INSTITUTO TECNOLÓGICO SUPERIOR "POLICÍA NACIONAL"

CARRERA: INVESTIGACIONES DE POLICÍA JUDICIAL

Incidencia de la informática como herramienta para la prevención del delito en el Distrito Metropolitano de Quito en el año 2012

TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE: TECNÓLOGO EN INVESTIGACIONES DE POLICÍA JUDICIAL

NOMBRE DEL AUTOR: WILLIAN ROBERTO MEJÍA GAVILANES
NOMBRE DEL DIRECTOR: DR. GONZALO BÁEZ ITURRALDE

QUITO
2014

CERTIFICACIÓN

Trabajo de Graduación presentado previo a la obtención del título de Tecnólogo en Investigaciones de Policía Judicial

En mi calidad de Director del trabajo de titulación, desarrollado por el señor **WILLIAN ROBERTO MEJÍA GAVILANES**, estudiante de la Carrera de Investigaciones de Policía Judicial, para optar por el título de **TECNÓLOGO EN INVESTIGACIONES DE POLICÍA JUDICIAL**, cuyo título es

"INCIDENCIA DE LA INFORMÁTICA COMO HERRAMIENTA PARA LA PREVENCIÓN DEL DELITO EN EL DISTRITO METROPOLITANO DE QUITO EN EL AÑO 2012",

Considero que el trabajo presentado reúne los requisitos y méritos suficientes para ser sometido a la evaluación del jurado examinador que se designe.

En la ciudad del D.M. de Quito a 27 de Marzo del 2014

REPÚBLICA DEL ECUADOR
POLICÍA NACIONAL

INSTITUTO TECNOLÓGICO SUPERIOR "POLICÍA NACIONAL"

REGISTRO INSTITUCIONAL NO. 17-039P

"INCIDENCIA DE LA INFORMÁTICA COMO HERRAMIENTA PARA LA PREVENCIÓN DEL DELITO EN EL DISTRITO METROPOLITANO DE QUITO EN EL AÑO 2012"

POR: WILLIAN ROBERTO MEJÍA

El presente Trabajo de Graduación **TECNÓLOGO EN INVESTIGACIONES DE POLICÍA JUDICIAL** luego de cumplir con todos los requisitos normativos, se aprueba, en nombre del Instituto Tecnológico Superior "Policía Nacional", en la ciudad del D.M. de Quito, a los 27 días del mes de Marzo del 2014

NOMBRE
……..
FIRMA
C.I……

NOMBRE
……
FIRMA
C.I……

NOMBRE

FIRMA
C.I……..…..

DEDICATORIA

Dedico este trabajo primeramente a DIOS, Ser Supremo, que ha permitido mi existencia; A MIS PADRES, quiénes supieron estar pendiente de mí en todo momento, mis maestros quienes me acompañaron en este proceso educativo e impulsaron a que siga adelante y cumpa con todas las metas que me he propuesto.

Roberto Mejía

DECLARACIÓN EXPRESA

La responsabilidad del contenido del presente trabajo de investigación de Graduación presentado previo a la obtención del título de TECNÓLOGO EN INVESTIGACIONES DE POLICÍA JUDICIAL me corresponde, y mediante la presente en forma voluntaria, capaz ante la ley realizo una sesión exclusiva de todos los derechos al INSTITUTO TECNOLÓGICO SUPERIOR DE LA POLICÍA NACIONAL, para que el presente trabajo forme parte del patrimonio intelectual del ITSPN y lo utilice conforme crea conveniente.

WILLIAN ROBERTO MEJÍA GAVILANES

C.C. 1716204613

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ABSTRACT

Los delitos informáticos afecta la economía de muchos pobladores de la ciudad de Quito, por lo que la concurrencia de éste se ha convertido en una problemática social. De manera que, analizar la incidencia del delito informático, permitirá legitimar la problemática social en el Distrito Metropolitano de Quito en el año 2012. Las variables de la hipótesis utilizada son Informática y Prevención del delito ya que, estas son las palabras claves para poder definir la investigación. La población que proveerá de información será los habitantes y usuarios de las diferentes instituciones bancarias ubicadas en la Av. Amazonas, entre la Avenida Patria y Colón. Otro de los factores a investigar será los diferentes tipos de delitos informáticos, ya que la combinación de ellos puede acarrear muchos problemas a la comunidad quiteña.

