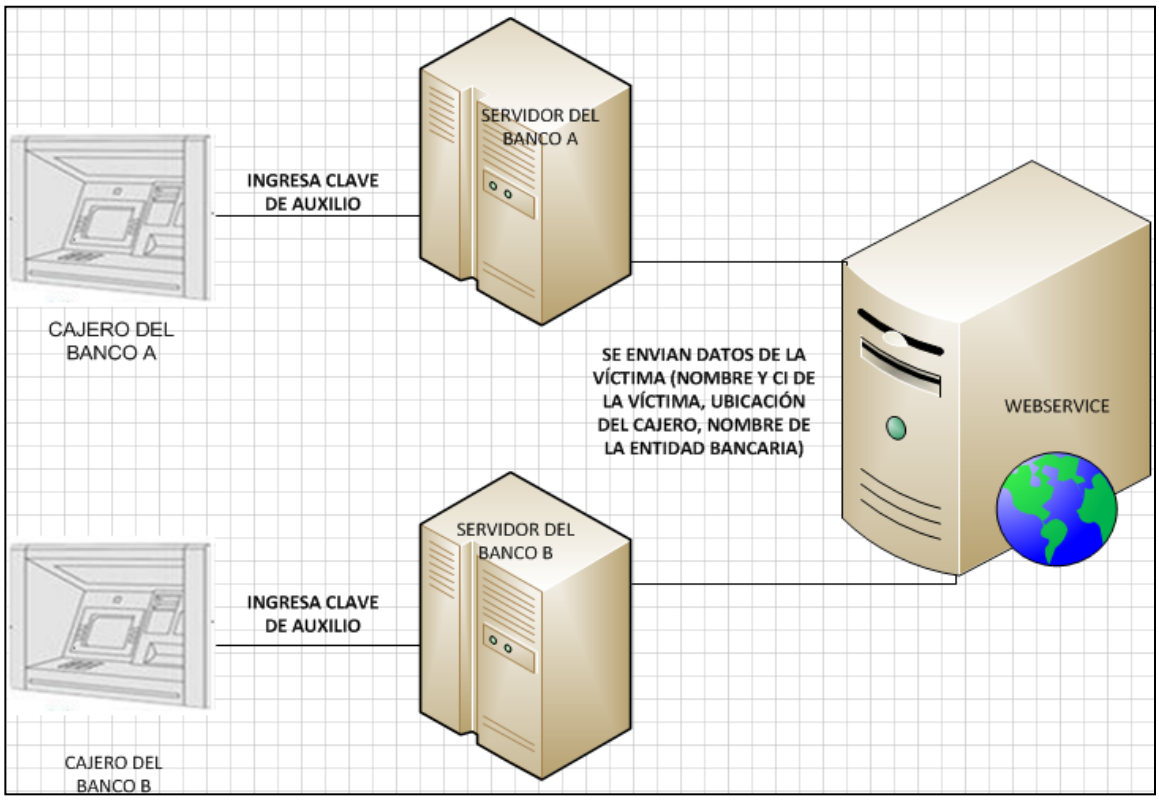


Figura 3.5 *Descripción del Módulo Despachador.*

Fuente: *Autores*

3.4.5 Diseño Módulo Alarma

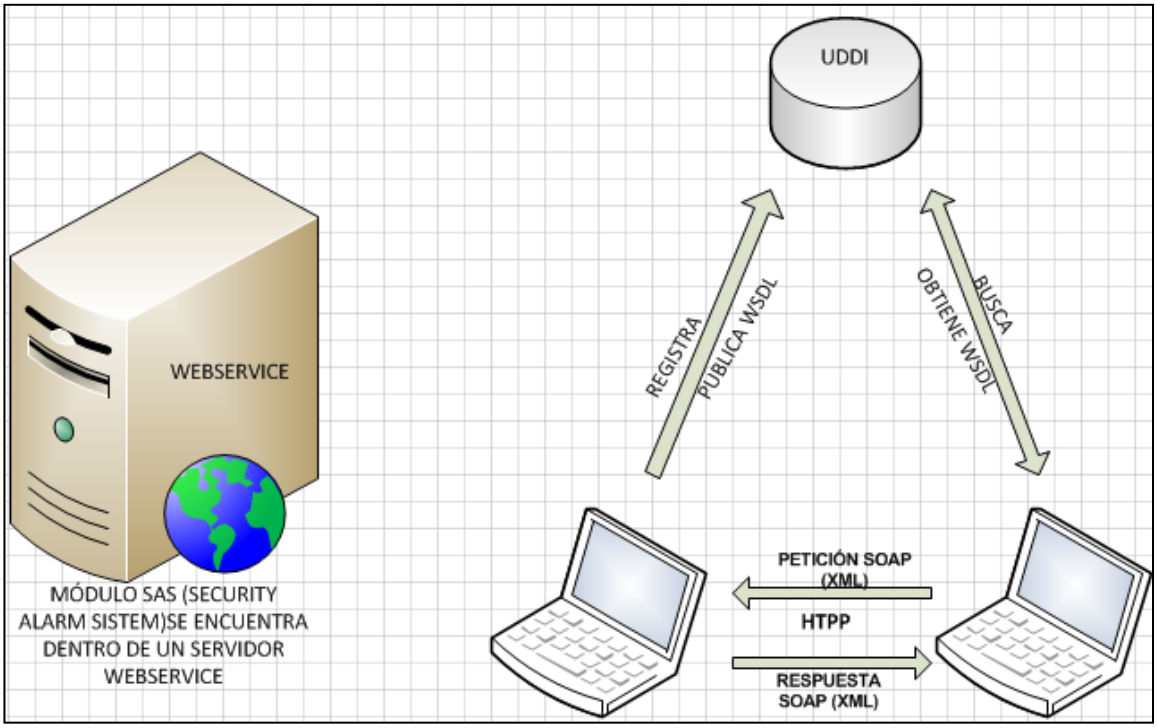


Figura 3.6 *Descripción del Módulo de Alarma.*

Fuente: *Autores*

3.4.6 Diseño Módulo Recepción

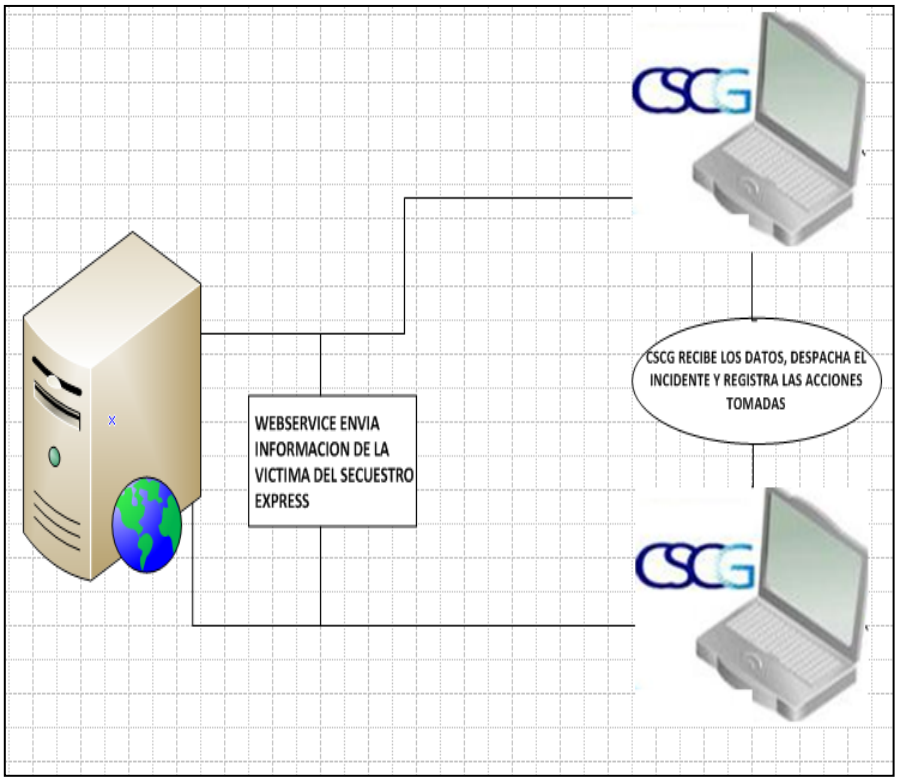


Figura 3.7 *Descripción del Módulo Receptor.*

Fuente: *Autores*

3.4.7 **Diseño Integración de una Red Colaborativa del Sistema de Alerta que genera la Corporación.**[6]

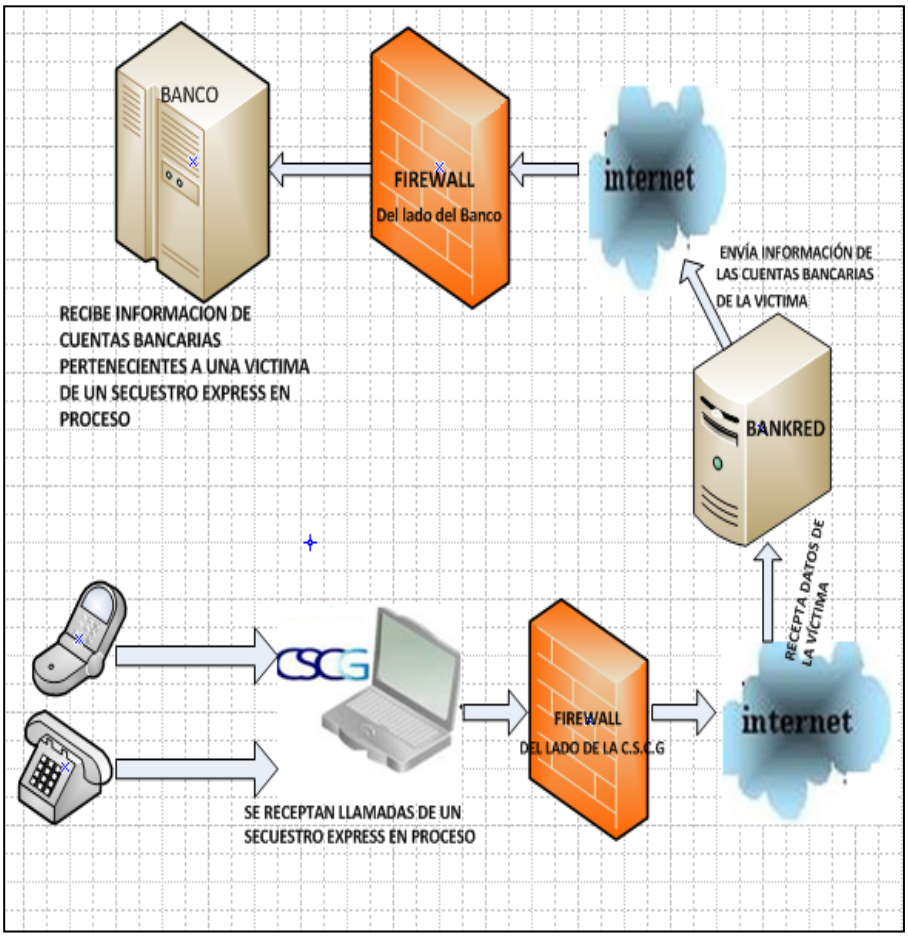


Figura 3.8 *Descripción del Sistema (II situación).*

Fuente: *Autores*

---

[6] **BANRED:** Es una empresa especializada en el procesamiento de transacciones financieras, compensación de cobros y pagos e intercambio de información.

3.4.8 **Diseño Integración de una Red Colaborativa del Sistema de Alerta que genera la Corporación. Módulo Despachador.**

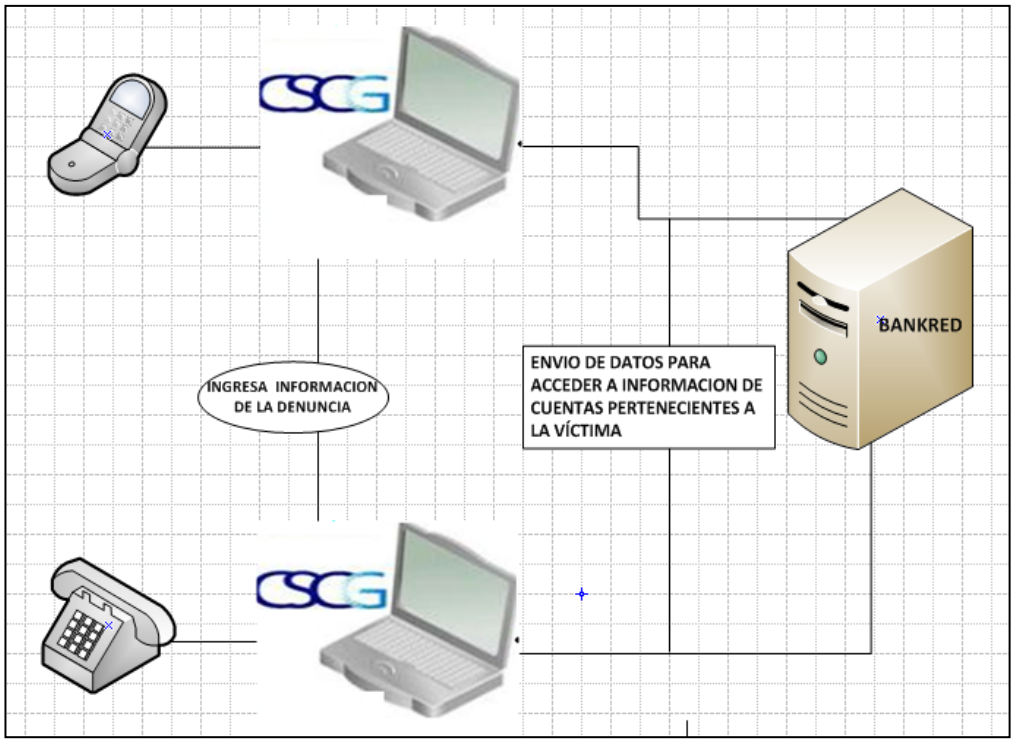


Figura 3.9 *Descripción del Módulo Despachador (II situación)**.***

Fuente: *Autores*

3.4.9 **Diseño Integración de una Red Colaborativa del Sistema de Alerta que genera la Corporación. Módulo Alerta.**

Nuestro módulo de alerta no varía, utilizamos el mismo procedimiento que el sistema de alerta que genera el Banco, su diseño podemos observarlo en la ***Figura 3.6,*** donde graficamos la forma en que el Módulo funciona.

3.4.10 **Diseño Integración de una Red Colaborativa del Sistema de Alerta que genera la Corporación. Módulo Receptor.**

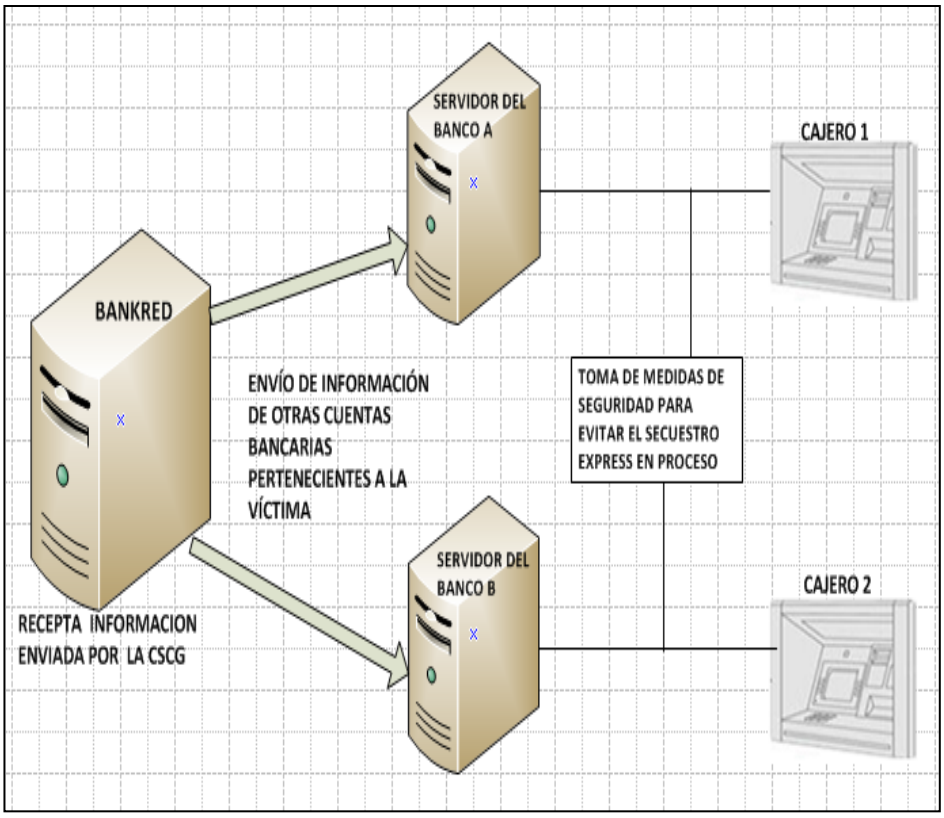


Figura 3.10 *Descripción del Módulo Receptor (II situación)**.***

Fuente: *Autores*

3.4.11 **Diseño de la Base de Datos**

El diseño de la base de datos es fundamental en la implementación de los proyectos, ya que la información debe estar en forma dinámica.

