DESARROLLO DE UNA APLICACIÓN MÓVIL DE SEGURIDAD CIUDADANA EN EL PERÚ UTILIZANDO INFORMÁTICA FORENSE

Development of a mobile application of Public Safety in Peru using Computer Forensics

Óscar Amao Quijandría[1], Augusto Cortez Vásquez[1,2]

PRESENTACIÓN: MAYO 2016 ACEPTACIÓN: JUNIO 2016

RESUMEN

La presente investigación presenta una solución para combatir la delincuencia mediante la telefonía móvil. Por tal motivo, se realizará una aplicación para combatir los hechos delictivos que se realizan por medio de los teléfonos inteligentes. Funcionaría utilizando un sistema que verifique hechos delictivos y los guarde en un servidor para que, finalmente, el usuario pueda evitar ser víctima de algún delincuente; además, se ofrecería la posibilidad de alertar a los demás usuarios. Los datos guardados en el servidor se almacenarán de una forma correcta que les permita ser tomados en cuenta en procesos legales, para lo cual se aplicará la informática forense.

Palabras clave: Seguridad ciudadana, Telefonía móvil, Android, Informática Forense.

ABSTRACT

The present research is a solution to combat crime via mobile phone, for this reason an mobile application will be made to combat criminal acts that are performed by the Smartphone. Using a system to verify the offenses and keep them in a server so that finally the user can prevent and not be the victim of the alleged offender, in addition to alerting other users. Data stored on the server will be stored in a correct way to be taken into account in legal processes, which apply computer forensics.

Keywords: Citizen Security, Mobile Phones, Android, Computer Forensics.

1 Facultad de Ingeniería de Sistemas e Informática - UNMSM. E-mail: rakso.x@hotmail.com

2 Facultad de Ingeniería - Universidad Ricardo Palma. E-mail: acortezv@urp.edu.pe

1. INTRODUCCIÓN

El surgimiento de la sociedad del conocimiento, construida sobre la base del intercambio de información en gran escala, posible gracias a las tecnologías de la información y comunicación, ha traído como consecuencia una reconfiguración de la sociedad mundial. Junto a ella, se presenta una serie de delitos que afectan la tranquilidad de la sociedad en su conjunto. La ciudadanía, entendida como «la cualidad y el derecho de los ciudadanos», ha sido uno de los objetos de estudio más prototípicos dentro de la sociología, la ciencia política y el derecho (Carrión, 2007). Por otro lado, la tecnología creada por el hombre debe estar al servicio de él y proporcionar herramientas para resolver los problemas que los acosan. Este trabajo de investigación presenta una solución para el problema de los delitos que atentan contra la seguridad ciudadana.

1.1 Antecedentes

Según los estudios, análisis y estadísticas, la inseguridad ciudadana ha ido aumentando no solo por la cantidad de personas que realizan actos delictivos, sino por las modalidades o herramientas que estas llegan a usar. La tecnología ha aumentado, en un primer momento, para ayudar a los usuarios, pero se ha utilizado, adicionalmente, con el fin de delinquir sin que se pueda penar a los responsables, debido a la falta de pruebas y por no repercutir en los derechos de los demás. De ese modo, se ha protegido a los supuestos culpables por los vacíos legales (INEI, 2014).

La OCDE[3] define al delito informático como cualquier comportamiento antijurídico, no ético o no autorizado, que esté relacionado con el procesamiento automático o transmisión de datos.

Según las últimas estadísticas que se realizaron sobre los actos delictivos, en una población de 100 personas, se examinó cuántas son víctimas de robo, estafa, intentos de robo y amenazas.

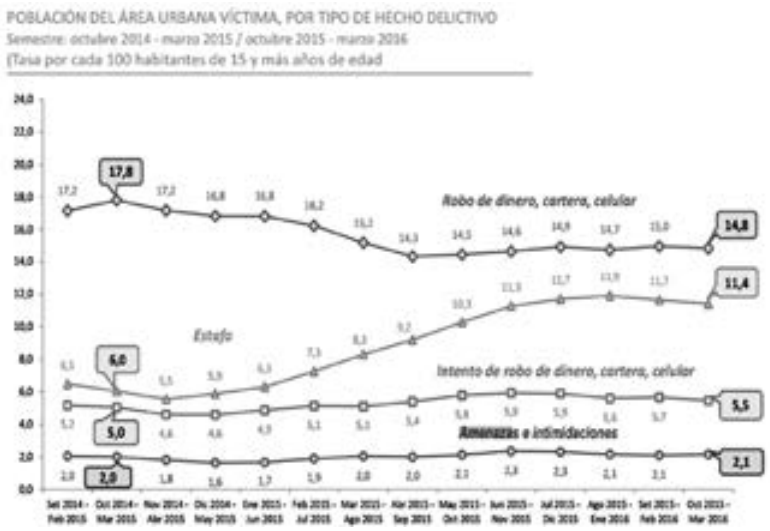

Fig. 1. Fuente: Instituto Nacional de Estadística e Informática (INEI). Informe Técnico – Estadísticas de Seguridad Ciudadana Nº 6 – Marzo 2016.

3 *OCDE: La* ***Organización para la Cooperación y el Desarrollo Económicos*** *es un organismo de cooperación internacional cuyo objetivo es coordinar sus políticas económicas y sociales.*

Como se puede apreciar, de cada 100 personas, 1,7 personas son víctimas de robo; 6,3, de estafa; siete, de intento de robo; y tres, de amenazas e intimidaciones.