Descriptores: Delito informático, economía, problemática social, Avenida Amazonas

ABSTRACT

Computer-related crime affects the economy of many inhabitants of the city of Quito; therefore the concurrence of this has become a social problem. So, analyze the incidence of cybercrime, will allow legitimate social problems in the Metropolitan District of Quito in the year 2012. The hypothesis used variables are computer science and crime prevention since these are the key words to define the research. The population provided information will be residents and users of the different banking institutions located in the Av. Amazonas, between Av. Patria and Colon. Another factor to investigate will be different types of computer-related crime, since the combination of them can cause many problems to the Quito community.

Descriptors: Computer Crime, economy, social issues, Avenida Amazonas

INTRODUCCIÓN

La presente investigación está enfocada en dar una posible solución al delito informática. De manera que, la propuesta no busca solucionar un problema sino evitar que ésta se reproduzca y afecte a más habitantes del sector. La persistencia de este problema incide en el prestigio de muchas instituciones bancarias privadas y estatales, por lo que sus clientes optarán por utilizar servicios bancarios alternativos

Los resultados del proyecto de investigación están divididos de la siguiente manera:

- Capítulo I, Marco teórico contiene: Antecedentes Investigativos, la Fundamentación Teórica Marco conceptual, Marco Legal e Hipótesis
- Capítulo II, Metodología de la Investigación está estructurado de la siguiente forma: Tipos de investigación, Técnicas y herramientas de la investigación, recolección de datos. Procesamiento de la Información
- Capítulo III, La propuesta, la cual está elaborada de acuerdo a los resultados obtenidos en la investigación
- Capítulo IV, Conclusiones y recomendaciones.

MARCO CONTEXTUAL

Antecedentes

Entender los delitos informáticos desde una problemática social es enfocarse a la influencia que tienen las Tecnologías de la Información y la Comunicación (TICS) sobre los intercambios de códigos y la interrelación que tienen los actores sociales sobre el problema. Por ello, es necesario analizar el contexto informático que ha tenido el internet sobre los diferentes procesos socio-culturales.

Como ejemplo del impacto que tiene el internet sobre las relaciones humanas, en el año 2005, en el gobierno de Lucio Gutiérrez un grupo de ciudadanos se organizaron para llamarse la *Rebelión de los Forajidos,* fue un movimiento espontáneo que se constituyó para derrocar al presidente del Ecuador.

El uso de los aparatos tecnológicos como los celulares o móviles permitieron difundir las ideas de derrocamiento. Además estos medios de difusión fueron de gran utilidad, ya que por el desinterés mediático de los canales convencionales, los mensajes de textos y correos electrónicos tenían el compromiso de ajustar y precisar la convocatoria, consignas, lemas y sitios de encuentro.

La *Rebelión de los Forajidos* es el primer hito tecnológico que fue promovido en el país, el cual estaba enfocado a prescindir de una organización institucional de los partidos tradicionales, donde los jóvenes fueron los actores principales para la difusión y formación de los grupos sociales con sentido autónomo.

De la misma manera, el internet se ha convertido en una herramienta potencial para la política permitiendo construir a pesar de toda restricción o brecha económica, un espacio público alternativo del presente y del futuro.

Por consiguiente, el uso de las TIC se convirtió en herramienta de lucha resistencia y articulación, con el fin de crear fisuras en la captación, seguimiento y vigilancia estatal o corporativa, además de alcanzar una visibilización ciudadana real de los temas que influyen en la vida diaria de millones de personas.

Es importante resaltar a nivel de política *online,* se tiene el caso de Julián Assange, director de *Wikileaks,* la cual es una organización mediática internacional sin ánimo de lucro que postea a través de sus sitio Web documentos anónimos e informes filtrados con contenido sensible en materia de interés público.