En la Base de Datos del Banco se puede observar la interrelación de las tablas y lo importante que es la comunicación y envió de información entre ellas.

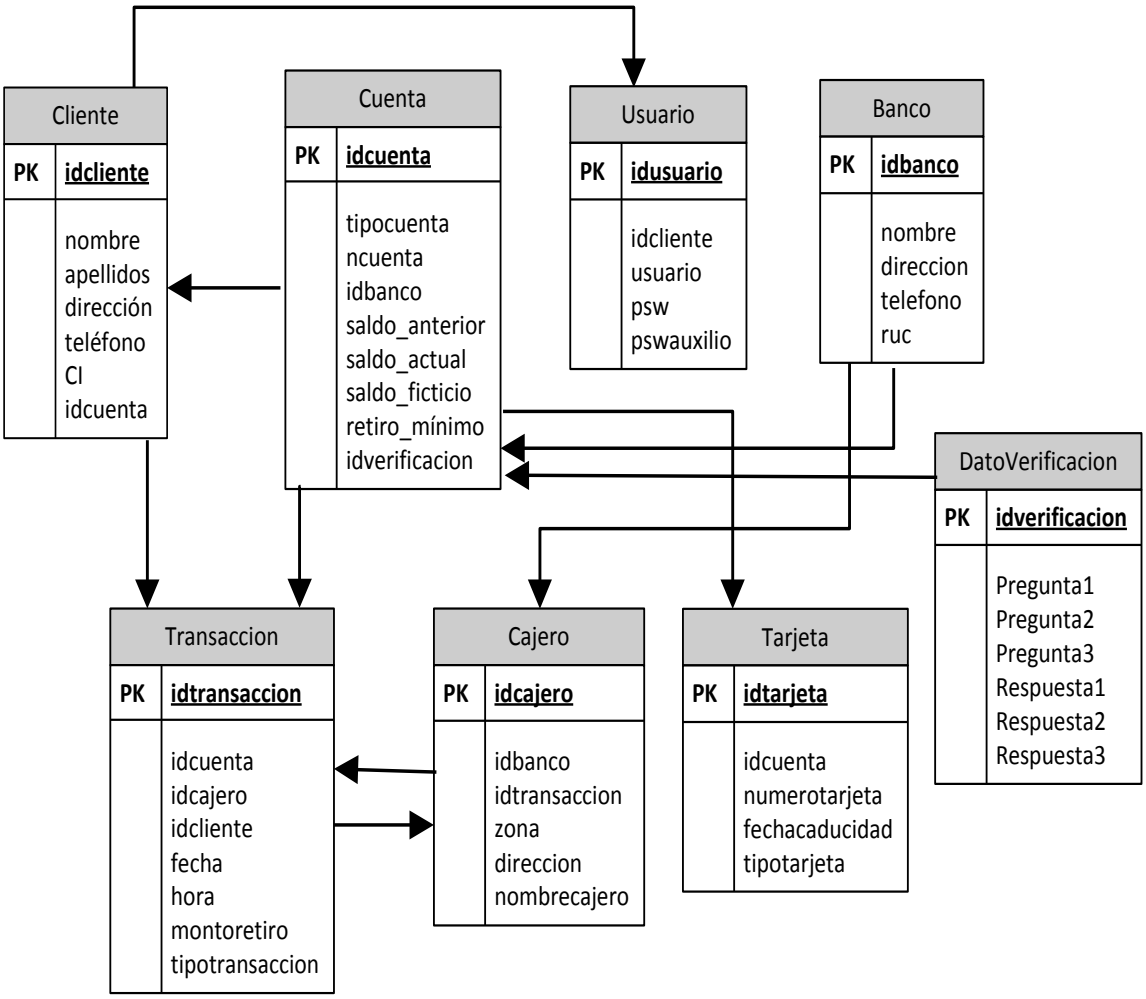


Figura 3.11Base de Datos de la Entidad Bancaria.

Fuente: *Autores*

En la Base de Datos de la CSCG, hemos realizado la creación de 5 tablas diseñadas de tal forma que almacene la información necesaria para el buen funcionamiento de nuestro sistema.

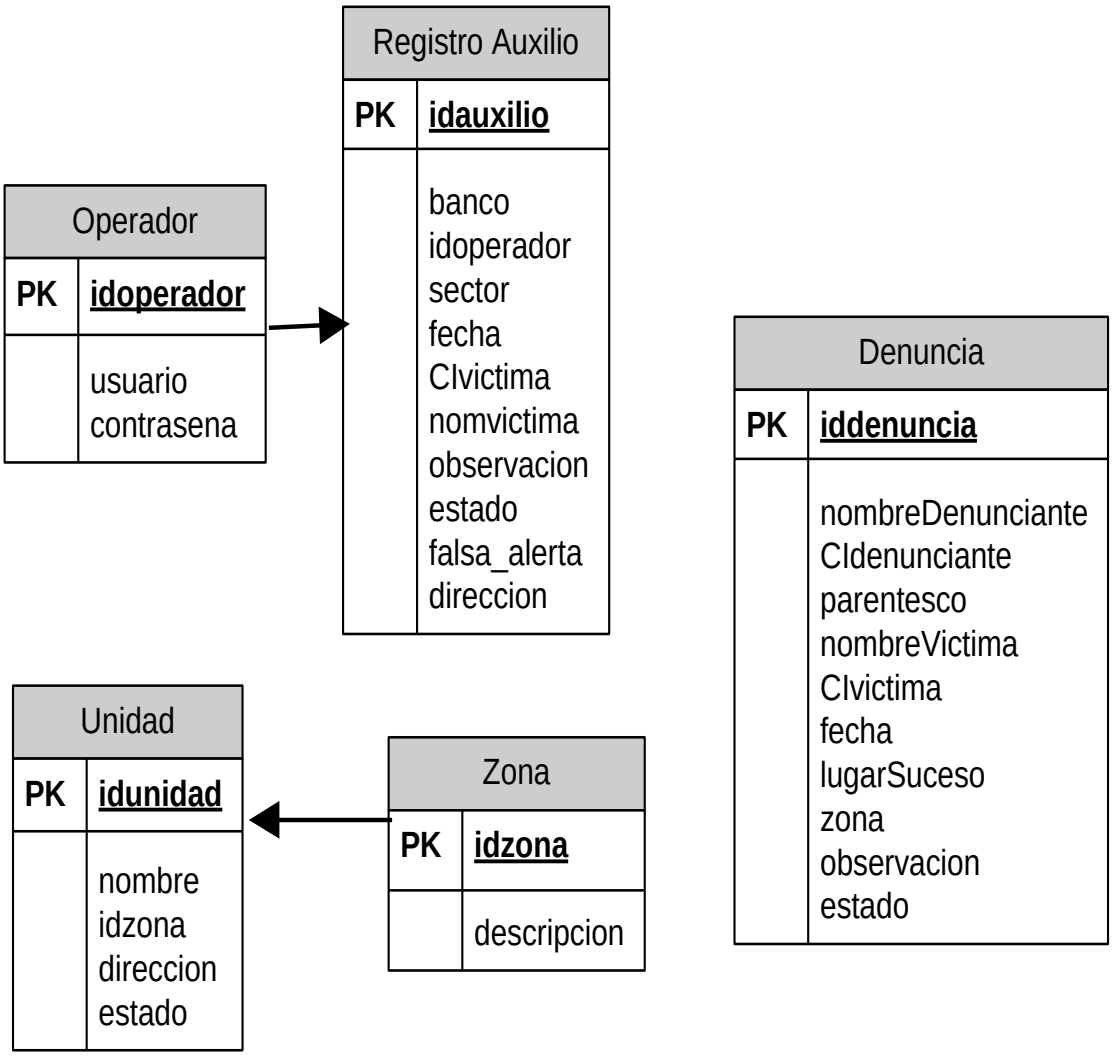


Figura 3.12 Base de Datos de la CSCG.

Fuente: *Autores*

En la Base de Datos del Web Service, hemos realizado la creación de 1 tabla diseñada de tal forma que almacene la información recibida por el Banco o la CSCG.

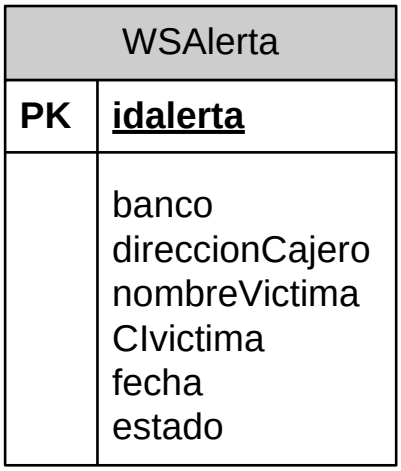


Figura 3.13 *Base de Datos del Web Service*

Fuente: *Autores*

En la Base de Datos del Banred hemos realizado la creación de 1 tabla diseñada de tal forma que pueda recibir y enviar la información necesaria para el buen funcionamiento de nuestro sistema.

Figura 3.14 *Base de Datos del Banred*

Fuente: *Autores*

CAPÍTULO 4

4. IMPLEMENTACION Y PRUEBA

4.1 PLATAFORMA UTILIZADA

Se eligió trabajar con la plataforma Microsoft Windows XP Professional, debido a que es una plataforma que provee entornos de escritorios más utilizados a nivel empresarial, personal y colectivo.

4.2 HERRAMIENTAS PARA LA IMPLEMENTACIÓN DEL SISTEMA

Este sistema será implementado con herramientas actuales y adaptables a los requerimientos exigidos por el mismo, permitiendo con esto tener una gran eficiencia, un fácil uso y a su vez una mayor escalabilidad.

Módulo Despachador

oftware	Descripción
WINDOWS XP PROFESSIONAL	Sistema Operativo
VISUAL C# NET	Ambiente de desarrollo

Tabla 1 Software utilizado para el desarrollo del proyecto

Fuente: Autores

Módulo Alarma

Software	Descripción
SQL SERVER 2005	Motor de Base de Datos
WINDOW SERVER 2008	Servidor

Tabla 2 Software utilizado para el desarrollo del proyecto

Fuente: Autores

Módulo Receptor

Software	Descripción
WINDOWS XP PROFESSIONAL	Sistema Operativo
VISUAL C# NET	Ambiente de desarrollo

Tabla 3 Software utilizado para el desarrollo del proyecto

Fuente: Autores

4.3 HERRAMIENTAS DE DESARROLLO

4.3.1 Visual C# Net: Se utilizo éste lenguaje porque ofrece al programador una interfaz común para trabajar de manera cómoda y visual con cualquiera de los lenguajes de la plataforma .NET.

4.3.2 SQL Server 2005: Se utilizó SQL SERVER 2005 porque además de las ventajas que nos brinda al ser una herramienta de fácil uso respecto al ingreso y manipulación de los datos, nos ofrece métodos para acceder a la información.

Como usuario de la herramienta se puede acceder a archivos en otros equipos, realizar copias de seguridad en ubicaciones de red entre otros beneficios.

4.3.3 WINDOW SERVER 2008: Se utilizo WINDOW SERVER 2008 por su capacidad altamente modular, que permite incluso realizar una instalación sin el entorno gráfico, optimiza los recursos de hardware y del propio sistema, y aumenta la seguridad

A continuación enumeramos algunos beneficios del Windows Server 2008:

- Nuevo proceso de reparación de sistemas NTFS[7]: proceso en segundo plano que repara los archivos dañados.

- Sistema de archivos SMB2: de 30 a 40 veces más rápido el acceso a los servidores multimedia.

- Address Space Load Randomization (ASLR): protección contra malware en la carga de controladores en memoria.

---

[7] NTFS: (New Technology File System). Es un sistema de archivos diseñado específicamente para Windows NT, y utilizado por las versiones recientes del sistema operativo Windows. Ha reemplazado al sistema FAT utilizado en versiones antiguas de Windows y en DOS.

- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización.

4.3.4 Uso de Certificados Digitales

Un Certificado Digital, es un documento electrónico emitido por una entidad reconocida a nivel mundial (Ej.: Banco Central, VeriSign[5]), la cual llamaremos de ahora en adelante Entidad Certificadora.

"El propósito principal de un certificadora digital es comprobar que la clave pública contenida en el certificado pertenece a la entidad a la que se emitió el certificado."

De esta manera el cliente o el servicio que trate de interactuar con este servidor de manera segura, tendrá la certeza de que esta comunicándose efectivamente con quien desea comunicarse y podrá enviar los mensajes por un canal seguro (SSL), usando encriptación por medio de la llave pública del certificado de la entidad, la cual a su vez podrá desencriptar los datos con la ayuda de su propia llave privada que emitida por la Entidad Certificadora.

Al principio cuando el servidor todavía no puede recibir requerimientos Web, y desea instalar un Certificado Digital para su organización debe pasar por los siguientes pasos:

- Contratar los servicios de una Entidad Certificadora: Para lograr esto la organización debe ponerse en contacto con la entidad a controlar y entregarle ciertos atributos, como son los datos de la empresa y en retorno recibirá el certificado con su clave pública; su clave privada (utilizada para desencriptar los mensajes.

- Implantar el certificado en su servidor: Esto se hace por medio del IIS, el cual permite colocar el certificado de tipo servidor para que pueda ser entregado a los clientes que requieran una comunicación segura.

- Elegir que sitios desea que ofrezcan el servicio: Para lograr esto se debe administrar el IIS y revisar que directorios virtuales serán accedidos de manera segura, eligiendo así, que opciones se van habilitar (SSL, requerir certificados de clientes, etc.).

Una vez configurada la infraestructura del Web Service, los requerimientos de los clientes de manera segura (es decir usando https), recibirán, si es la primera vez que acceden a la página, el Certificado Digital correspondiente a la Entidad, el cual si se desea podrá ser revisado para verificar los datos de validez, y de la entidad que lo emitió. Si el cliente acepta este certificado se entablará una comunicación segura con el servidor.

4.3.5 Como se instala una Entidad Certificadora

Microsoft Windows Server ofrece una interfaz amigable y sencilla para poder instalar una Entidad Certificadora en una organización, a continuación se enumeran los pasos generales para poder lograrlo.

Antes de comenzar los pasos para la instalación de una Entidad Certificadora, es necesaria saber que existen dos tipos de entidades y conocer sus diferencias, para saber cual es la que se desea instalar en el servidor. Los tipos de Entidades Certificadoras son:

4.3.5.1 Stand-Alone: Los certificados que pueden ser emitidos por este tipo de Entidad Certificadora son para clientes o equipos que se encuentran por fuera del dominio. Adicionalmente esto quiere decir que el servidor es único, es decir no hace parte de una organización y por lo tanto los clientes no hacen parte de un dominio específico.

4.3.5.2 Enterprise: Se usa esta modalidad de Entidad Certificadora, si los certificados son para equipos o clientes dentro de un dominio, es decir dentro de la misma organización, para que esto funcione es necesario que los usuarios tengan cuentas de Active Directory en el servidor, cosa que no se necesita en el esquema Stand-Alone, adicionalmente se debe tomar esta modalidad si deseamos que clientes de nuestra organización se puedan comunicar desde afuera y se puedan autenticar por medio de sus certificados con la organización.

El Active Directory almacena información sobre los recursos de la red y provee los servicios que hacen que sea más fácil localizarlos, administrarlos y de usar; éste también provee la administración de una forma de organización centralizada, administración y control de acceso a los recursos de la red.

4.4 QUE DATOS SE DEBEN PROTEGER

La información que se encuentra almacenada en la Base de Datos del Banco debe de tener la seguridad respectiva ya que son datos personales de los usuarios, entre los datos más importantes tenemos los siguientes:

- Nombres y Apellidos del Cliente.
- Dirección del Cliente.
- Cédula de Identidad del Cliente.
- Teléfono del Cliente.
- Cuentas de las distintas entidades bancarias que el cliente posee.
- Claves de acceso a los diferentes servicios, proporcionados por el Banco (Clave Normal y Clave de Auxilio).