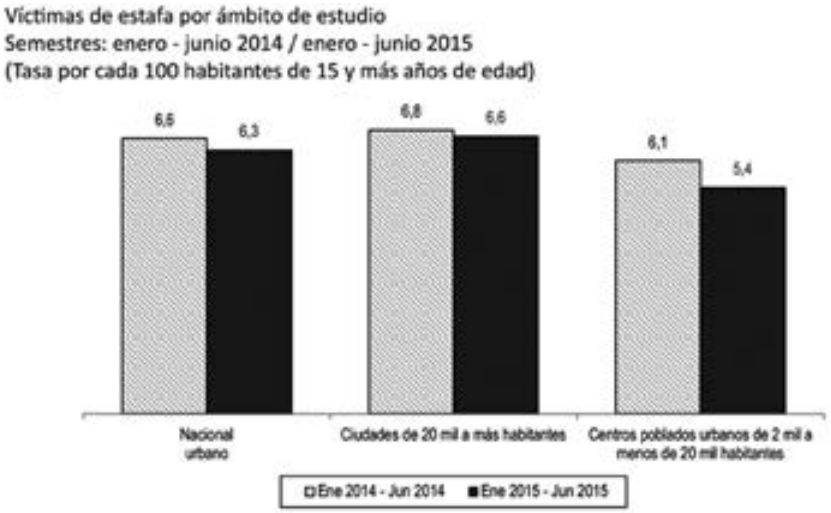

Fig. 2. Fuente: (Instituto Nacional de Estadística e Informática (INEI). Informe Técnico – Estadísticas de Seguridad Ciudadana Nº 3 Estafas – Setiembre 2014)

Vemos claramente que estos delitos ocurren generalmente de persona a persona. Sin embargo, también se pueden observar delitos que no necesariamente necesitan del contacto directo con la víctima, pues los delincuentes usan algún medio de comunicación para realizar estafas, amenazas o intimidaciones, y extorsiones, lo cual ayudaría a encubrir la identidad del criminal a través de un número desconocido por la víctima (García, 2014).

Las estafas que se muestran en la figura 2 son estadísticas que se separan pero que también se realizan por medio de equipos móviles.

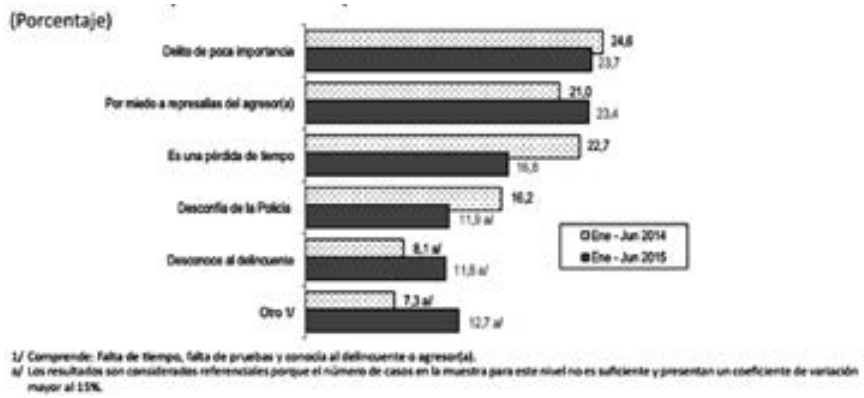

Fig. 3. Fuente: Instituto Nacional de Estadística e Informática (INEI). Informe Técnico – Estadísticas de Seguridad Ciudadana Nº 3 Motivos – Setiembre 2014.

Las amenazas o intimidaciones, las estafas o las extorsiones pueden ocurrir por medio de llamadas telefónicas, mensajes de texto, correos electrónicos y mensajes escritos que son dejados por debajo de

la puerta del hogar o negocio. No obstante, no todos estos delitos son denunciados. Como se puede apreciar en la siguiente gráfica de porcentajes, existen razones específicas por las que no se realizan las denuncias de los actos delictivos.

Situación problemática
Problema general
El mecanismo de seguridad y alerta al ciudadano es deficiente..

Problemas específicos
– No existe un medio para diferenciar una llamada amenazante de una normal;
– El registro de denuncias de hechos delincuenciales no está actualizado;
– El proceso de registro de denuncias es tedioso y complicado;
– No existe un repositorio de números amenazantes.

Objetivos
Objetivo general
– Desarrollar una aplicación móvil para mejorar el sistema de seguridad y alerta para filtrar los números amenazantes.

Objetivos específicos
– Construir un repositorio para el alojamiento de números sospechosos,
– Crear un sistema para detectar las llamadas de los números amenazantes,
– Brindar la facilidad para el registro de denuncia por medio del sistema,
– Implementar, validar y verificar la funcionalidad del sistema.

2. MARCO TEÓRICO
2.1. Delincuencia

La delincuencia se refiere a la cantidad de hechos delictivos que se realizan en un lugar. Gracias a ella, se puede conocer el nivel de inseguridad que hay en dicho sitio. Sin embargo, no necesariamente quien cometió un hecho delictivo es un delincuente, pues se puede llegar a probar que el acusado delinquió de forma accidental. Así lo señala Juan Vásquez (2007):

> Una persona que mate por accidente comprobado no es necesariamente un delincuente. Un niño que robe un pan para no morirse del hambre será anímicamente sano y no podremos considerarlo como infractor. En el seno de una comunidad existen individuos capases de respetar y observar las leyes, pero también hay otros para quienes esto resulta imposible.

Existe un conflicto entre el interés social y el interés de garantizar y proteger los derechos fundamentales de las personas, contra los cuales se rebela el delincuente. Hurtado Pozo (1996) señala, respecto del delincuente:

> La rebelión de éste contra el orden constituido lo convierte en un sujeto peligroso que, según evoca la expresión, debería ser eliminado, sometido o vuelto inocuo. Con este objeto, debe recurrirse a medios eficaces y, entre éstos, al Derecho Penal en especial (sic).

El delincuente es tomado como objeto de estudio de la criminología contemporánea, ya que, debido a él, se elabora una política que los sancione y proteja al ciudadano posiblemente afectado en un futuro (Guerra, 2013).

2.2. Seguridad

El término de seguridad, en general, puede definirse como un estado en el que no existen riesgos, que van desde la seguridad internacional hasta la seguridad de la persona. Cabe indicar que, en esta investigación, nos referiremos a la seguridad de la persona. Melissa Nobile González (2003) expresa: «Este concepto ha venido sufriendo transformaciones importantes a nivel teórico y práctico, en tanto a la intensa dinámica mundial ha requerido nuevas concepciones para lograr adaptarse a sus propias necesidades».