Otro hito informático, tenemos el cierre repentino de *Megaupload,* este sitio Web es una de las páginas más grandes de intercambio de archivos en el mundo donde, el FBI intervino de forma justificada afirmando que los archivos compartidos en el sitio digital atentaban a las violaciones de derechos de autor y lavado de dinero. Estos acontecimientos nos permiten evidenciar y demostrar el crecimiento de una gestión especializada de los estados en la comunicación política y de censura en Internet.

Planteamiento Del Problema

La inseguridad es un problema social que ha afectado a todos los individuos de una manera directa o indirecta. Por ello, las políticas de seguridad se han convertido en vitales para el desarrollo del país, es así como en la Nueva Constitución del Ecuador incorpora la seguridad ciudadana en el artículo 39, donde afirma que: “El Estado garantizará la seguridad ciudadana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir formas de violencia y discriminación, y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a los órganos especializados en los diferentes niveles de gobierno”.

Esto, sin duda, demuestra la importancia de mejorar la seguridad del país en base a diferentes proyectos que involucran el respeto a los derechos humanos y su compromiso con la construcción de la justicia social. Sin embargo, estas políticas no han logrado disminuir la violencia generada por la inseguridad. Por lo que, es necesario que la seguridad social sea entendido como un tema complejo y amplio, que debe ser visualizado desde diferentes posturas.

Para Fernando Carrión “la violencia tiene dimensiones claramente diferentes e interrelacionadas. La inseguridad que es la dimensión que hace referencia a los hechos concretos de violencia objetiva producidos o lo que es lo mismo la falta de seguridad”. (2007, pág. 10) Es así que, la inseguridad no sólo se encuentra en las calles de la ciudad de Quito, sino que gracias a los avances tecnológicos, el crimen se ha organizado de mejor manera y ha planificado nuevas maneras de realizar sus actos delictivos.

El uso de nuevas tecnologías a nivel mundial y especial en el Ecuador sigue incrementándose al mismo ritmo que los delitos cometidos mediante el uso inadecuado de los mismos, para ejemplificar la superintendencia de bancos a registrados los fraudes más frecuentes

1. Fraudes relacionados con las claves de banca electrónica de los usuarios. Con estas claves, los delincuentes realizan transferencias de cuentas de clientes hacia otras personas y luego realizan retiros en efectivo.
2. Ofertas en página web de productos o servicios que no existen
3. Suplantación de identidad, es decir que los delincuentes abren cuentas o realizan transacciones a nombre de las personas a las que les han robado su cédula o pasaporte. (SIB, 2012)

En el país los fraudes o delitos informáticos están en pleno auge, ya que en el año 2010 cientos de personas han sido perjudicadas, por este acto y en su mayoría son gente de la capital y de la ciudad de Guayaquil

De manera que, hablar de delitos informáticos no es nuevo en la ciudad Quito, el problema radica en la reincidencia que existe y cómo, estos actos se repiten a diario en las diferentes instituciones bancarias, por lo que cada institución ha optado por tomar las respectivas medidas de seguridad.

Formulación de Problema

¿Cuál es la incidencia de la informática, como herramienta, para la prevención del delito en el Distrito Metropolitano de Quito en el año 2012?

Objetivo General

Analizar la incidencia del delito informático como herramienta para la prevención del delito en el Distrito Metropolitano de Quito en el año 2012.

Objetivos Específicos

- Determinar los factores que afectan a la seguridad informática en el Distrito Metropolitano de Quito

- Definir los delitos informáticos que afectan a la población del Distrito Metropolitano de Quito para organizar procesos y propuestas de seguridad.

- Plantear una propuesta de solución para disminuir el impacto que provocan los fraudes informáticos.

Justificación

La razón de investigar sobre los delitos informáticos surge de la inexistencia de información que guíe a los usuarios a cuidar sus claves personales, ya que en investigaciones previas se ha detectado que la falta de conocimiento en el manejo de las redes sociales y las aplicaciones de los servicios bancarios.