4.5 IMPLEMENTACIÓN DEL SISTEMA

El motivo principal por la cual se optó en utilizar el lenguaje C# para este

proyecto denominado: “DISEÑO Y PROTOTIPO DE UNA RED COLABORATIVA USANDO UN SISTEMA DE ALERTAS TECNOLÓGICAS CON EL FIN DE APLACAR EL SECUESTRO EXPRESS CON RETIRO DE CAJERO AUTOMATICO” fueron por las siguientes consideraciones:

- Conocimiento previo de la herramienta por los integrantes del grupo.
- El lenguaje C# ofrece una interfaz amigable y de fácil adaptación con cualquiera de los lenguajes de la plataforma .NET.
- Esta respaldado a través de una licencia de una marca reconocida (Microsoft).
- La funcionalidad de Visual C# es flexible, amigable, intuitiva y sencilla para el usuario final.

4.5.1 Diseño de Interfaz del Usuario de la C.S.C.G

El usuario de nuestro sistema visualizara una pantalla donde ingresará el usuario y el password.

Figura 4 *Pantalla login.*

Fuente: *Autores*

Para la elaboración del sistema se ha decidido crear una plantilla principal a nivel de usuario, donde tendrá las siguientes opciones:

- Alarmas.
- Registro de Denuncias (ingreso de la denuncia).
- Denuncias.
- Consultas (las consultas generadas pueden ser por alarma o denuncia).
- Estadísticas denuncia.
- Estadísticas Auxilio.

La pantalla principal muestra las opciones que nuestro sistema permite realizar, en la primera opción se visualizarán las alertas generadas por las claves de auxilio, la información recibida es confiable.

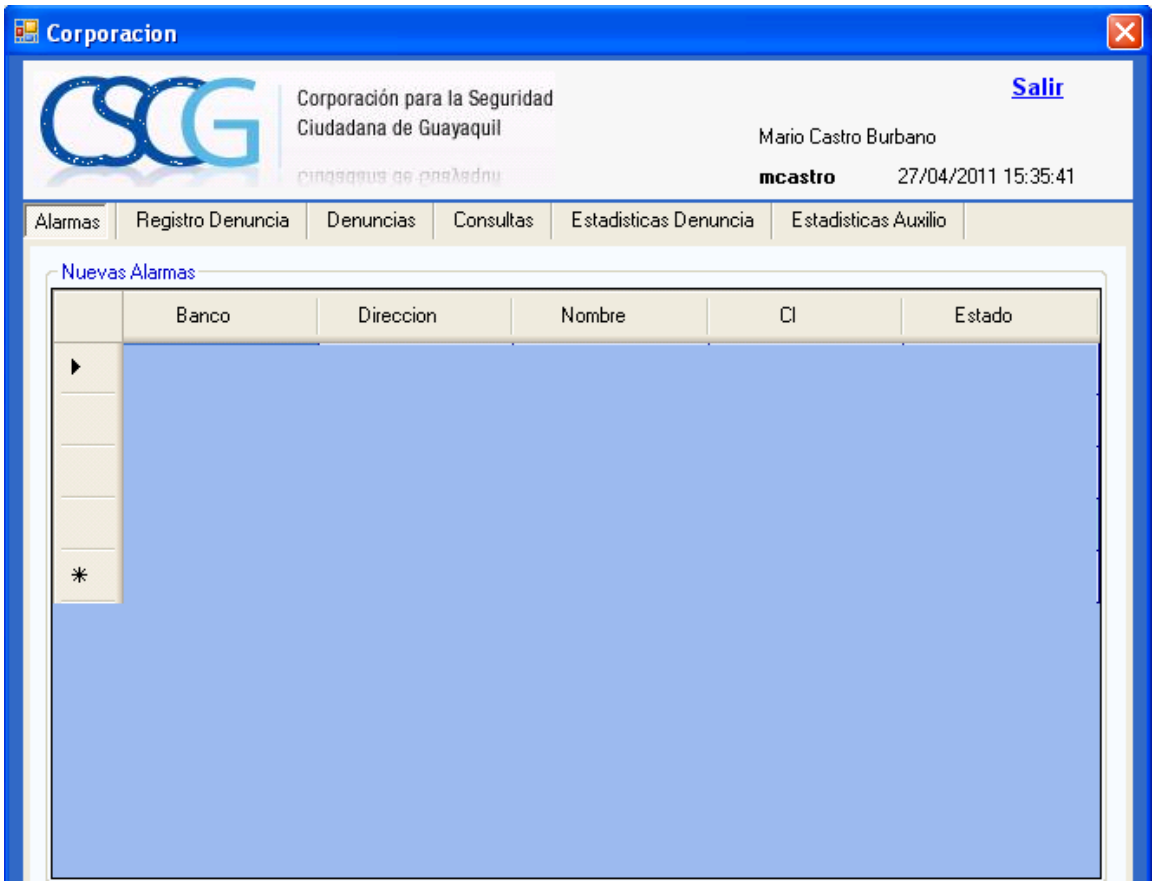


Figura 4.1 *Pantalla donde se visualizará los datos de las alarmas.*

Fuente: *Autores*

Al dar clic en la alerta ingresada se obtiene una nueva pantalla donde se encontrarán los datos de la alarma de auxilio ingresada, como: Banco (nombre del Banco del que pertenece el cajero), Dirección (direccion de la ubicación del cajero), Víctima (nombres completos del usuario que esta siendo victima de un secuestro express), CI Victima (cantidad de 10 dígitos),

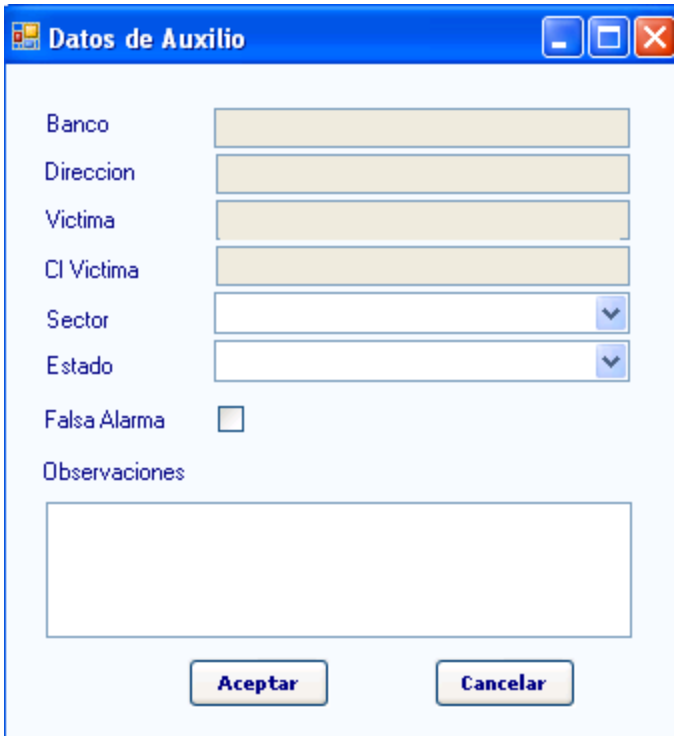


Figura 4.2 *Pantalla donde se visualizarán los datos generados por la alarma de auxilio.*

Fuente: *Autores*

La segunda opción es utilizada cuando la C.S.C.G recibe una llamada dando aviso sobre una víctima de un secuestro express, aquí el receptor deberá ingresar cierta información que será tomada de la persona que realiza la denuncia.

Figura 4.3 *Pantalla Ingreso de Denuncia.*

Fuente: *Autores*

La tercera opción es utilizada cuando el receptor o alguna entidad desean observar todas las denuncias ingresadas con sus respectivos estados (pendiente, solucionado).

Figura 4.4 *Pantalla de visualización de las denuncias.*

Fuente: *Autores*

La cuarta opción es utilizada cuando se desea realizar consultas sobre las alarmas y denuncias ingresadas a la CSCG para tener un detalle específico de los diferentes incidentes en fechas determinadas, aquí solo se habilitara la opción escogida por el usuario ya sea en las Consultas por denuncia o por Alarma.

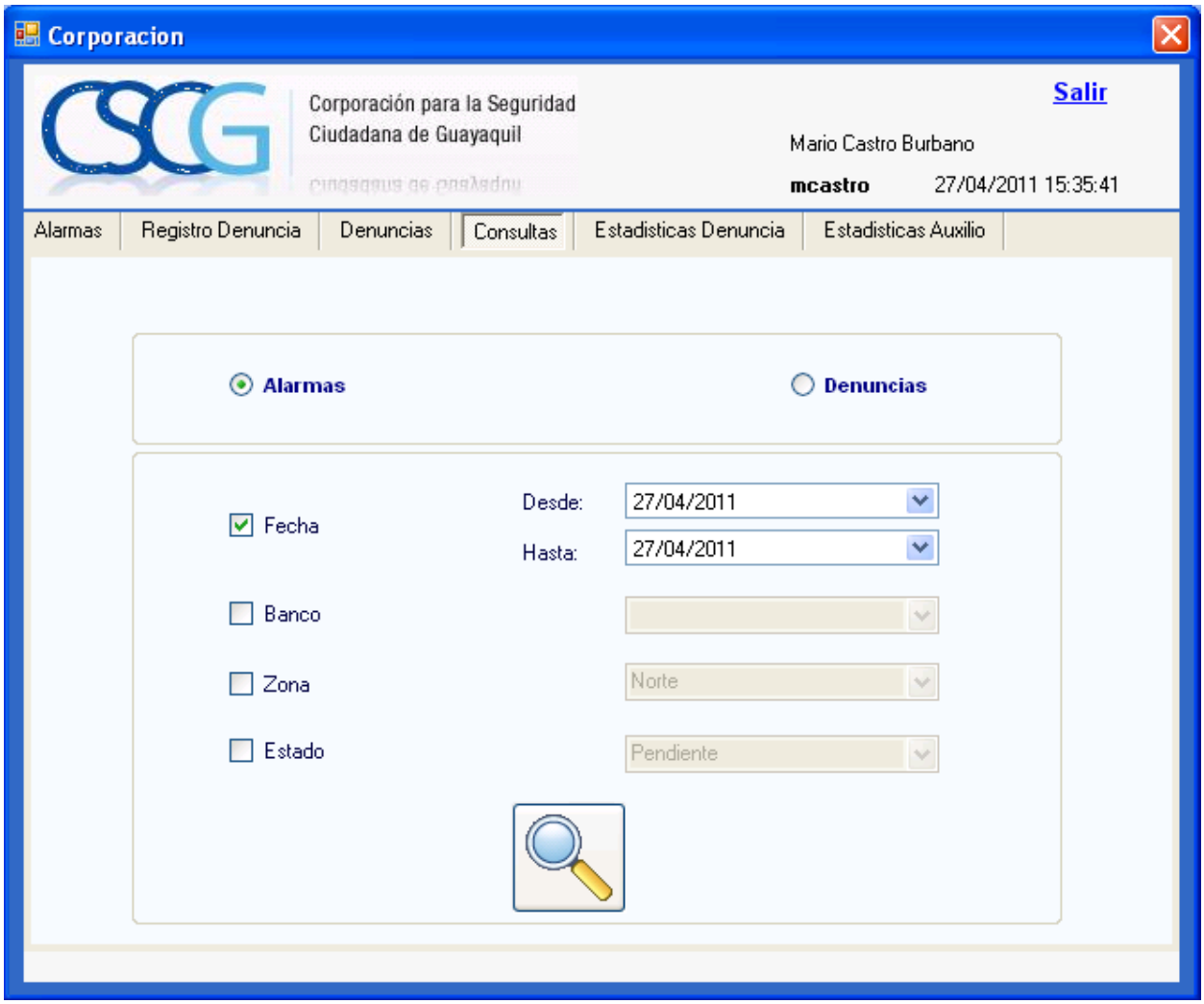


Figura 4.5 *Pantalla de visualización de consultas.*

Fuente: *Autores*

La quinta y sexta opción es utilizada cuando se necesite visualizar por medio de gráficos estadísticos, esto permitirá al receptor una mejor interpretación,

descripción y análisis del comportamiento de determinados datos, tanto de denuncias como de registro de auxilios.

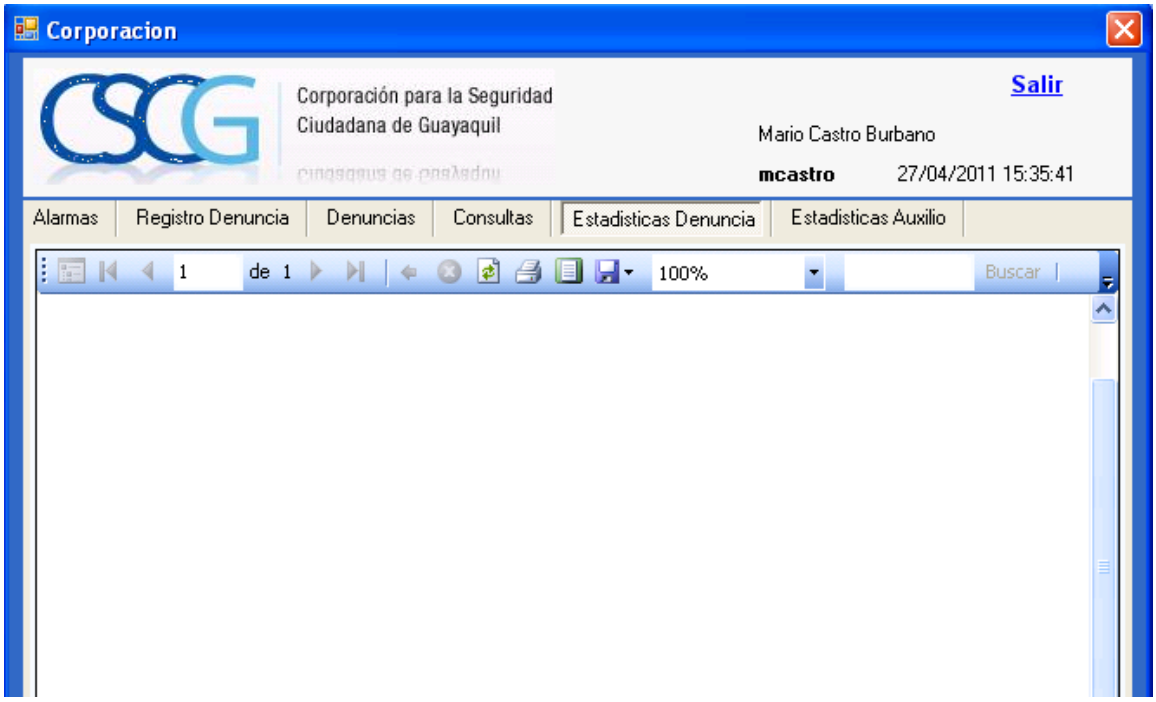


Figura 4.6 *Pantalla de visualización de reportes.*

Fuente: *Autores*

4.5.2 Generación Automática de Alertas

4.5.2.1 Sistema de Alerta que genera el Banco

Cuando el usuario de un Banco ingresa su clave en el cajero automático se debe verificar cual es la clave que ha ingresado. Ver Anexo A

Si la Clave es detectada como una Clave de Auxilio, entonces el Servidor del Banco envía la información necesaria al Módulo “Security Alarm System” , y esta información es dirigida a la CSCG. Ver Anexo B

4.5.2.2 Sistema de Alerta ue genera la Corporación

Cuando la C.S.C.G recibe una llamada sobre una víctima de un posible Secuestro Express el receptor (Usuario del módulo) debe ingresar datos personales del denunciante y de la victima así como lugar en que ocurrió dicho suceso. Ver Anexo C

Una vez ingresada la información el receptor (usuario del módulo) debe enviar la información con los datos de la denuncia al Banred y éste envía la señal de alerta a todas las Instituciones Financieras donde la víctima posee cuentas.

Una vez que el Banco receptó la alerta, procede a poner en stand by las cuentas de la víctima hasta que se compruebe su veracidad. Ver Anexo D

4.5.3 Registro de Acciones

El registro de acciones en nuestro proyecto sirve de ayuda para futuros reportes o datos estadísticos sobre el promedio de secuestros Express en fechas

determinadas del año, o usuarios de Instituciones Bancarias que son víctimas más frecuentes o sectores donde se realiza dicho delito.

Una vez que el receptor (usuario del modulo) ha detectado la Alarma de Auxilio, despacha el incidente enviando ayuda policial. Todas estas acciones que han sido tomadas para salvaguardar a la víctima son ingresadas y guardadas.

Si alguna entidad o persona quisiera ver los reportes, solo se necesitará accesar al Módulo, dar clic a la opción Consultas y de ahí escoger la opción: Alarma o Denuncia, una vez hecho esto, seleccionar como desea generar el reporte (ya sea por fecha o por nombre del Banco). Ver Anexo E

4.6 Pruebas y Resultados

Aquí se detallan las pruebas realizadas para determinar la eficiencia y eficacia de nuestro módulo.