Si eso queda claro, se puede llegar a obtener diferentes conceptos según el lugar y el ámbito donde la palabra «seguridad» se mencione. En nuestro país, nos referimos a la seguridad como un servicio que debe ser prestado por el Estado en sus diversos ámbitos, como seguridad ciudadana, seguridad legislativa, entre otros (Info Región, 2007).

2.3. Ciudadanía

La ciudadanía tiene ámbitos que pueden diferenciarse. Existe la ciudadanía en el sentido político, que ve en dónde se rige y quién es el responsable de brindar derechos según su localidad. También, la filosofía la define como el deber de un ciudadano de tener carácter y sentido de ciudadanía. Para entender el concepto de ciudadanía es preciso definir el concepto de ciudadano. El *Diccionario de la lengua española* lo define de la siguiente manera: «Habitantes de las ciudades antiguas o de estados modernos, como sujetos de derecho políticos y que interviene, ejercitándolos en el gobierno del país».

Esta definición destaca la naturaleza del ciudadano en relación a los derechos políticos que ejerce en el país del cual es residente legal; es decir, la ciudadanía implica el reconocimiento de los derechos de un habitante por un Estado. Desde la posición de Alberto Olvera (2008), se puede decir que

> La sociología se pregunta por el origen histórico del estatuto de ciudadanía, por su evolución y desarrollo, y por el contenido de los derechos que constituyen la ciudadanía, y ubica estos procesos como parte de una larga etapa histórica en la que las relaciones entre los individuos y el Estado se han ido redefiniendo. La filosofía política se cuestiona sobre el carácter y el sentido de la ciudadanía, sobre el significado de ser ciudadano, sobre las relaciones que debe haber entre individuos y estado, y sobre las relaciones entre ciudadanía y democracia. Los dos enfoques son en realidad complementarios, pues se informan mutuamente

2.4. Seguridad ciudadana

La seguridad ciudadana se considera como un bien escaso para la población. Cada vez más, esta se ve disminuida en América Latina, pero no por las fuerzas policiales que ocurren en el país, ya que es el resultado de un trabajo en equipo entre las diferentes organizaciones que brindan este bien, como el Estado, las autoridades locales y la sociedad civil. Para poder aumentar la seguridad ciudadana se establecen ciertos parámetros, tanto en el lado judicial como en el estado de derecho, como el límite de la libertad, el pago de multas, las denuncias, etc. Así lo manifiesta Fernando Carrillo (2007):

> La seguridad ciudadana se ha convertido en un asusto prominente n la agenda de la consolidación democrática y el desarrollo de América Latina. Impone elevados costes económicos y se introduce en la vida política. La política como bien público, es responsabilidad primaria del Estado, pero también compete a las autoridades locales y la sociedad civil. Una estrategia global frente a la violencia requiere del fortalecimiento del Estado de Derecho, la reforma del sistema judicial y de la policía, de las prisiones, mayores esfuerzos en la prevención, y mayor participación de la sociedad civil.
>
> La seguridad ciudadana es una situación social en la que predomina la sensación de confianza, entendiéndola como ausencia de riesgos y daños a la integridad física y psicológica. Con ella, el Estado debe garantizar la vida, la libertad y el patrimonio ciudadano.

Según la Ley No 27933, Ley del Sistema Nacional de Seguridad Ciudadana, se entiende por Seguridad Ciudadana lo siguiente:

> la acción integrada que desarrolla el Estado, con la colaboración de la ciudadanía, destinada a asegurar su convivencia pacífica, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos. Del mismo modo, contribuir a la prevención de la comisión de delitos y faltas (Zárate et. al., 2013).

2.5. Delitos

El delito es una conducta humana que se opone al orden y la ley. Esta última es la que establece qué hechos son considerados como tales. Por tanto, el delito puede ser considerado diferente según la ley de cada lugar. Expresándonos en términos de Jorge Machicado (2010), podemos afirmar que «el delito fue siempre una valoración de la conducta humana condicionada por el criterio ético de la clase que domina la sociedad».

También sería posible considerar que es la acción u omisión por la cual un individuo transgrede el bien jurídico tutelado por el Estado haciendo caso omiso de los preceptos legales que rigen en el país. Por ende, se debe entender que un delito es un hecho que solamente es precisado por la ley. Su único autor es el hombre que lo comete, pues, si el hombre no existe, el delito tampoco (Cervantes, 2005).

2.6. Delitos contra la libertad

Intimidación y amenaza

El delito de robo con intimidación se comprende cuando se llega a obtener el objeto de valor de la víctima inmediatamente después de que se le intimidó en el robo usando un arma blanca o de fuego. Por su parte, el delito de amenaza ocurre cuando se llega a obtener el objeto de valor de la víctima en un futuro, pero no en el mismo momento en el que ocurre el delito.

Si se considera la definición de cada uno de ellos y, de acuerdo a los tribunales, la diferencia radica en que estaremos ante un delito de robo con intimidación cuando la amenaza se realiza por parte del ladrón con el objetivo de conseguir la entrega inmediata del objeto. Por otro lado, nos encontramos frente a un delito de amenaza condicional con ánimo de lucro si la amenaza se lleva a cabo con el propósito de lograr la entrega de ese objeto en un futuro. Sin embargo, también se puede amenazar con el único fin de lastimar psicológicamente a la víctima (Esteban Abogados, 2015).

Delitos contra el patrimonio

Extorsión

La extorsión es un hecho que consiste en obligar a la víctima a dar el dinero o bienes por medio de la intimidación. El Código Penal del Perú, en el artículo 200, consigna lo siguiente:

> El que mediante violencia o amenaza obliga a una persona o a una institución pública o privada a otorgar al agente o a un tercero una ventaja económica indebida u otra ventaja de cualquier otra índole, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años…. La misma pena se aplicará al que, con la finalidad de contribuir a la comisión del delito de extorsión, suministra información que haya conocido por razón o con ocasión de sus funciones, cargo u oficio o proporciona deliberadamente los medios para la perpetración del delito… El que mediante violencia o amenaza, toma locales, obstaculiza vías de comunicación o impide el libre tránsito de la ciudadanía o perturba el normal funcionamiento de los servicios públicos o la ejecución de obras legalmente autorizadas, con el objeto de obtener de las autoridades cualquier beneficio o ventaja económica indebida u otra ventaja de cualquier otra índole, será sancionado con pena privativa de libertad no menor de cinco ni mayor de diez años (Ministerio de Justicia y Derechos Humanos, 2016).

Tipos de extorsión

a) Extorsión Telefónica (residencial o celular): puede ser un medio de extorsión o de fraude. Con una llamada telefónica, los delincuentes pueden obtener dinero a través de amenazas y engaños.
b) Extorsión presencial: se trata del tipo de extorsión que se hace de forma directa. Es decir, se refiere a la intimidación violenta y directa que se hace a la víctima o las víctimas para obtener dinero, joyas u otros.
c) Extorsión por derecho de piso: es una variable de extorsión, también conocida como «cobro de vacuna», que tiene características mixtas. En otras palabras, puede ser telefónica o presencial. Está relacionada con el cobro de cuotas o «derecho de piso». En esta modalidad, los delincuentes exigen el pago de cuotas a comercios, profesionistas con interrelación pública (médicos, abogados, entre otros) y a empresarios, con el fin de garantizarles protección.

Estafa

La estafa es un delito contra la propiedad o patrimonio que consiste en hacer creer a la víctima la existencia de algo inexistente. Tomemos el típico caso de venta de una casa a 100 000 soles cuando esa casa en realidad no existe. Tal como lo menciona el Código Penal (2016) artículo 196:

> El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.

Delitos informáticos

La rapidez de los cambios en la ciencia, la tecnología y el conocimiento, y la acelerada aplicación de las novedades en la estructura del trabajo y la vida en comunidad, requieren, de los ciudadanos, la disposición para adaptarse a cambios continuos en términos de productividad económica y, sobre todo, de bienestar personal y comunitario. Sin embargo, algunos individuos no se adaptan a las transformaciones y se resisten a la convivencia pacífica utilizando la tecnología de forma distorsionada. Felipe Villavicencio Terreros (2014) expresa:

> El difamar a una persona a través de los medios de comunicación (sea por correo electrónico, Facebook o twitter), no puede constituirse como un delito informático por el solo hecho de emplear la tecnología informática como medio, pues este delito puede realizarse a través de otros medios como son verbal, escrito, etcétera.

Así que, en los casos en los que un delito solamente se realice con dispositivos virtuales como celulares, no puede ser considerado como delito informático, pues existe la posibilidad de que este también se pueda realizar de forma directa.

La informática forense abarca todo lo que se refiere a la preservación, identificación, extracción y documentación de evidencia informática guardada como dato o información codificado magnéticamente. Esta parte de la ciencia indica que la evidencia digital es usualmente creada transparentemente por el sistema operativo de la computadora sin el conocimiento del usuario. La información puede estar escondida a la vista, pues, para encontrarla, se necesitan herramientas de informática forense y técnicas forenses útiles para la identificación de datos ocultos. Valga decir que, después de haber realizado estos análisis, se podrían presentar como pruebas en un proceso legal (Vacca, 2013).

Metodología forense general

La metodología a emplear es un proceso de preservación y documentación de la evidencia, el cual se divide en cuatro pasos importantes (AFDM).

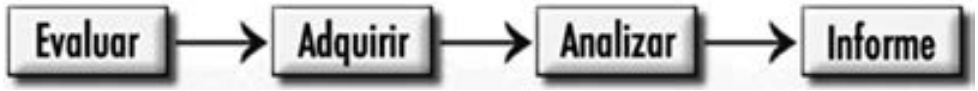

Fig. 6. Fuente: (Informática 64, Pagina web www.informatica64.com, 2014)

Evaluar

Conseguiremos la autorización para registrar un dispositivo móvil, conjuntamente con las políticas legales que lo conllevan. Cuando solicitemos permisos al usuario, identificaremos el equipo a evaluar, realizaremos una evaluación previa y prepararemos la adquisición de pruebas.

Adquirir

Se trata de la construcción de la investigación ayudada por la recopilación de datos, y el almacenamiento y archivamiento de estos, que serán datos inadmisibles para la supuesta víctima y el victimario.

Analizar

Analizaremos los datos adquiridos del equipo, host y de almacenamiento, según sea el tipo de denuncia que se realiza.

Informe

El objetivo es el de recopilar y organizar todos los resultados de los análisis y escribir un informe que detalle los resultados para los involucrados (Vacca, 2013). Los pasos, sin embargo, no son estrictamente secuenciales. La informática forense digital se encuentra dentro de la informática forense. Por lo tanto, si hablamos de pruebas virtuales, estaríamos refiriéndonos a la informática forense digital, la cual se encarga de la identificación, preservación, análisis, interpretación y presentación de evidencias digitales (Navarro, 2015).

Dispositivos móviles

Si pensamos en dispositivos móviles, lo primero que recordamos es un teléfono móvil. No obstante, en la actualidad, son varios los dispositivos móviles disponibles en el mercado: PC portátiles, PocketPC, tabletas, etc. Morillo Pozo (2009) los define de la siguiente manera:

Por dispositivo móvil nos referimos a un dispositivo que puede conectarse a Internet. No obstante, algunas veces también se clasifican cámaras digitales y reproductores MP3 o MP4 estándares como dispositivos móviles.

La diversidad de dispositivos móviles que existen hoy en el mercado propicia una problemática para quien debe programarlos, ya que cada uno de estos dispositivos tiene características particulares que los diferencian (memoria determinada, lenguaje, entorno específico y otros).

Los dispositivos móviles funcionan con Sistemas Operativos Android e IOS. En nuestra investigación, nos centraremos en Android debido a que funciona con software libre y es el más usado en nuestro medio.

Aplicación móvil

Se trata de un pequeño software que utiliza los recursos del equipo para cumplir una función para la que fue elaborada. Si tenemos en cuenta esto, no existe ni un móvil que no tenga un aplicativo. Así lo explican Javier Cuello y Jose Vittone (2013):

En esencia, una aplicación no deja de ser un software. Para entender un poco mejor el concepto, podemos decir que las aplicaciones son para los móviles lo que los programas son para los ordenadores de escritorio.