4.6.1 Prueba de Eficacia

Para realizar estas pruebas simulamos un secuestro express en proceso.

Primera Situación:

El usuario del Banco es víctima de un secuestro express con modalidad de retiro de dinero, inserta su tarjeta de débito ingresando su clave de auxilio.

Figura 4.7 *Pantalla inicial del cajero.*

Fuente: *Autores*

En ese momento el servidor del Banco detecta la alerta y envía toda la información a la CSCG, ésta operación es totalmente transparente para el delincuente ya que el usuario (víctima) sigue realizando su transacción con normalidad.

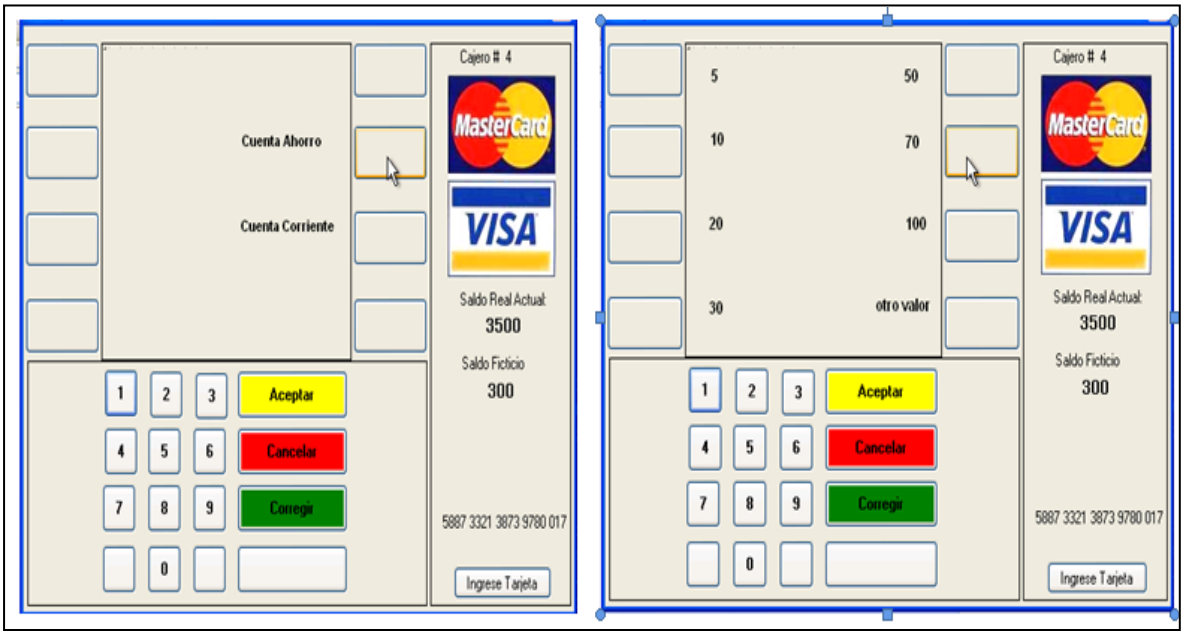


Figura 4.8 *Pantallas del funcionamiento normal del cajero (1).* ***Fuente:*** *Autores*

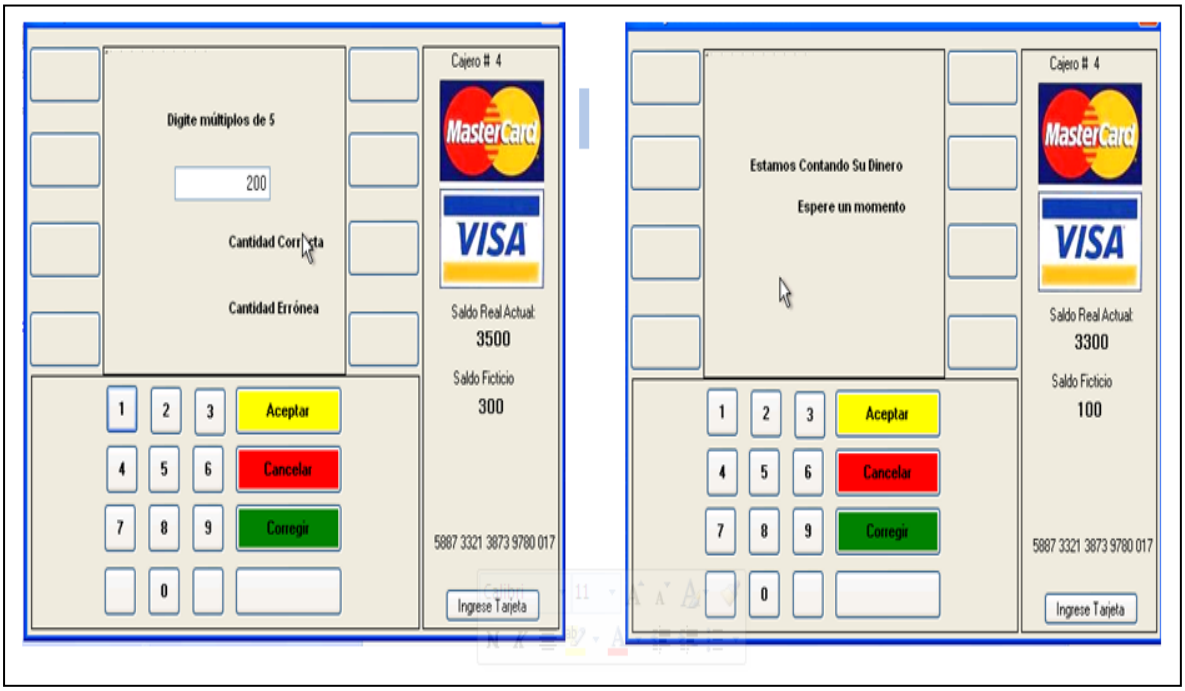


Figura 4.9 *Pantallas del funcionamiento normal del cajero (2).*

Fuente: *Autores*

El receptor de la CSCG debe visualizar en su monitor una lista de las diferentes alertas, las cuales deben ir llegando en orden de aparición.

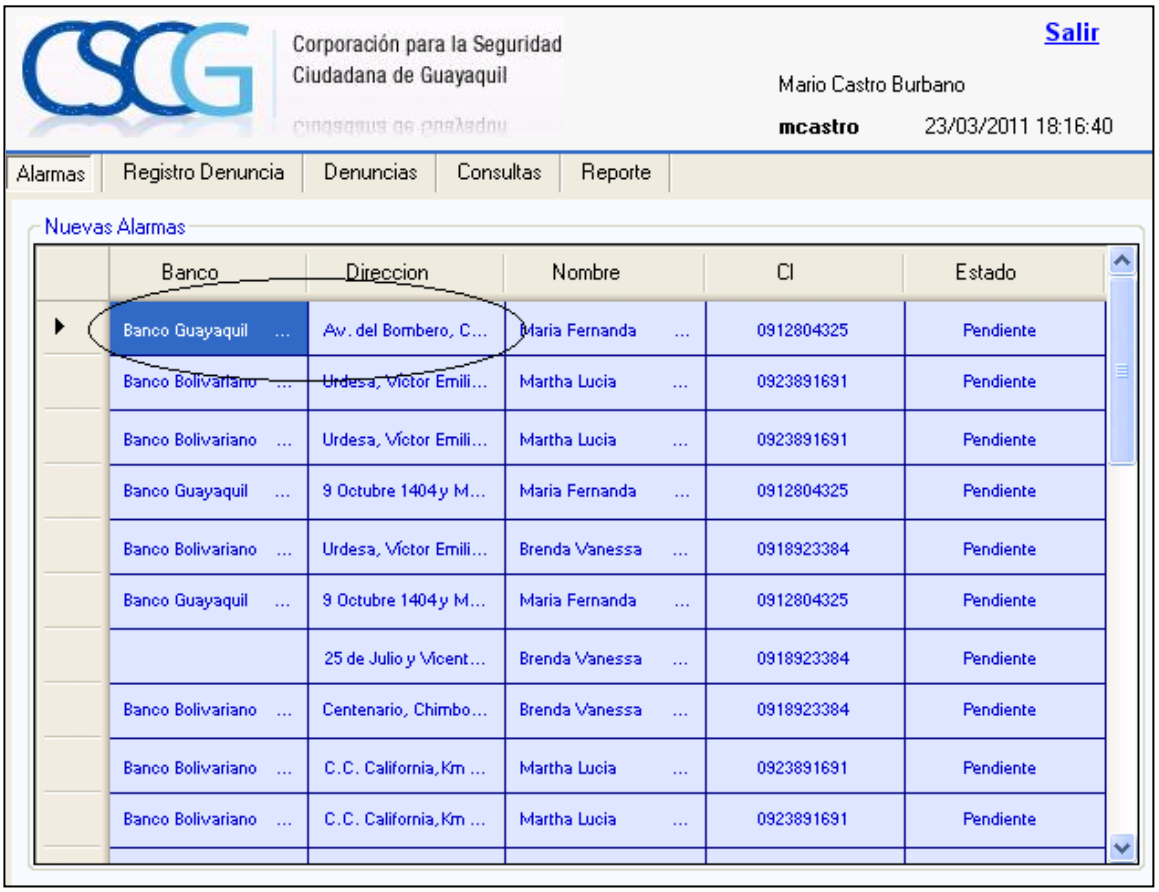


Figura 4.10 *Pantalla de Recepción de nueva alarma.*

Fuente: *Autores*

El receptor al dar clic sobre una de las alarmas, debe observar una nueva pantalla donde saldrá la información necesaria para que él pueda despachar dicho incidente y enviar la ayuda policial.

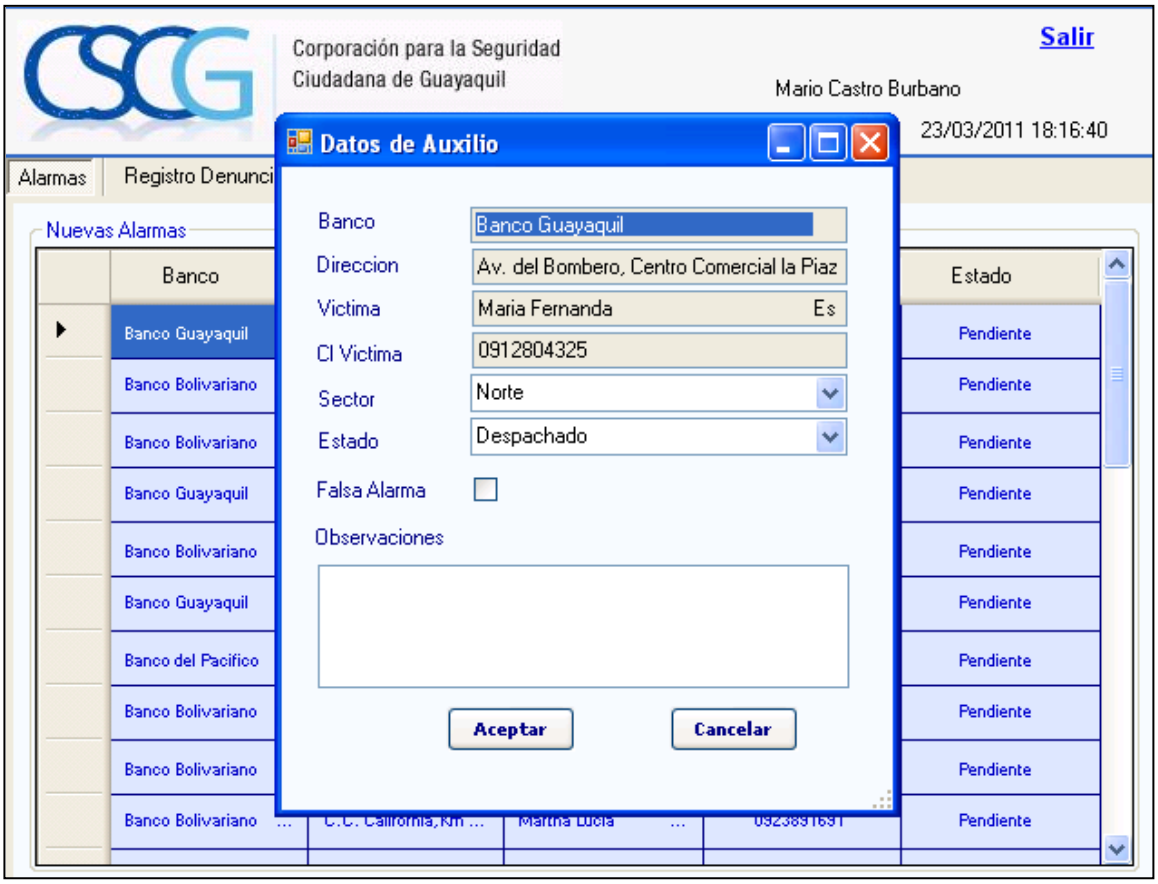


Figura 4.11 *Pantalla donde se visualiza la información de la alarma.*

Fuente: *Autores*

El receptor después que ha despachado la alerta y enviado la respectiva ayuda policial, guarda la información, esta información podrá ser visualizada en

reportes los cuales pueden ser utilizados a futuro para realizar estadísticas delincuenciales o como prueba de la funcionalidad de nuestro sistema.

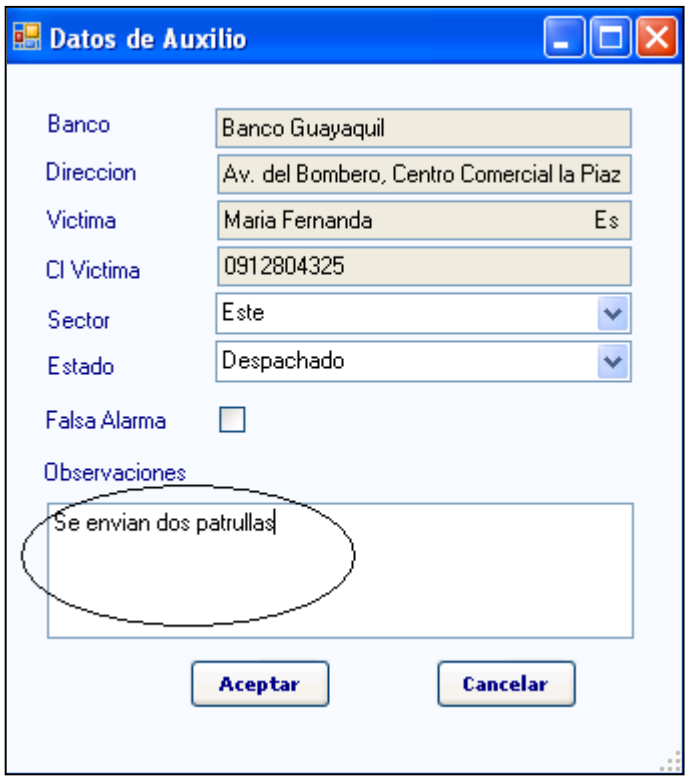


Figura 4.12 *Pantalla donde el receptor ingresa "observaciones" sobre la alarma despachada.*

Fuente: *Autores*

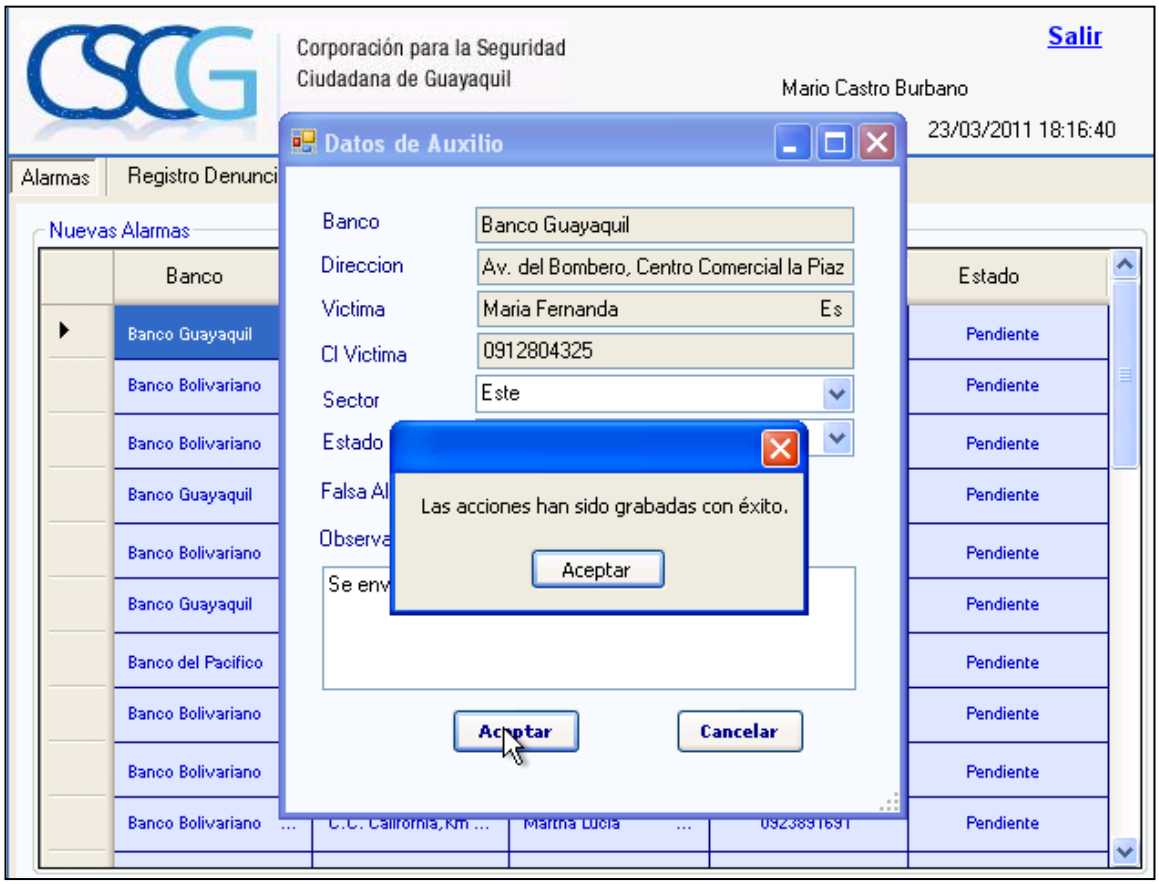


Figura 4.13 *Pantalla donde se visualiza que la alarma ya ha sido despachada y las acciones grabadas.*

Fuente: *Autores*

Segunda Situación:

La CSCG recepta una llamada de auxilio sobre una posible víctima de secuestro express, en ese momento el receptor deberá dar clic a la segunda opción de su sistema el cual es “DENUNCIA”.

Una vez dado clic en la opción debe visualizar una pantalla donde el receptor deberá realizar una serie de preguntas al denunciante para obtener una información más detallada sobre el incidente en mención.

Figura 4.14 *Pantalla donde el receptor deberá ingresar la información de la Denuncia.*

Fuente: *Autores*

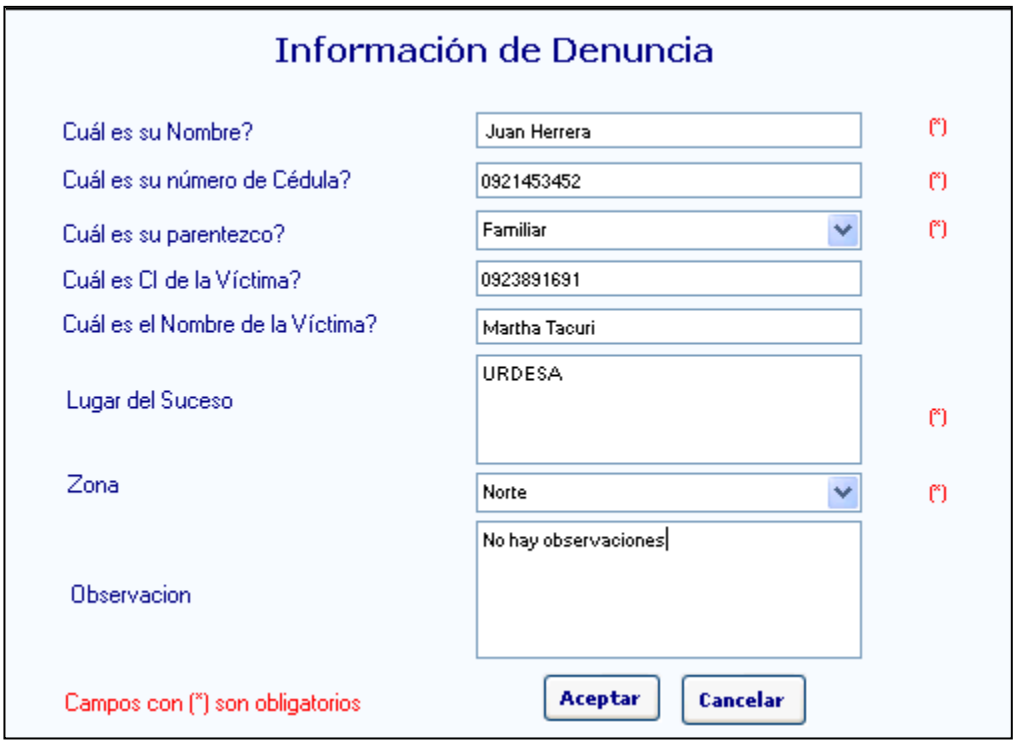


Figura 4.15 *Pantalla donde observamos los datos ingresados de la Denuncia.*

Fuente: *Autores*

Una vez ingresada la información, el receptor deberá dar clic en la opción guardar, en ese momento la alarma será enviada al Banred para que este envíe la alerta a las diferentes Instituciones Bancarias donde la víctima posee cuentas.

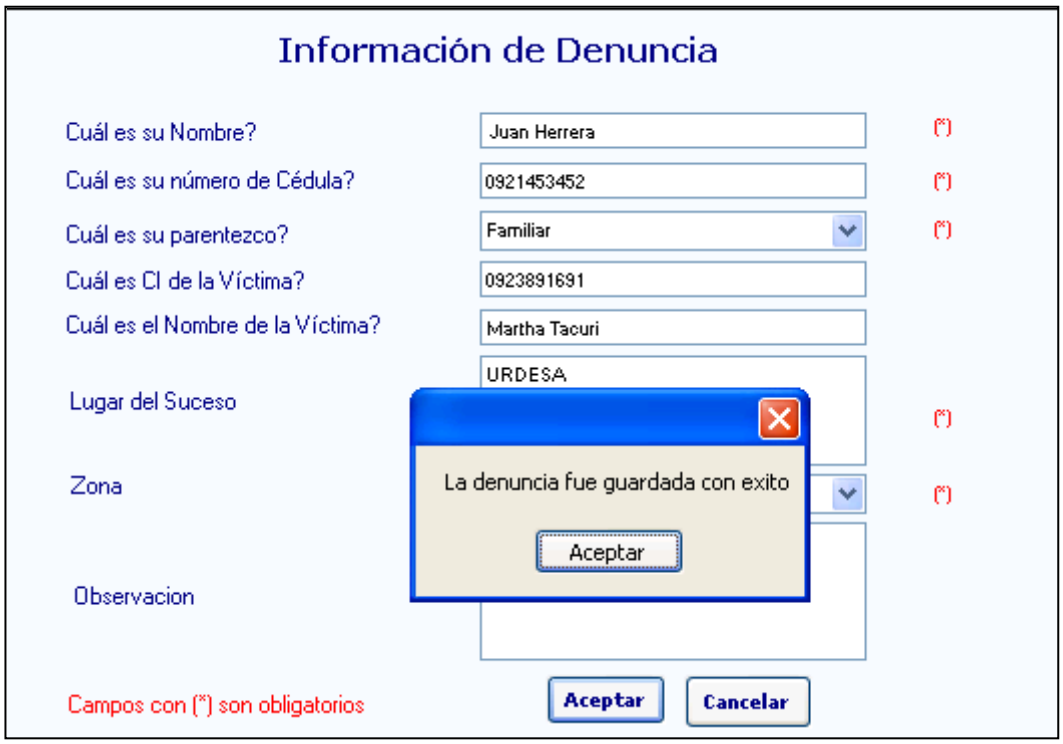


Figura 4.16 *Pantalla donde observamos los datos de la denuncia guardadas.*

Fuente: *Autores*

Una vez detectada la alerta por la Institución Bancaria, ésta se encargará de verificar la veracidad de dicha denuncia a través de preguntas aleatorias que solo el usuario sabrá responderlas.

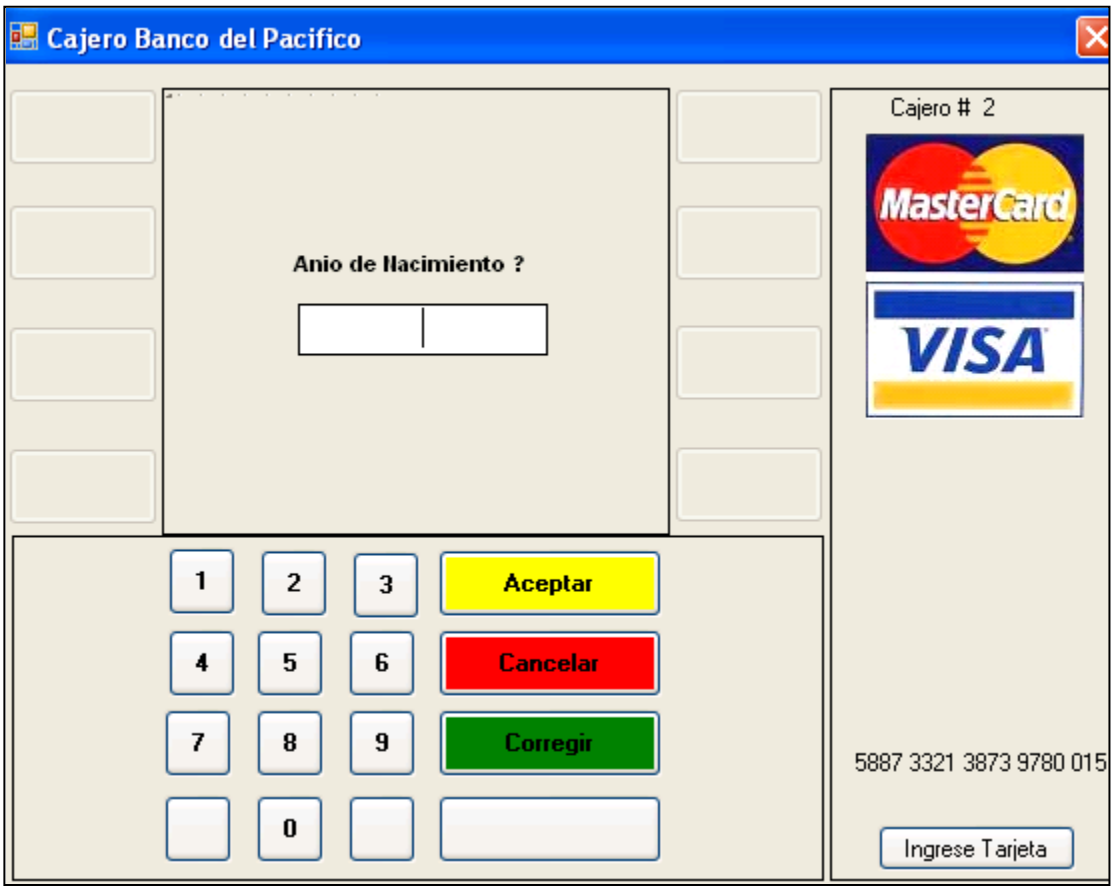


Figura 4.17 *Pantalla donde se muestra la pregunta aleatoria utilizada para comprobar la veracidad de la denuncia.*

Fuente: *Autores*

Si el usuario ingresa correctamente la respuesta a dicha pregunta, el cajero mostrara una nueva pantalla donde tendrá que digitar su clave sea esta de auxilio (si la persona realmente es victima de un secuestro) o la normal (si dicha denuncia fue falsa).

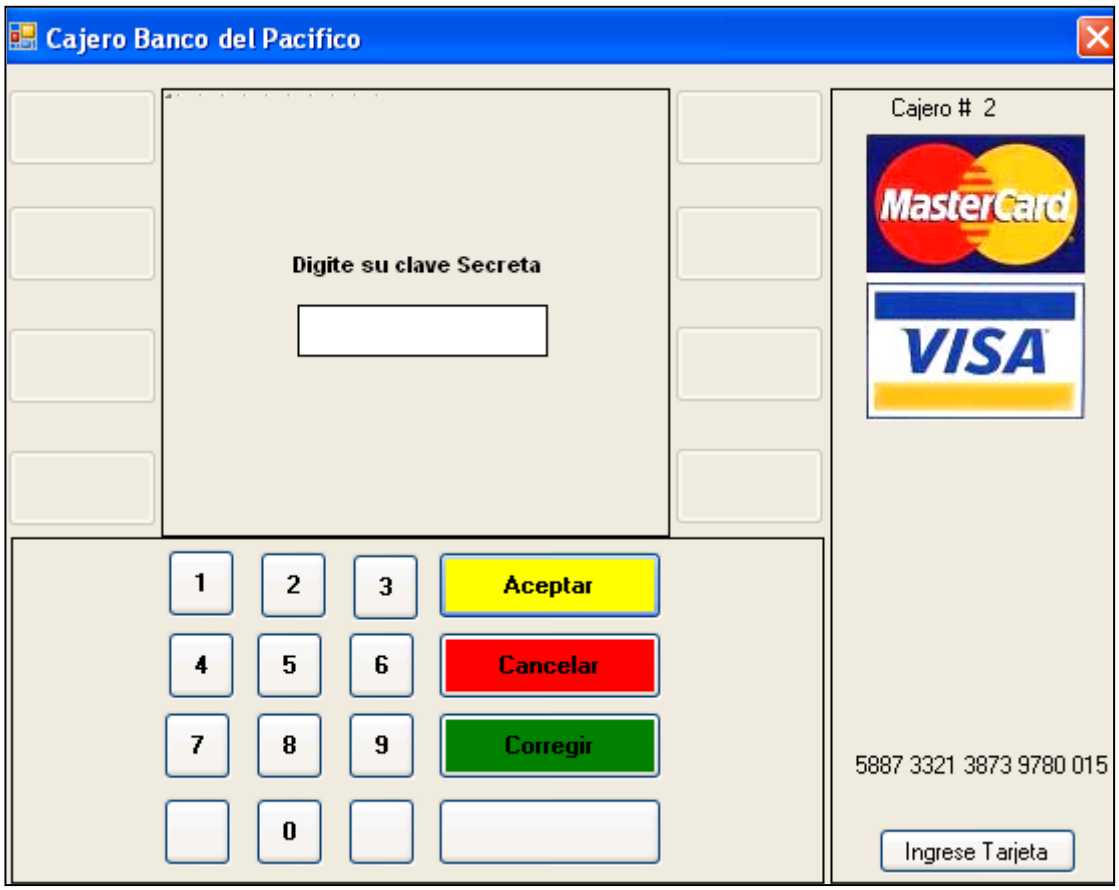


Figura 4.18 *Pantalla donde se visualiza el ingreso de la clave.*

Fuente: *Autores*

Cabe mencionar que las denuncias ingresadas por los receptores pueden presentar tres (3) estados:

- Pendiente (la denuncia se encuentra en espera, no ha sido designada).
- Despachado (cuando la denuncia ha sido asignada a la Entidad).
- Solucionado (cuando se ha tomado alguna acción en relación a la denuncia).

Figura 4.19 *Pantalla donde se visualiza el estado de las denuncias.*

Fuente: *Autores*

4.6.2 Prueba de Eficiencia

Esta prueba fue realizada para obtener el tiempo promedio de espera en el caso de que ocurra cualquiera de las dos situaciones mencionadas al inicio de nuestra tesis.

Primera Situación: tiempo de espera desde que el usuario (víctima) ingresa la clave de alerta hasta cuando se despacha la ayuda policial por parte de la Entidad de Seguridad.

NÚMERO DE PRUEBA	TIEMPO(s)
1	0:0:12
2	0:0:10
3	0:0:9
4	0:0:3
TOTAL	0:0:34

PROMEDIO = TOTAL/4	0:0:8.5

Segunda Situación: tiempo de espera desde que la Entidad de Seguridad recepta una llamada de auxilio sobre un posible secuestro express hasta cuando esta alerta es dirigida a las Entidades Bancarias donde la víctima es cliente.

NÚMERO DE PRUEBA	TIEMPO(s)
1	**0:1:05**
2	**0:1:00**
3	**0:0:48**
4	**0:0:44**
TOTAL	**0:3:37**
PROMEDIO = TOTAL/4	**0:0:54.25**

CAPÍTULO 5

5 ANÁLISIS FODA, FACTIBILIDAD Y MATERIALIZACIÓN DEL PROYECTO

5.1 FODA

5.1.1 Fortalezas

- Brindar apoyo a la ciudadanía con un sistema de seguridad que permita no reducir sus ahorros cuando se es víctima de un secuestro express.
- Brindar a las instituciones la confianza que podrán ganar los usuarios con un sistema que le ayude a salvaguardar su dinero.
- Sistema de Seguridad innovador, que permitirá reducir el secuestro express con modalidad de retiro obligado de dinero en nuestra ciudad.
- La transferencia de datos entre Entidades son seguros y confiables.
- Es desarrollado utilizando los protocolos más confiables con lo que se refiere a seguridad en el envío de datos.
- Creación de datos estadísticos confiables para el uso de instituciones y/o personas.