Una aplicación móvil es una aplicación informática que funciona en dispositivos móviles inteligentes. Según sea su tipo (gratis o de paga), el usuario podrá hacerse de estas (Pimienta, 2015).

Estructura de una aplicación Android

Las aplicaciones Android toman ventaja del lenguaje de programación java, consolidado y de libre acceso, para facilitar a los programadores el desarrollo de aplicaciones para su sistema. Como se sabe, toda la base de Android se inspira en Linux. Menciona Juan Garrido (2013) lo siguiente:

La estructura del sistema operativo Android se compone de aplicaciones que se ejecutan en un framework Java de aplicaciones orientadas a objetos sobre el núcleo de las bibliotecas de Java en una máquina virtual Dalvik con compilación en tiempo de ejecución. Las bibliotecas escritas en lenguaje C incluyen un administrador de interfaz gráfica , un framework OpenCore, una base de datos relacional SQLite, una Interfaz de programación de API gráfica OpenGL ES 2.0 3D, un motor de renderizado WebKit, un motor gráfico SGL, SSL y una biblioteca estándar de C Bionic.

Por ende, las aplicaciones se desarrollan en java con Android Software Development Kit, más conocido como Android SDK, de forma abierta. Cualquiera puede acceder al código fuente para poder solucionar problemas o bugs que aparecen con el tiempo (Ribas, 2016).

Android

Joan Ribas (2016) también señala que Android es una plataforma de desarrollo libre y de código abierto. Tiene una gran cantidad de servicios disponibles, como los GPS, lectores de códigos o una base de datos. Al utilizar Android, se programa en Java, en C o en C++.

Por lo tanto, cabe resaltar que Android es un sistema operativo inicialmente pensado para teléfonos móviles, solo que está basado en Linux. Es libre, gratuito y multiplataforma. Si se considera que Android siempre se está actualizando y tiene diferentes versiones, en este proyecto se desarrollará la solución desde la versión 4.4 de Android, que estará disponible en el *Play Store* de manera gratuita (Nieto, 2011).

3. ANÁLISIS Y DESARROLLO DEL APLICATIVO MÓVIL

Modelo del negocio

Negocio

Los delitos realizados por los medios virtuales, relacionados con amenazas o intimidaciones, extorsiones y estafas, suelen realizarse sin que el afectado sepa si es seguro contestar a ese número o responder el mensaje. Esto obliga al afectado, ya que no saber a quién pertenece ese número, a realizar la denuncia en la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI (PNP). Ello se debe a que no se puede realizar una denuncia por los delitos mencionados si es que no se conoce el número.

El sistema de trámite de denuncia se realiza cuando un ciudadano quiere realizar una después de que ha sido víctima de un delito. De esa manera, el afectado se dirige a la comisaría más cercana para realizar la denuncia. Ya en la comisaria, un oficial lo atiende y recoge todos los datos del denunciante. Podrían adicionarse datos a la denuncia para que tenga mayor validez y sea aceptada. Una vez elaborada y firmada por el ciudadano, deberá esperar a que el oficial la acepte y se inicien las investigaciones.

Si la denuncia no fue aceptada, termina el proceso. Si lo es, se tomarán las medidas necesarias que derivarán en un caso legal. Todas las evidencias necesarias que ayuden a esclarecer quien es el culpable serán útiles. Al finalizar la sentencia, el proceso termina y la denuncia es archivada.

Actores del negocio

Solamente nos enfocaremos en las denuncias sobre una amenaza, extorsión, estafa o intimidación. Se reconocen los siguientes actores:

ACN01	Oficial de Comisaria	Es la persona que registra la denuncia del ciudadano, quien anota los datos necesarios para que esta sea considerada y aceptada.	
ACN02	Ciudadano	Es la persona que realiza la denuncia, y proporciona sus datos y cualquier otra información que ayude a la identificar al sospechoso.	
ACN03	Sospechoso	Es la persona que realiza el delito y quien es la causa de realizar la denuncia.	

Tabla 3. Actores del Negocio. Fuente: elaboración propia.

Casos de Uso del Negocio

CUN01	Realizar comunicación	Sospechoso	
CUN02	Contestar número desconocido	Ciudadano	
CUN03	Solicitar denuncia	Ciudadano	
CUN04	Entregar evidencia	Ciudadano	
CUN05	Registrar la denuncia	Oficial	

Tabla 4. Casos de uso del negocio.

Diagrama de casos de uso del negocio

Proceso de denuncia de un delito

En la tabla 1, se puede apreciar a los actores que tiene el proceso de denuncia de un delito. Primeramente, el sospechoso realiza una comunicación con el ciudadano, el cual no tiene forma de detectar si la llamada es segura. Al momento de contestar o recibir la comunicación del sospechoso, existe la posibilidad de que fuera un delito. En ese momento, el ciudadano se acerca a la comisaría más cercana y brinda información de lo sucedido al oficial. Este registra todo y agrega datos extra si es que los hubiera. Finalmente, se firma la denuncia, que será evaluada para su aceptación. Así culmina el proceso.

DIAGRAMA DE CASOS DE USO DEL NEGOCIO DEL PROCESO DE DENUNCIA

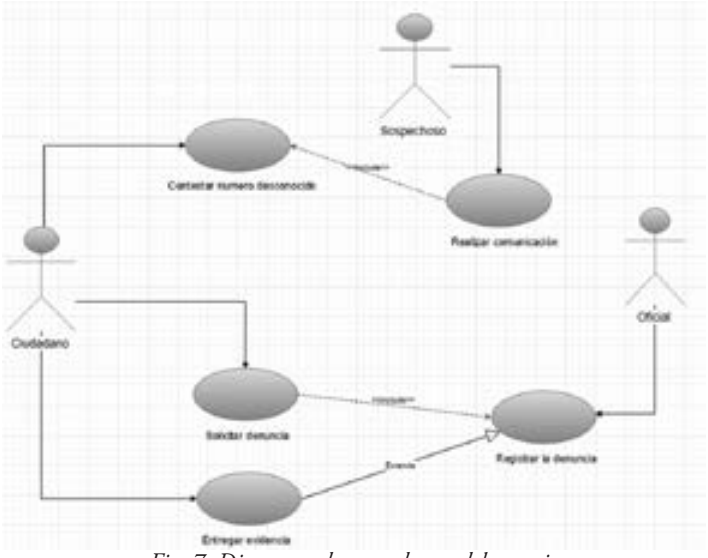

Fig. 7. Diagrama de casos de uso del negocio

Métodos y modelos generales

Teniendo en cuenta las diferentes metodologías que existen para la informática forense, tenemos que considerar cuáles pueden estar dirigidas a los dispositivos móviles, y estudiar qué procesos nos serian útiles en el análisis forense. Como aún el termino de informática forense en dispositivos móviles no es muy utilizado, no existe un estándar para poder aplicarlo. Por ello, mencionaremos los modelos que se usan hoy y analizaremos cuál estaría más cercano a resolver nuestro problema.

Así que el modelo general de la informática forense en aplicativos móviles es como sigue:

1. Fase de identificación y solicitud forense.
2. Fase de preparación.
3. Fase de adquisición de la evidencia
4. Fase de preservación
5. Fase de análisis
6. Fase de presentación
7. Fase de retroalimentación y devolución de la evidencia.

Lo anterior nos permite inferir que siempre se utilizan estas siete fases con las que se analiza un dispositivo móvil. No obstante, recordemos que la metodología a usar es propuesta por Themis, software que lo divide en tres etapas: antes, durante y después del acto delictivo.

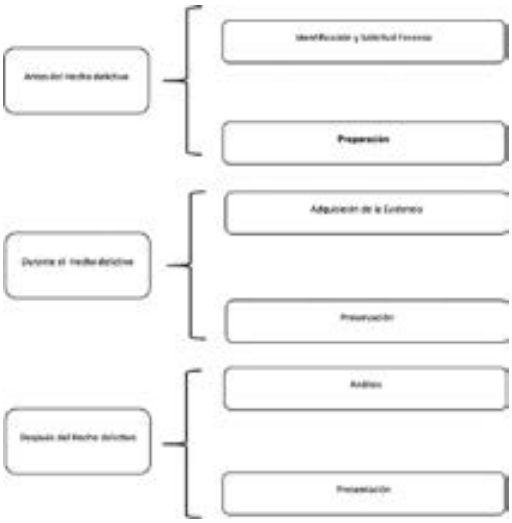

Fig. 8. Metodología a usar en informática forense.

Como se puede apreciar en la figura 5, hemos repartido la metodología general de la informática forense como lo propone el software Themis. Se separa en tres fases generales, las cuales vamos a considerar, para nuestra aplicación, como si tuvieran un alto porcentaje de éxito. Como se puede ver, la devolución del equipo se elimina por tratarse de un aplicativo móvil que recolectará los datos vía web, los cuales serán encriptados para asegurar que no sean modificados por ninguna de las dos partes, tanto la víctima y el victimario, lo que implica datos sin alteraciones.

Modelo de solución

Nuestro aplicativo móvil tendrá por objetivo recorrer las tres etapas mencionadas.

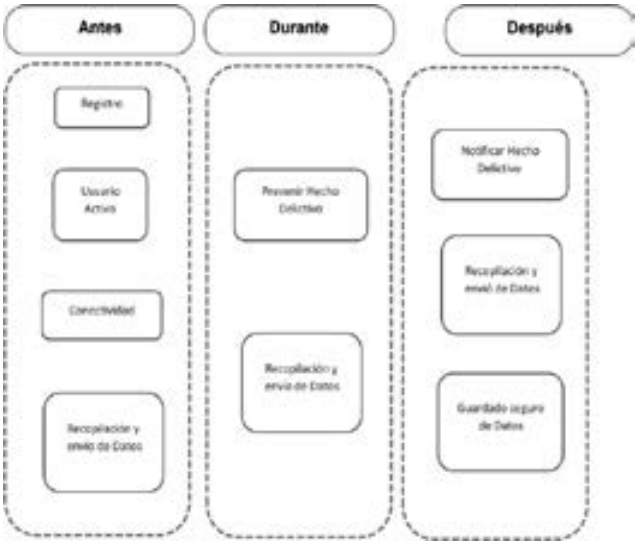

Fig. 9. Modelo de solución planteado.

Detalle del modelo de solución

Fase inicial – Antes del hecho delictivo

Esta fase, en la que procederemos a registrar al usuario en nuestra aplicación, es importante para verificar los datos del usuario. También, tenemos que considerar que los usuarios que se registren no den información falsa ni utilicen la aplicación de una manera irresponsable. Luego, se procederá a recolectar los datos que serán de ayuda para la verificación y el uso correcto de la aplicación. Se registrará un nivel de confianza, que aumentará según la cantidad de datos a ser verificados, para que nos muestre qué tan confiable es el criterio del usuario al momento de usar la aplicación.

Registro

En esta sección, vamos a registrar al usuario. Este ingresará su información básica:

1. Nombres,
2. Apellidos,
3. Edad,
4. DNI,
5. Correo electrónico,
6. Contraseña,
7. Confirmar contraseña,
8. Aceptar los términos y condiciones de la aplicación.

Después de realizar este registro, el usuario podrá ingresar a la aplicación, y al ser su primera vez, se le notificarán todas las características de la aplicación y algunas normas que debe recordar. El nombre del usuario será su DNI y su contraseña será la que ingresó en su registro.

Usuario activo

Tenemos que verificar que esta cuenta esté activa cuando ocurran los percances, como la pérdida o el robo del equipo. Esto asegurará que este último no sea usado por otra persona que no sea el dueño. También, en esta sección de la aplicación, se confirmarán los datos y se le asignará un valor de confiabilidad a los usuarios que procedan a realizar estos mínimos pasos, los cuales apoyarán sus críticas y denuncias para que puedan realizarse por medio del aplicativo móvil sin intención de molestar o perjudicar a alguien y puedan ser considerados de forma seria y responsable. Por medio de este paso, se le pedirá al usuario que ingrese nuevamente la clave, aunque ya esté ingresada. Como un requisito mínimo, se le solicitará, una vez por día, que ingrese la clave, de manera que la aplicación funcione durante todo un día. De esa manera, se espera la siguiente confirmación de contraseña para que pueda ser tomada en cuenta.