5.1.2 Oportunidades

- Es extensible a diferentes áreas donde se requiera tener bajo buen recaudo un bien personal, no solo en el área bancaria.
- En vista a la inseguridad y la falta de un sistema que ayude a los ciudadanos a estar seguros, entrar en los diferentes mercados no será muy complicado.
- Tener la oportunidad de crecer a nivel nacional, debido a que todas las instituciones Bancarias y/o empresas desean brindar seguridad a sus clientes.
- Con el uso de nuevas tecnologías, apoderarnos del mercado puesto que no existe muchos competidores en el mercado.

5.1.3 Debilidades

- Se requerirá personalización para poder establecer nuestros módulos en las diferentes áreas donde se requiera seguridad.
- La infraestructura es cambiante para lo cual se necesitará de mantenimiento constante tanto a nivel de hardware y software.
- Que la seguridad en la transferencia de datos, sea violentada por hackers y a su vez los datos hayan sido alterados.

- Inseguridad en la implementación del módulo por parte de las entidades Bancarias.

5.1.4 Amenazas

- La competitividad en la calidad y costos del producto ya que en la actualidad todos buscamos métodos seguros para mantener nuestros recursos.
- Empresas de Seguridad ofrezcan sus servicios a menores costos y con mayor capital humano.
- Que el mercado cree productos sustitutivos para brindar seguridad a los usuarios.
- Falta de acceso a posibilidades de capacitación y/o actualización de nuevas tecnologías a nuestro módulo.
- En el sistema de alerta que genera la Corporación, se debe tener precaución que la llamada no sea usada para hacer daño a una tercera persona.

5.2 FACTIBILIDAD DEL PROYECTO

5.2.1 Descripción de los servicios del sistema

El proyecto ofrece un sistema de alerta entre la Institución Bancaria y la Corporación para aplacar el secuestro express.

- **Detección instantánea de la clave de auxilio.**

Nuestro sistema proporciona una detección instantánea de la clave de auxilio en el momento que el usuario la ha ingresado.

- **Proporcionar la ayuda inmediata en caso de secuestro express.**

La Entidad de Seguridad recibirá constantemente alertas que hayan sido enviadas de la Entidad Bancaria al Web Service, al ser afirmativo dicho evento la Institución de Seguridad (C.S.C.G) despachará el incidente inmediatamente y registrará las acciones que han sido tomadas para dicha situación.

Un sistema de alerta entre la Corporación y la Institución Bancaria, cuando la Corporación es la que recibe una llamada sobre un posible secuestro express.

- **Proporcionar un aviso de alerta inmediata a la Institución Bancaria.**

En el momento que la Corporación recibe una llamada de un posible secuestro express, estos datos son verificados por medio de la cédula de identidad de la víctima y enviados al Banred para que éste proceda con la información sobre sus diferentes cuentas y a que Entidades Bancarias pertenece, si el nombre de la victima coincide con la de algún cliente, entonces la Institución Bancaria debe tomar las medidas preventivas y así evitar que se cometa dicho delito.

5.3 MATERIALIZACIÓN DEL PROYECTO

5.3.1 Costos de Desarrollo e Implementación

Los costos de los artículos utilizados para el desarrollo del sistema son:

TIPO DE GASTOS	COSTO INDIVIDUAL	CANTIDAD	COSTO TOTAL
Equipos	$ 1.500,00	3 portátiles	$ 4.500,00
Gastos de Oficina	$ 50,00	5 meses	$ 250,00
Software	$ 745,00		$ 745,00
Sueldos	$ 500,00	3 personas x 5 meses	$ 7.500,00
Hosting Principal	$ 405,00		$ 405,00
Hosting Back up	$ 210,00		$ 210,00
Costos de Enlace	Se utiliza la misma infraestructura de las entidades involucradas en la Red Colaborativa		
Imprevistos	$ 1000,00		$ 1000,00
			$ 14.610,00

Tabla 4 Costos para el desarrollo del sistema.

Fuente: Autores

CALCULO DEL TIR:

0 = 14610 / (1 + i)0 +2000 / (1 + i)1+2000 / (1 + i)2+2500 / (1 + i)3+3000 / (1 + i)4 +3000 / (1 + i)5 +3500 / (1 + i)6 +4000 / (1 + i)7 +4000 / (1 + i)8

TIR = 5%

Dado que se obtuvo una TIR positiva y mayor a la tasa mínima que se ganaría si se invirtiera el dinero en alguna entidad bancaria, se concluye que el proyecto es factible de realizar.

5.4 ANÁLISIS DE VIABILIDAD

Realizar un análisis de viabilidad es muy importante, ya que por medio de él sabremos con exactitud si un proyecto es factible o no. Este proyecto toma en cuenta los siguientes análisis.

5.4.1 Análisis Costo – Beneficio

El análisis costo – beneficio nos permite definir con mayor factibilidad todas las alternativas planteadas para la realización del proyecto.

5.4.1.1 Costos

En los últimos años el delito del Secuestro Express con modalidad de retiro obligado de dinero se ha incrementado convirtiéndose en un problema que aqueja financiera y psicológicamente a los usuarios.

- Según el Diario Expreso el 2009 fue el año del Secuestro Express del 1 de enero hasta el 18 de diciembre de 2009, las denuncias estuvieron en 269 casos. ***Fuente: Domingo, 27 de diciembre de 2009, Diario Expreso***.

- Según el Centro de Estudios e Investigaciones Estadísticas del ICM (ESPOL) desde el 1 de Enero hasta finales del mes de Diciembre del 2010 las denuncias estuvieron en 323 casos. ***Fuente: www.icm.espol.edu.ec/delitos***

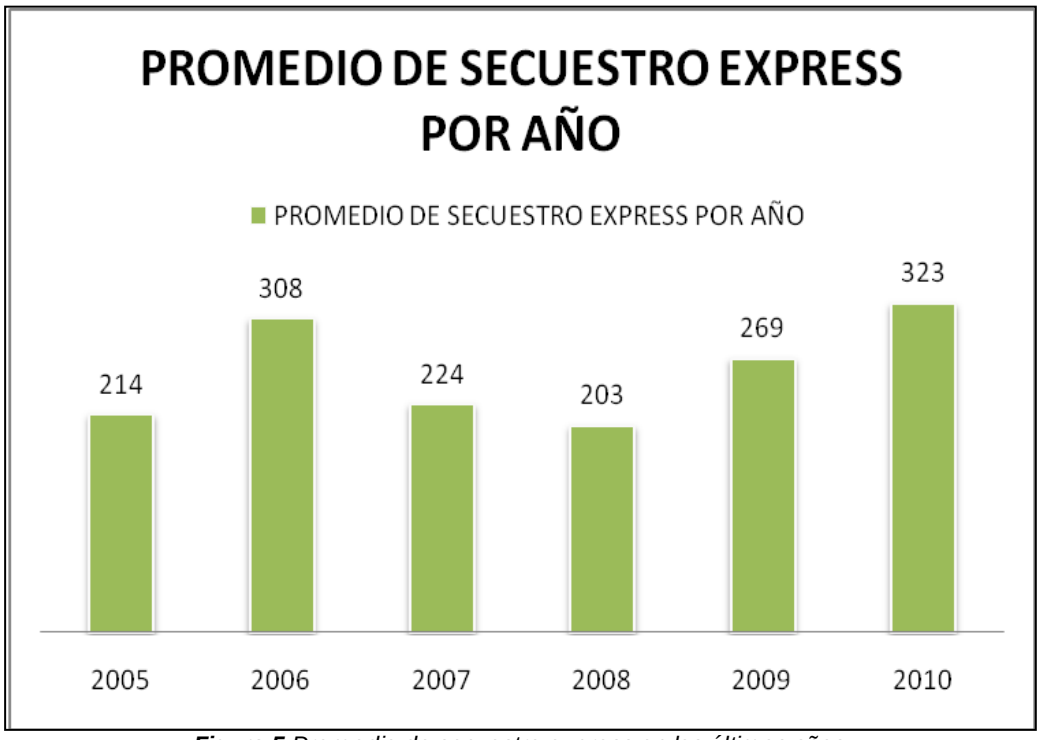


Figura 5 *Promedio de secuestro express en los últimos años.*

Fuente*: Autores*

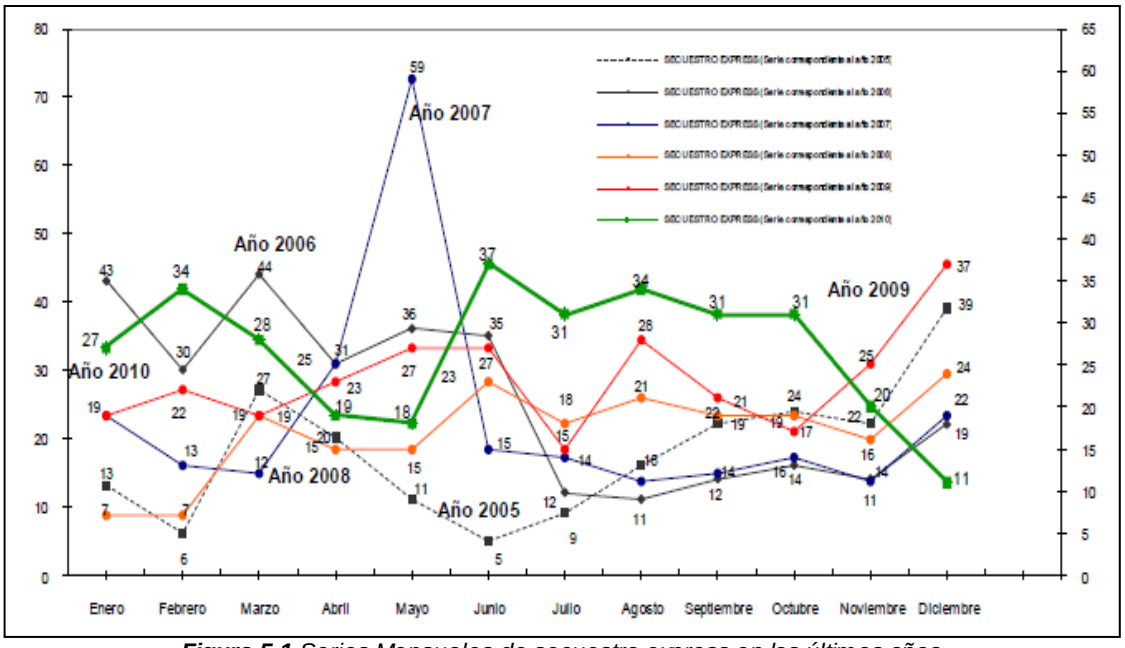


Figura 5.1 *Series Mensuales de secuestro express en los últimos años.*

Fuente: *www.icm.espol.edu.ec/delitos.*

En los costos que involucra esta lucha contra el SECUESTRO EXPRESS, tenemos los siguientes puntos importantes:

1. Costos relacionados con los daños psicológicos de la víctima que pueden derivar en la carencia de confianza y la capacidad de actuar ante cualquier peligro en un entorno ya que muchas veces estas víctimas no solo sufren pérdida de pertenencias sino que algunos han sido agredidos físicos y sexualmente.
2. Costos relacionados con la parte financiera de la víctima puesto que estos delincuentes roban todos sus objetos de valor, sus documentos y el dinero de sus cuentas.
3. Costos relacionados con las labores policiales muchas veces combinados con las Fuerzas Armada, en los operativos realizados en las zonas más conflictivas e inseguras de la ciudad de Guayaquil.
4. Costos relacionados en la entrega de plaquillas a los taxis amarillos por parte de la CTG para asegurar que éste pertenece a una cooperativa legal de transportes, se hace esto debido a que el 66% de las víctimas han sido ocupantes o pasajeros de dicho vehículo.

Como se puede observar los principales costos que intervienen en este proyecto son los que a continuación presentaremos, colocando junto a ellos una

ponderación entre 1 a 10 donde 1 es un costo mínimo y el 10 un costo máximo, esta ponderación se la realiza para determinar la proposición de valor del proyecto. De la misma manera se hace con los beneficios.

- Costos Monetarios: $ 10’000.000 aprox. (9)
- Tiempo : 4 horas y media aprox. (9)

5.4.1.2 Beneficios

Entre los beneficios que nos brinda el uso de un Sistema de Alerta con el fin de aplacar el Secuestro Express son los siguientes:

- Funcionales
    1. Detección automática de un secuestro express en progreso mediante la clave de auxilio ingresada por la victima. (6)
    2. Los Datos enviados son confidenciales y tienen la debida seguridad para que no sean alterados por terceras personas. (8)
- Emocionales
    1. Mejora el rendimiento policial.(6)
    2. Reduce el riesgo de que la víctima pierda todo su bien monetario por parte de los delincuentes.(8)
    3. Confianza hacia las Instituciones Bancarias que protegen los intereses de sus clientes, (7)

Proposición de valor = ∑ Beneficios/ ∑ Costos

= 35 / 18 = 1,94

Como se puede observar el resultado obtenido de la proposición de valor es mayor a 1, lo cual nos indica que la implementación de este proyecto, disminuirá los costos producidos cuando se produce un secuestro express.

5.5 ANÁLISIS DE DEBILIDADES Y FORTALEZAS DE LAS TECNOLOGÍAS

TECNOLOGÍA	FORTALEZA	DEBILIDAD
Firmas Digitales	Asegura la autenticidad de quien envía el mensaje al tener una entidad adicional que verifique la veracidad del certificado.	Para que funcione bidireccionalmente todos los clientes deben tener certificados instalados en sus máquinas, esto no es viable para todo tipo de usuario.
Autenticación	Es ideal para pocos	Si existen muchos

usuario/Contraseña	usuarios y servicios específicos para usuarios.	usuarios entonces la administración es más complicada.
Encriptación Mensaje SOAP	Si la llave es lo suficientemente fuerte, el sistema asegura que el mensaje SOAP no va a ser accedido fácilmente	Al encriptar los mensajes se vuelven más grandes por lo tanto más pesados para el tráfico, adicionalmente se requiere que el cliente tenga acceso a la clave de encriptación dificultando la administración.

CONCLUSIONES Y

RECOMENDACIONES

CONCLUSIONES

1. Con la elaboración del Análisis FODA, nos hemos dado cuenta que nuestro sistema es único e innovador y eso es una ventaja para poder lograr el alcance que deseamos.

2. Se concluyó que nuestro sistema es un buen recurso a implementar en la CSCG (Corporación para la Seguridad Ciudadana de Guayaquil), debido a que ellos están siempre dispuestos a trabajar por el bienestar de la Seguridad de los Ciudadanos.

3. Los reportes y gráficos estadísticos generados por nuestro sistema demuestran los resultados en una forma clara y detallada, los cuales permiten una mejor interpretación de los datos obtenidos.

4. Se demostró a través de las varias pruebas que el envío y recepción de alertas se mantiene confiable e inalterable debido al uso de seguridades que nuestro sistema maneja.

RECOMENDACIONES

1. Las configuraciones de Seguridad que se han implementado en el WebService, se deben revisar objetivamente cada 6 meses y realizar los ajustes necesarios en beneficio de salvaguardar la información.

2. Se debe promover la formación en seguridad, lo cual podría hacerse ofreciendo entrenamiento al personal, asistiendo a conferencias o cursos.

3. El usuario (receptor) del sistema debe ser debidamente capacitado antes de la utilización del módulo para que no existan errores en el uso debido del mismo.

4. A los usuarios de las Entidades Bancarias se les deben educar en el manejo de sus claves (clave normal y clave de auxilio) y cuando usarlas, para que a futuro no tengan algún problema y se vean afectados.