Conectividad

La conectividad tendrá que estar presente en el momento del registro del usuario, Primeramente, si el equipo se encuentra siempre conectado a internet, no habrá problemas en el momento de enviar los datos al servidor que contendrá todos los datos de los usuarios, pero en el caso que el usuario no esté conectado a internet, se procederá a guardar los datos de manera encriptada dentro del equipo. Así se asegurará su veracidad y que no sea alterado por ningún otro usuario o aplicación. Una vez que el equipo se conecte a internet, estos datos serán enviados al servidor para ser guardados.

Recopilación y envío de datos

Una vez que la aplicación obtenga los datos del usuario, tomará los datos del equipo móvil junto a sus registros de llamadas y mensajes. De esa forma, podrán ser tomados como datos del estado inicial de la aplicación. Es decir, la aplicación enviará estos datos como estado inicial del equipo al servidor.

También, en el envío, se utilizará un protocolo que asegure la confiabilidad de los datos y que no existan errores de envío junto a normas que regulen los imprevistos. Una vez recibidos los datos del estado inicial del equipo, se guardarán para futuros casos de análisis.

Fase intermedia – durante hecho delictivo

En esta fase, veremos las funcionalidades de la aplicación. Nos centraremos en el caso de que ocurra la problemática planteada: amenazas, estafas, intimidaciones y extorsiones. Se debe tener en cuenta que la aplicación proporcionará opciones en el momento en que ocurran estos hechos, notificando lo que ocurre y ocurrirá en el futuro después del hecho delictivo.

Prevenir hecho delictivo

Veremos que nuestra aplicación está en comunicación con otros usuarios y que, si alguno de nuestros usuarios registró una llamada de un hecho delictivo y lo señaló como tal, automáticamente prevendrá a los demás, de manera que no contesten la llamada o mensaje de ese número. Sí se permitirá contestar o leer los mensajes enviados, pero bajo la responsabilidad del usuario.

Recopilación y envío de datos

Cuando ocurra la prevención de un hecho delictivo, se guardarán la información de la llamada o mensaje del perpetrador y las acciones que realiza el usuario.

Una vez que se cuenta con todas estas características, se procede a enviar los datos al servidor. Se considera este como el segundo estado del usuario dentro del día de confirmación de su cuenta activa.

Fase final – después del hecho delictivo

En esta última fase, se procederá a notificar los hechos delictivos que ocurrieron al equipo, dando seguridad a la información que será enviada e inaccesible para el usuario y quien realizó la llamada o el mensaje. En esta fase, también se procederá a hacer un guardado seguro que dure en el tiempo para que sea posible analizarlo cuando ocurra algún caso legal.

Notificar hecho delictivo

Notificar la ocurrencia del hecho delictivo

Clasificar: amenaza, estafa, intimidación o extorsión.

Recibiremos, en un caso, la llamada de un número que no conozcamos. Luego, al contestar, ocurrirá el hecho delictivo y, una vez finalizada la llamada, la aplicación te preguntará si ocurrió algo con la llamada y permitirá responder «Sí» o «No». En el caso de que se conteste que no, la ventana de pregunta se cerrará. Pero, en el caso de contestar «Sí», la aplicación tomará acciones. En primer lugar, preguntará sobre lo que acaba de ocurrir; si fue una amenaza, un intento de estafa, intimidación o extorsión. Una vez seleccionado el tipo de hecho delictivo, la aplicación procederá a guardar los datos del registro de llamada, y asegurar que el número no vuelva a poder conectarse con el usuario que lo notificó.

En el caso de los mensajes, sucede de forma parecida. Luego de haber leído el mensaje, la aplicación preguntará si ocurrió algo sospechoso en el mensaje con las mismas opciones. Solo si el usuario contesta que «Sí», la aplicación volverá a preguntar qué tipo de hecho ocurrió: amenaza, intento de estafa, intimidación o extorsión. Una vez especificado, la aplicación tomará los datos y se encargará de no volver a recibir los mensajes.

Recopilación y envío de datos

En esta parte, se envían al servidor los datos de la información sobre el delito que acaba de ocurrir. Este se convierte en otro estado en el que el usuario fue la primera víctima en denunciar ese número

por medio de nuestra aplicación. De tal forma, aporta una ayuda a la comunidad que también utiliza la aplicación para la prevención de delitos.

Guardado seguro de datos

En esta sección, se guarda, en el servidor, la información más útil sobre el hecho delictivo que acaba de ocurrir siempre que el equipo esté conectado. En el caso de no estar conectado a internet, la aplicación almacena la información de manera segura para enviarla cuando el equipo tenga internet. Cuando lleguen los datos al servidor, se procede a encriptarlos. Esto proporciona la seguridad de que estos registros no sean alterados y sean precisos acerca de lo que acaba de ocurrir dentro de la aplicación.

Al ocurrir un caso legal en el que esté de por medio nuestra aplicación, el usuario que necesite usar la información, otorgará la que pertenece a su cuenta para que pueda ser verificada. Todo un proceso debe cumplirse antes de que se le otorgue la información que desea. Una vez la tenga, se la procederá a copiar y *desencriptar*. Por último, será analizada sobre el caso que se desee.

4. CONCLUSIONES

Como se ha visto, el progreso de la tecnología en los dispositivos móviles ha otorgado beneficios a los usuarios, pero también les ha dado la oportunidad a criminales de convertir en más insegura la ciudad. Se pudo ver que, en la actualidad, los problemas de seguridad no solamente pueden amenazar a la persona físicamente, sino que puede resultar efectivo llamar o enviar un mensaje de extorsión. La situación se agrava si consideramos que las normas legales respecto a las evidencias informáticas no ayudan al proceso de las denuncias. Por ende, se vuelve necesario cumplir con ciertas normas para que las pruebas sean efectivas. Además, es menester considerar el uso de un sistema que ayude a corroborar que alguien fue víctima de este tipo de crimen para que la población no se sienta indefensa.