ANEXOS

ANEXO A

CODIGO DE VERIFICACION DE CLAVE

```
SqlDa.Fill (Dataset);
 if (Dataset.Tables[0].Rows. Count > 0)
 {
   cliente.Nombres = Convert.ToString (Dataset.Tables [0].Rows [0][0]);
   cliente.Apellidos = Convert.ToString (Dataset.Tables [0].Rows [0][1]);
   cliente.Ci = Convert.ToString (Dataset.Tables [0].Rows [0][2]);
   cliente.Direccion =Convert.ToString (Dataset.Tables [0].Rows [0][3]);
   cuenta.setIdcuenta(Convert.ToInt32(Dataset.Tables[0].Rows[0][4]));
cuenta.setSaldoactual(Convert.ToInt32(Dataset.Tables[0].Rows[0][5]));
  if (key == Convert.ToString(Dataset.Tables[0].Rows[0][6]))
     {
       Pswnormal = true;
     }
  if (key == Convert.ToString(Dataset.Tables[0].Rows[0][7]))
     {
       Pswauxilio = true;
}
```

ANEXO B

CODIGO DE RECEPCION Y ENVIO DE INFORMACION A LA CSCG

```
m_service = new AlertaWeb.AlertaWS ();
                    // Subscribe for event

m_service.nuevaAlerta (cliente.Nombres, cliente.Apellidos, cliente.Ci,
banco.Nombrebanco, cuenta.getNumcuenta (), cajero.Direccioncajero, new DateTime
(), 1, m_alertID);

private void bguardar_Click(object sender, EventArgs e)
      {
         RegistroAuxilio r = new RegistroAuxilio ();
         String query = "", usu= "", pss = "";
         int idusu = 0;
         String nombre = "", banco = "", civictima ="", direccion ="", idaux = "";
         update = new AlertaWeb.AlertaWS();
         update.alertaDespachada (Convert.ToInt32(txtid.Text.Trim()));

         banco = txbanco.Text;
         civictima = txtci.Text;
         direccion = txtdireccion.Text;
         nombre = txtvictima.Text;
         idaux = (this.txtid.Text);

         r.setAcciontomada (this.comboPatrulla.Text.TrimEnd ());
         r.setBanco (banco.TrimEnd ());
         r.setCiVictima (civictima.TrimEnd ());
         r.setNomVictima (nombre.TrimEnd ());
         r.setIdauxilio (Convert.ToInt32 (idaux));
         r.setIdoperador (Convert.ToInt32 (this.lbidope.Text));

         if (GrabarAccionesTomadas(r))
         {
            MessageBox.Show ("Las acciones han sido grabadas con éxito.");
         }
         else
         {
            MessageBox.Show ("No se pudo realizar la grabación, intente nuevamente.");
         }
```

```
            this.Close ();
        }

public void alertaDespachada(int id)
{
            this.Invoke ("alertaDespachada", new object [] );}
```

ANEXO C

CODIGO DE INGRESO DE DENUNCIA

```
if (nombredenunciante == "" && ceddenunciante == "" && parentezco == "" &&
nombrevictima == "" && clave == "")
{
    MessageBox.Show ("Debe ingresar los campos solicitados");
    t_denunciante.Text= “”;
    t_ceddenunciante.Text = "";
    t_nomvictima.Text = "";
    }
 else if (ceddenunciante != "")
 {
   if (ceddenunciante.Length != 10 || !EsCedulaValida(ceddenunciante))
   {
      MessageBox.Show ("Cédula de Denunciante Inválida, ingrese nuevamente");
       t_ceddenunciante.Text = ""
    }
}
 else if (cedulavictima.Length!= 10 || !EsCedulaValida(cedulavictima))
{
    MessageBox.Show ("Cédula de Víctima Inválida, ingrese nuevamente");
    t_cedvictima.Text = "";
 }
else if (!(EsNombreValido(nombredenunciante)))
 {
     t_denunciante.Text = "";
     MessageBox.Show ("No debe ingresar números, nombre de Denunciante
inválido");
 }
else if (!(EsNombreValido(nombrevictima)))
{
   t_nomvictima.Text = "";
   MessageBox.Show ("No debe ingresar números, nombre de Victima inválido");
 }
```

ANEXO D

CODIGO DE ENVIO DE INFORMACION AL BANRED

```
//envio de mensaje de Banred a Instituciones Financieras//

      byte[] outStream = encoder.GetBytes(t_clave.text);
      serverStream.write(outStream,0, outStream.Length);
      serverStream.Flush();
      clientetcp.close();
     }
   }
catch(Exception ex)

try
{
//Broadcast
this.tcpListener = new TcpListener (PAddress.Any, 9050);
this.listenThread = new Thread(new ThreadStart(ListenForClient));
this.listenThread.Start ();
}
this.psw.Text = “”;
Lbsaldoactual.Text = “”;
Lbsaldoficticio.Text = “”;
Lbreal.visible = false;
Lbficticio.visible = false;
this.quitarColorDiagrama (1);
this.seteoColorDiagrama (2);
Idtarjeta = ts.leerNumTarjetaAleatorio ();
this.num.visible = true;
this.num.Text = idtarjeta;
flag = ts.verificarNumeroTarjeta(idTarjeta);
exisdemun = cs.existeDenunciaParaEstaCuenta (idTarjeta);

if(flag && ¡exisdemun)
{
this.psw.visible = true;
this.lbalerta.visible = false;
this.label1.visible = false;
this.secret.visible = true;
}
```

```
Else
{
  Else
{
  Tab6.Show ();
}}
}}
Catch(Exception exx)
{
Console.writeline (“ERROR EN EL INGRESO” +exx.Message);
}
```

ANEXO E

CODIGO PARA GRABAR ACCIONES

```
private Boolean GrabarAccionesTomadas (String dato)
 {
    String query1 = "", banco ="";
    String idoperador ="1";
    try
    {
        banco = dato.Substring (0, (dato.IndexOf (',')) - 1);
        Conexion conn = new Conexion ();
        con = new SqlConnection(conn.obtenerConexion());
        query1 = "insert into dbo.registroauxilio (banco, idoperador, acciontomada) values
('" + banco + "','" + idoperador + "','" + dato + "')";
        cmd = new SqlCommand(query1, con);
        SqlData = new SqlDataAdapter (cmd);
        Dataset = new DataSet ();
       con.Open ();
       SqlData.Dispose ();
       cmd.Dispose ();
       con.Close ();
       return true;
```

ANEXO F

LISTA DE PRECIOS DE HOSTING

Comparaciones entre Hosting

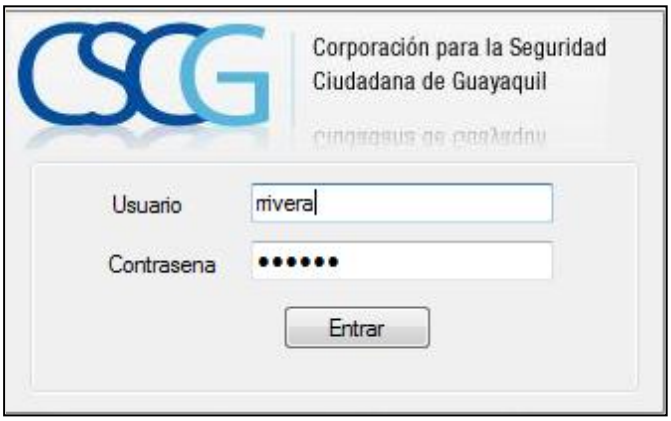
	TELCONET	COMPUVISIÓN	ECUAHOSTING	VISIONET
Almacenamiento	250 MB	ILIMITADA	2000 MB	1000 MB
Transferencia	7 GB	ILIMITADA	5000 MB	5000 MB
Soporte para Plataformas	PERL, ASP Y PHP	ASP, .NET	ASP	ASP, PHP
Soporte para Bases de Datos	ACCESS, MySQL Y SQL SERVER	MS SQL, ACCESS	MySQL, MS SQL, ACCESS	MS SQL, ACCESS, MySQL
Cuentas POP3	10	--	ILIMITADAS	ILIMITADAS
Cuentas FTP	24 x 7	ILIMITADAS	ILIMITADAS	ILIMITADAS
Velocidad de Servidores	--	--	6100 MHz	3100 MHz
Server Memoria	--	--	16 GB	1024 MB
Costo del Hosting x Año	$ 350,00	$ 119,88	$ 199,00	$ 199,00
Costo del Dominio por Año	$ 55,00	$ 9,00	$ 11,00	$ 12,00
Total	$ 405,00	$ 128,88	$ 210,00	$ 211,00

ANEXO G

PANTALLA PRINCIPAL DEL CAJERO (PROTOTIPO)

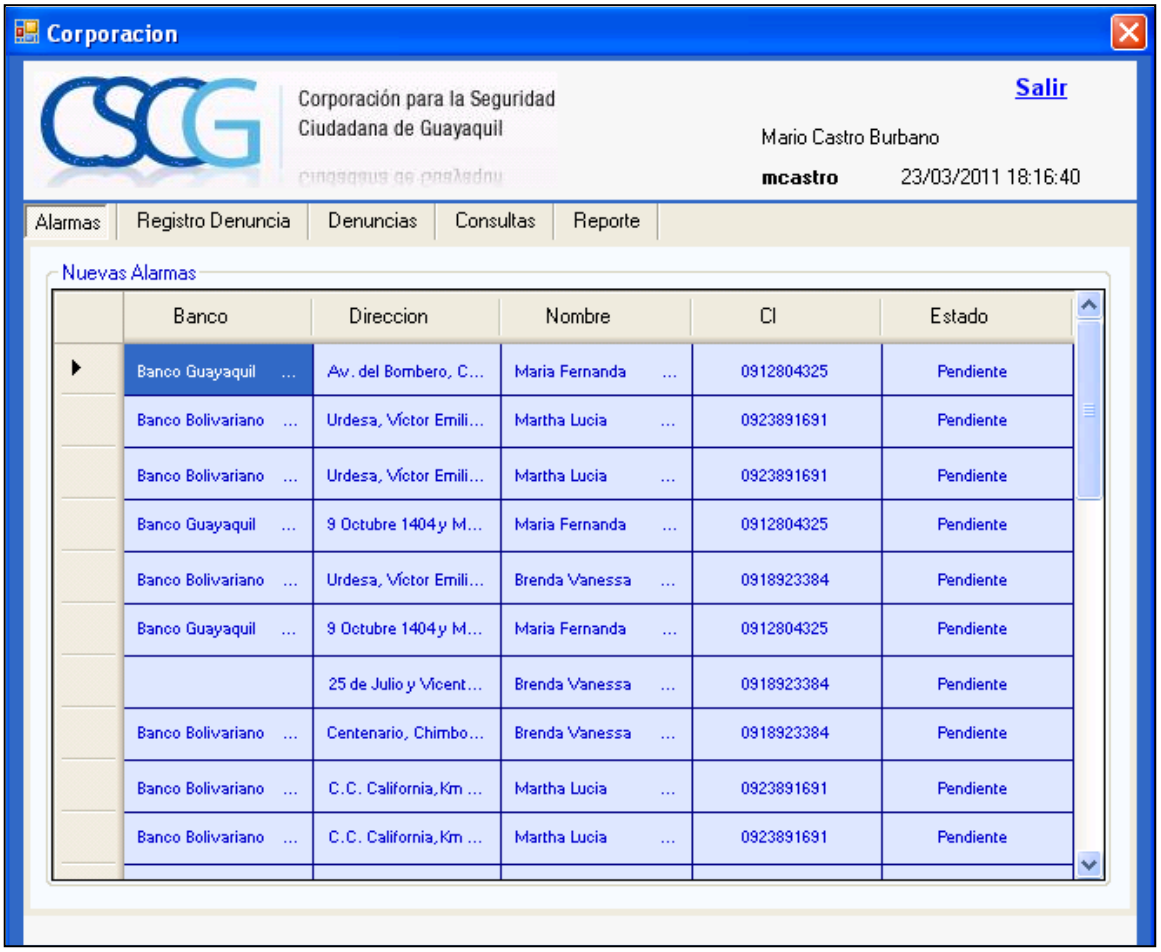
ANEXO H

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACIÓN "INGRESO DE USUARIO" (PROTOTIPO)



ANEXO I

PANTALLA PRINCIPAL DE MÓDULO PERTENECIENTE A LA CORPORACIÓN "RECEPCIÓN DE LOS DATOS DE ALARMA" (PROTOTIPO)

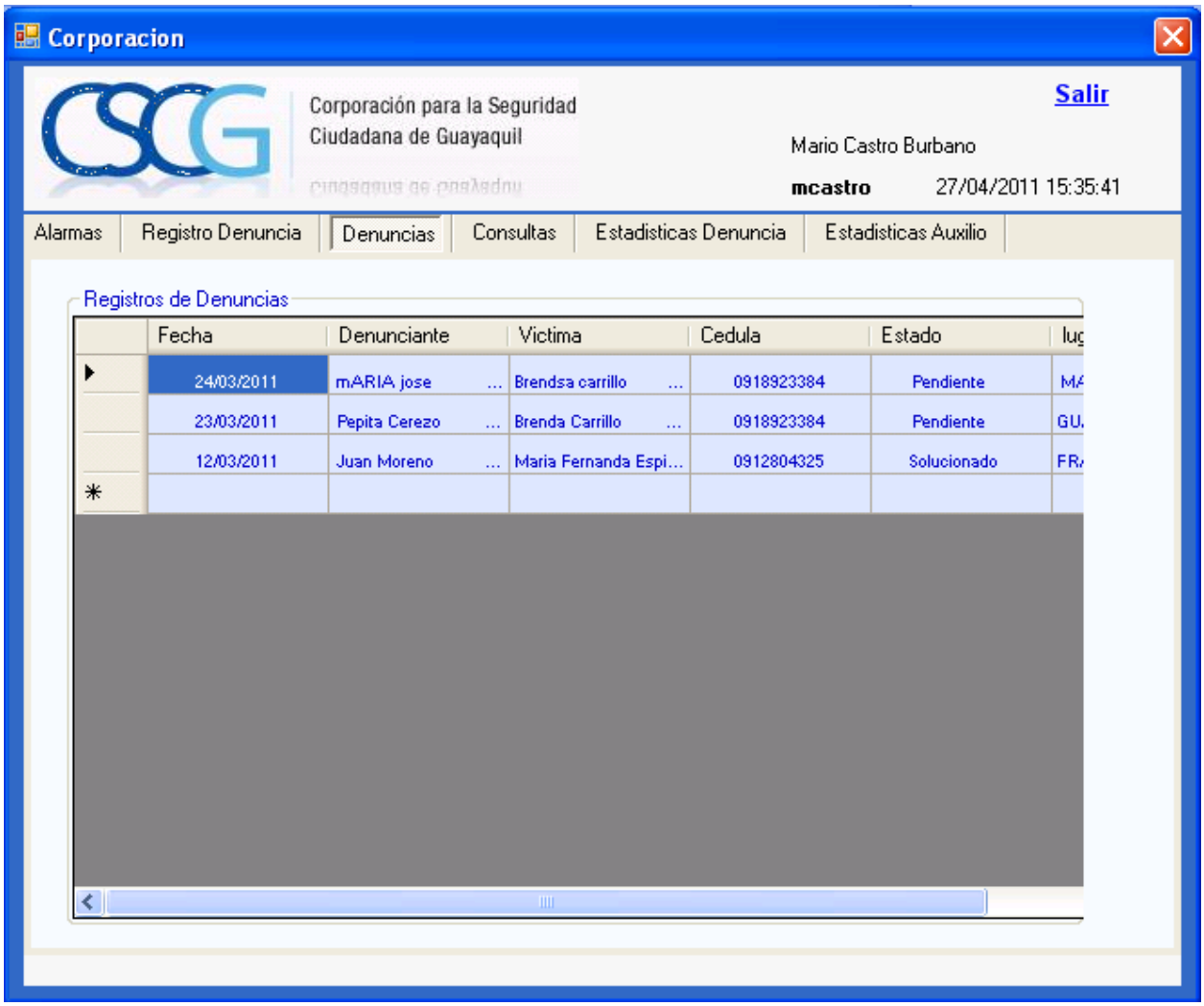


ANEXO J

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACIÓN "REGISTRO DE DENUNCIAS" (PROTOTIPO)