5. REFERENCIAS

[1] Aparicio, H. (2014). Extorsiones por teléfono aumentan en fiestas de navidad y año nuevo. *Perú 21*.

[2] Aparicio, H. (2014). MTC denuncia estafas telefónica donde piden dinero en nombre del ministerio. *Perú 21*.

[3] Carrillo, F. (2007). Un bien público cada vez más escaso. *Seguridad ciudadana en América Latina*. 181-198. América Latina: Dialnet.

[4] Carrión, C. (2007). *Educación para una sociedad del conocimiento*. México: Trillas

[5] Cervantes, L. (2005). Marco Conceptual del delito y la pena. *Imposición de la pena de muerte como medida punitiva para los delitos graves con reincidencia, específicamente en el secuestro*. 1-16. Puebla: UDLAP Bibliotecas.

[6] Choo, K.R. (2008) Organised crime groups in cyberspace: a typology. *Trends Organ Crim*e, 11(3). doi:10.1007/s12117-008-9038-9.

[7] Christie, J. (2010). Disconnected: The Safe Prisons Communications Act Fails To Address Prison Communications. *Jurimetrics, 51*(1), 17-59. Recuperado de http://www.jstor.org/stable/41307116

[8] Cuello, J. y Vittone, J. (2013). *Las aplicaciones*. 12-06-16. Recuperado de http://appdesignbook.com/es/contenidos/las-aplicaciones/

[9] El Peruano (2014). *Compendio de Normatividad sobre el uso de Tecnologías de Información en el Perú*. Lima: El Peruano.

[10] Esteban Abogados (2015) *¿Cuál es la diferencia entre robo con intimidación y amenazas condicionales?* Recuperado de http://www.abogado-penalista.es/abogados-robo.php (15/05/16)

[11] Gamboa, E. (2014). Alcalde de Pueblo Libre recibe amenazas de muerte por celular. Lima: *El Popular*.

[12] Garrido, J. (2013). *TFC Desarrollo de aplicaciones móviles* (6). España: Universidad Oberta de Catalunya.

[13] García, L. (2014). *Empresarios de Gamarra denuncian amenazas de extorsionadores*. Lima: El Comercio.

[14] Guerra, A. (2013). El delincuente. Nociones básicas. *Estudio sobre la delincuencia en la criminología peruana contemporánea*, *5*. Lima: Facultad de Derecho de la Universidad San Martín de Porres.

[15] Horsman, G., & Conniss, L. R. (2015). An investigation of anonymous and spoof SMS resources used for the purposes of cyberstalking. *Digital Investigation*, *13*, 80-93.
[16] Hurtado, J. (1996). Introduccion. *Derechos humanos y lucha contra la delincuencia.* Suiza: THEMIS 35. 553-567.
[17] INEI (2014). *Boletin de seguridad*. INEI: 1 y 2.
[18] Info Región (2007). *Perú: Conceptos básicos sobre seguridad*. 01-2010, de Juan Briceño Recuperado de www.inforegion.pe/46095/peru-conceptos-basicos-sobre-seguridad/ (22/05/16)
[19] Johansen, O. (2008). *Introducción a la teoría general de sistemas.* Colombia: Limusa - Noriega Editores.
[20] Kanashiro, G. (2014*) ¿Por qué es tan difícil luchar contra extorsionadores?* Lima: El Comercio.
[21] Machicado, J. (2010). Concepciones del delito. *Concepto de delito*. Bolivia: Apuntes Jurídicos.
[22] Ministerio de Justicia y Derechos Humanos. (2016). *Codigo Penal*. Perú: Ministerio de Justicia.
[23] Morillo, J. (2009). Introducción a los dispositivos móviles. En *Tecnología y desarrollo en dispositivos móviles* (37). Av. Tibidabo, 39-43: Universidad de Oberta de Catalunya.
[24] Mylo, A., Meletiadi, V., Mitrou, L. y Gritza, D. (2013). *Smartphone sensor data as digital evidence*. ELSEVIER, 1, 5-15. 11-2015, De ScienceDirect Base de datos.
[25] Navarro, J. (2015). *Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico*. España: Universidad Politecnica de Valencia.
[26] Nieto, A. (2011) ¿Qué es Android? *xatakandroid*. Recuperado de http://www.xatakandroid.com/sistema-operativo/que-es-android (12-06-16)
[27] Nobile, M. (2003). *México y la agenda contemporánea de seguridad internacional: un estudio sobre los alcances del uso del concepto de seguridad humana*. Puebla: Universidad de las Américas.
[28] Olvera, A. (2008). *Ciudadanía y Democracia.* México: Instituto Federal Electoral.
[29] Pimienta, P. (2015). Tipos de aplicaciones móviles y sus características. *Deideaaapp*. Recuperado de https://deideaaapp.org/tipos-de-aplicaciones-moviles-y-sus-caracteristicas/ (12-06-16)
[30] Rivas, J. (2009). Introducción al análisis forense. En *Análisis Forense en Sistemas Informáticos* (13). Av. Tibidabo, 39-43, 08035 Barcelona: Universidad Oberta de Catalunya.
[31] Rivas, J. (2016). Introducción a Android. En *Desarrollo de aplicaciones para Android*. (16-19). España: Anaya Multimedia.
[32] Vacca, J. (2013). Computer Forensic-Computer Crime Scene Investigation. En *Computer Forensic Fundamentals* (40). Boston Massachusetts: Charles River Media.
[33] Vazquez, J. (2007). La delincuencia. En *Delincuencia desde el enfoque estructural* (22-25). Cuencia Ecuador: Universidad del Azuay.
[34] Villavicencio, F. (2014). *Delitos informáticos*. Revistas PUCP, 1, 1-5. 10-2015, De Revistas PUCP Base de datos.
[35] Von-Bertalanffy (1968). *Teoría general de los sistemas*. Nueva York: Fondo de Cultura Economica.
[36] Zárate, P., Aragón, J. y Morel, J. (2013). La problematización de la inseguridad en el Perú. En *Inseguridad, Estado y desigualdad en el Perú y en América Latina: Un estado de la cuestión* (8-15). Lima: Instituto de Estudios Peruanos.