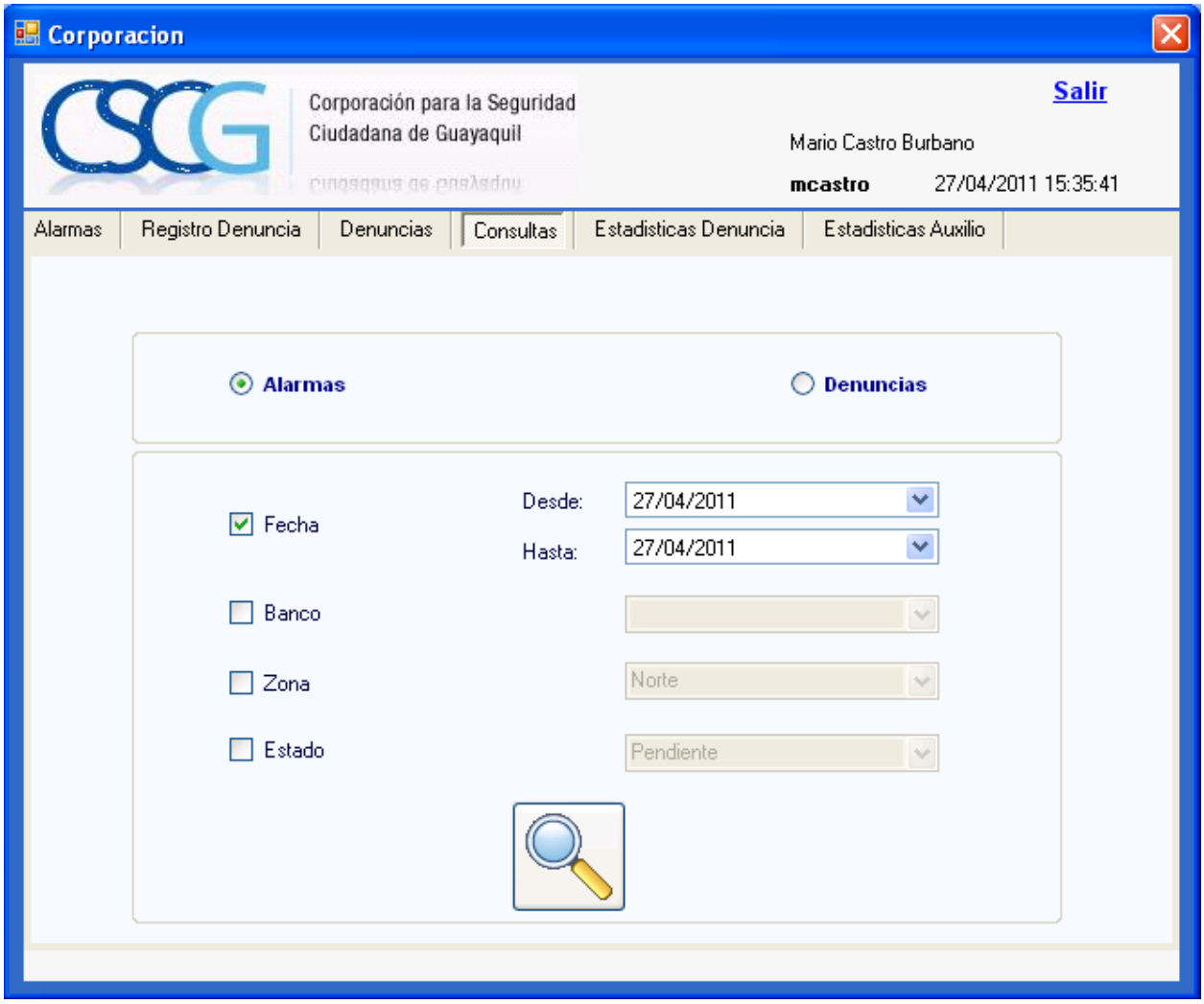
ANEXO K

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACIÓN "DENUNCIAS"



ANEXO L

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACIÓN "CONSULTAS"



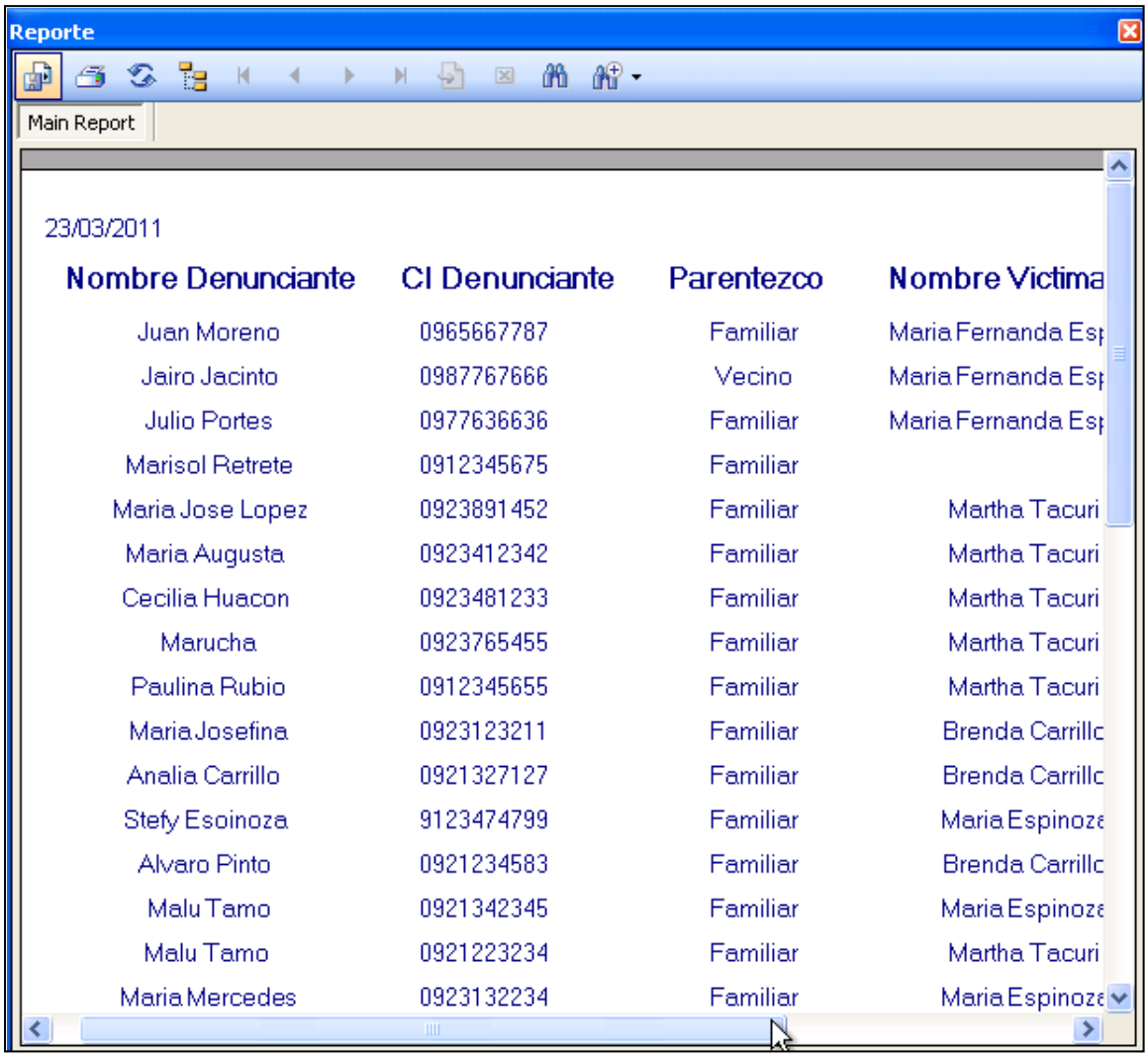
ANEXO L.1

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACIÓN "CONSULTAS" (ALARMAS).

Banco	Fecha	CI victima	Victima	Observacio	Estado
Banco del Pacifico	03/01/2011	0918923384	Brenda Vanessa Carrillo Arguello	envio de patrulla 100 para auxiliar a la victima 17 horas	Pendiente
Banco del Pacifico	03/03/2011	0918923384	Brenda Vanessa Carrillo Arguello	Se envian tres patrullas al sitio y una ambulancia	Despachado
Banco del Pacifico	03/03/2011	0918923384	Brenda Vanessa Carrillo Arguello	skldfjkldfs	Pendiente
Banco del Pacifico	03/07/2011	0918923384	Brenda Vanessa Carrillo Arguello	Se envia una unidad y se llama a los bomberos	Solucionado
Banco del Pacifico	03/07/2011	0923891691	Martha Lucia Tacuri Morocho	Se envia dos patrullas	Despachado

ANEXO L.2

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACIÓN "CONSULTAS" (DENUNCIAS)

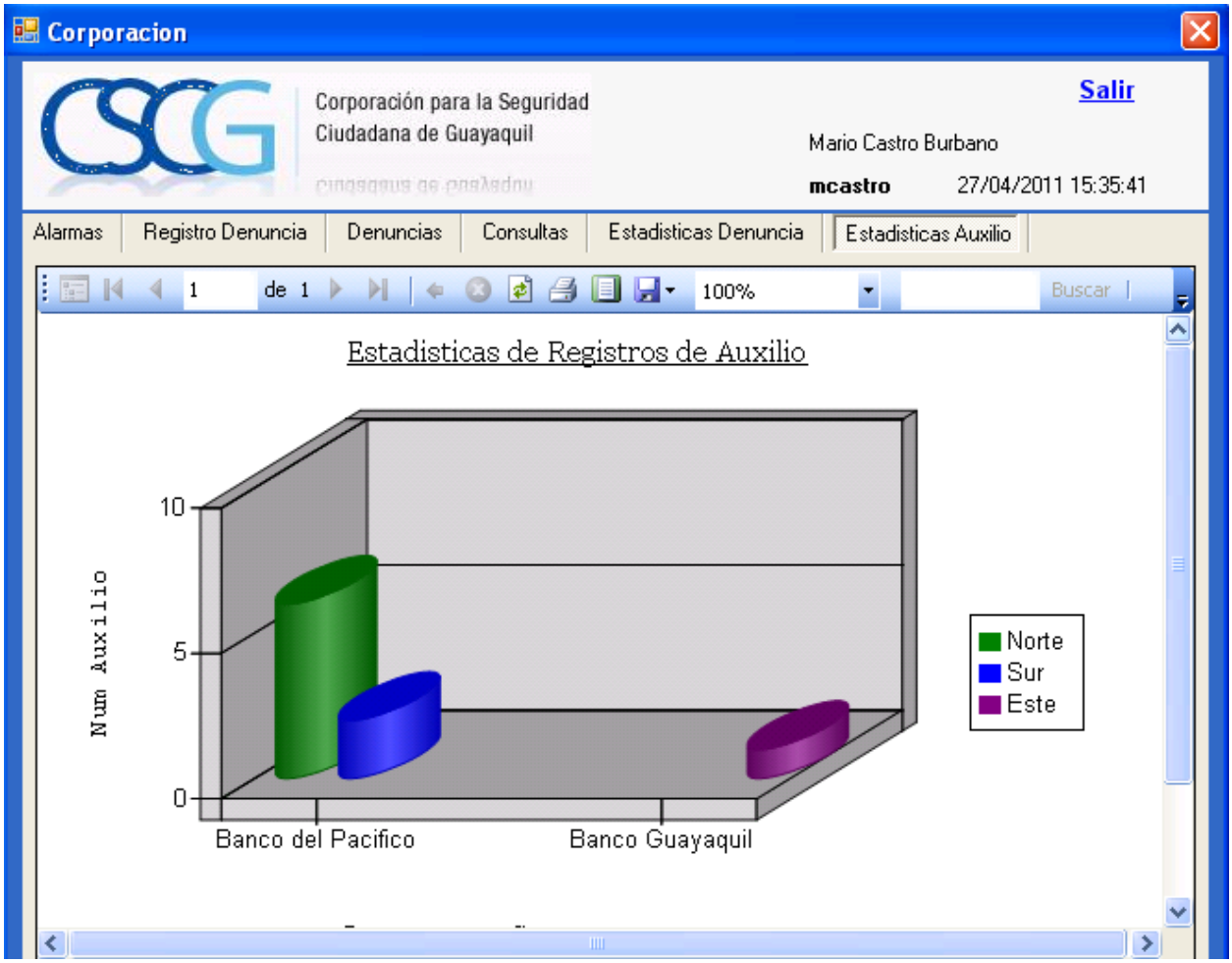


ANEXO M

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACION "ESTADISTICAS DENUNCIAS"

ANEXO N

PANTALLA PRINCIPAL DEL MÓDULO PERTENECIENTE A LA CORPORACION “ESTADISTICAS DE REGISTRO DE AUXILIO”



ANEXO O

PARTES INVOLUCRADAS

ENTIDAD BANCARIA

Banco Bolivariano

Analista. Ángelo Burbano. Programador.

Banco Guayaquil

Ing. Clemente Calderón. Gerente de Sistemas.

Ing. Lorena Tacury. Jefe de Soporte en Seguridad de Hardware.

ENTIDAD DE SEGURIDAD (C.S.C.G)

Ing. Álvaro Pinto. Administrador de Seguridad Informática.

Ing. Eduardo Yaguar. Administrador de Bases de Datos.

REFERENCIAS

REFERENCIAS BIBLIOGRÁFICAS

[1]Benjamín González C, XML Web Service, http://desarrolloweb.com/articulos/1545.php, 24 de Junio del 2004.

[2] Orlando Fabián Brea, Introducción a los Web Services en PHP, http://desarrolloweb.com/articulos/1852.php, 03 de Marzo del 2005.

[3] Roberto, Qué es y para qué sirve un Web Service, http://culturacion.com/2009/07/%C2%BFque-es-y-para-que-sirve-un-web-service/, 09 de Julio del 2009

[4]Juan Julian Merelo, Introducción a los Servicios Web y Microsoft .Net http://geneura.ugr.es/~jmerelo/ws/, 09 de Julio del 2002.

[5]Rich Salz, Securing Web Service, http://xml.com/lpt/a/1094, 15 de Enero del 2003.

[6]Daniel Sepúlveda, Protocolos Seguros, http://tejedoresdelweb.com/w/Protocolos_seguros, 31 de Marzo del 2008.

[7]Carlos Erazo, Protocolo TLS (Transport Layer Security), http://monografias.com/trabajos74/protocolo-tls-transport-layer-security/protocolo-tls-transport-layer-security.shtml, 17 de Julio del 2010.

[8] Instituto de Ciencias Matemáticas de la Escuela Superior Politécnica del Litoral., "Estadísticas de Delitos en la ciudad de Guayaquil", http://www.icm.espol.edu.ec/delitos, 05 de Enero del 2011.

[9]Marco Antonio Vázquez Esquivel, Base de Datos Telefónica, http://cursos.eie.ucr.ac.cr/claroline/backends/download.php?url=L03hcXVpbmFfQ2FqZXJvX0F1dG9t4XRpY28ucGRm&cidReset=true&cidReq=SP3100_001, 11 de Junio del 2009.

[10] Giusui Imbrenda y Willian Zurita, Tópico (Modelo Dinamico y Modelo Funcional), http://www.ldc.usb.ve/~vtheok/cursos/ci3711/apuntes/99-02-25/index.html, 25 de Febrero de 1999.

[11] Juan Gabriel Castillo, Informes Crystal Reports, http://www.elguille.info/colabora/NET2005/TheKin_proReportes.htm, 10 de Febrero del 2005.

[12]Jayaram Krishnaswamy, Generación de un simple Crystal Report utilizando VS 2005, http://www.aspfree.com/c/a/.NET/Generating-a-Simple-Crystal-Report-using-VS-2005/, 01 de Noviembre del 2006

[13]Nicolas Tedeschi, Web Service un ejemplo práctico,http://www.elguille.info/colabora/NET2005/elnatu_WebServices.htm, 08 de Junio del 2005.

[14] Sergio Tarrillo, Consumir un Web Service desde Windows .Form con C# y VB,http://www.elguille.info/colabora/NET2005/sergio_CallWebService.htm, 20 de Febrero del 2005

[15]Benjamín González, Vamos a hablar de los requerimientos que necesitan estas aplicaciones para ser ejecutadas, así como las estructuras de protocolos

sobre las que se asientan, http://www.desarrolloweb.com/articulos/1545.php, 24 de Junio del 2004.

[16]Orlando Fabián Brea, Explicamos qué son los servicios web y cuales son los elementos por los que están compuestos, http://www.desarrolloweb.com/articulos/1852.php, 03 de marzo del 2005.

[17]Share Point Magazine, Todo lo que necesitas saber sobre un BDC,http://sharepointmagazine.net/technical/administration/everything-you-need-to-know-about-bdc-part-3-of-8, 14 de Diciembre del 2008.

[18]Juan Julián Merelos Guervos, Introducción a los Servicios Web, http://geneura.ugr.es/~jmerelo/ws/, 09 de Julio del 2002.

[19]Microsoft, Acceso al Servicio Web, http://www.webnova.com.ar/articulo.php?recurso=426, Mayo del 2010.

[20]Rich Salz, Protección de Servicios Web, http://www.xml.com/lpt/a/1094, 15 de Enero del 2003.

[21]Daniel Sepúlveda, Protocolos Seguros, http://www.tejedoresdelweb.com/w/Protocolos_seguros, 15 de Mayo del 2010.

[22]Msdn**,** Acceso al Servicio Web, http://msdn.microsoft.com/es-es/library/ms580429.aspx, 15 de Noviembre del 2010.

[23]Msdn, Crear y Probar la Aplicación, http://msdn.microsoft.com/es-es/library/ms553011.aspx, 17 de Noviembre del 2010

[24]Msdn, Acceso a Base de Datos (C# y JAVA), http://msdn.microsoft.com/es-es/library/ms228366(VS.80).aspx, 19 de Noviembre del 2010.