Los beneficiarios de este proyecto de investigación son varios, entre ellos se encuentran los usuarios, los empleados de los diferentes bancos de la ciudad de Quito y los jóvenes, ya que ellos al estar a la par de la tecnología han dado un uso diferente a las TIC, es decir cómo se analizó en los antecedentes, la población juvenil ha logrado autorganizarse e integrarse en los diferentes procesos sociales.

Por lo que, las redes de la información han facilitado la participación activa de los ciudadanos en varios procesos políticos, por esta razón el sistema bancario, gobierno de turno y las instituciones privadas han creado espacios donde se logre

interrelacionar las opiniones de cada usuario para ejecutar proyectos que vinculen a la sociedad con las instituciones.

La originalidad del tema radica en la importancia que tiene el internet sobre las relaciones sociales y cómo ella ha creado su propio lenguaje, signos y representaciones, para que cada usuario se identifique con el medio.

Partiendo de esta premisa los delitos se han alejado de las calles de la ciudad y han ingresado al mundo virtual de las TIC, donde el desconocimiento de muchas personas ha facilitado que los delincuentes ejecuten sus delitos de manera tranquila y sin sanción.

Por esta razón, se pretende hacer una guía que brinde información a los usuarios y empleados de los bancos ya que, si no existe una cultura tecnológica los delitos aumentaran y el sistema bancario decaerá.

CAPITULO I

1. MARCO TEÓRICO

1.1. Antecedentes Investigativos

Relacionar con otras fuentes de estudio permitirá comprender la profundidad investigativa que ha tenido el problema, en otras instituciones universitarias. De manera que, para ello se visitará el sitio web “Bibliotecas del Ecuador”, el cual, tiene información bibliográfica sobre las tesis o proyectos de investigación realizadas en el país.

Según Juan Armendáriz graduado de la Universidad Técnica del Norte, se detectaron las siguientes conclusiones:

1. Es una realidad la presencia de nuevas formas delictivas debidas concretamente a que antes no existía un adelanto informático y electrónico de grandes magnitudes como ahora. Por esa circunstancia, se considera que resulta todavía insuficiente la legislación vigente tanto a nivel nacional como a nivel internacional.

2. Debido a la naturaleza de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

3. La falta de cultura informática en nuestra provincia es un factor crítico en el impacto de los delitos informáticos, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones

4. En la mayoría de los casos no se denuncian estos delitos, para evitar la alarma social o el desprestigio por un fallo en la seguridad. Las víctimas prefieren sufrir las consecuencias del delito e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial. Esta situación dificulta enormemente el conocimiento preciso del número de delitos cometidos y la planificación de las adecuadas medidas legales sancionadoras o preventivas. (2011, pág. 125)

Elsa Pico, en su proyecto de investigación sobre "Análisis de los fraudes informáticos y su incidencia en el acceso a la información", se obtuvo las siguientes conclusiones:

1. Una guía preventiva de seguridad ofrecerá información útil y de fácil comprensión para todos los usuarios de los sistemas informáticos de la institución financiera, logrando con ello que éstos tengan las pautas necesarias para combatir los fraudes tecnológicos.

2. La mayor debilidad encontrada en los sistemas informáticos dentro de Cooperativa de Ahorro y Crédito San Francisco Ltda., es el desconocimiento existente en el recurso humano de la institución.

3. En la actualidad existe una gran cantidad de fraudes informáticos, por lo cual se hace difícil el seleccionar los más comunes, puesto que día a día aparecen nuevas amenazas para nuestros los sistemas informáticos.

4. La principal finalidad de la guía preventiva de seguridad es crear una conciencia de prevención en el personal de la institución, como en sus respectivos clientes. (2012, pág. 124)

Revisando el Repositorio digital Manuela Sáenz del Instituto Tecnológico Superior Policía Nacional se encontraron varias tesis que tiene una base investigativa similar al tema de inseguridad informática.

De manera que para la tesis realizada por Jorge Aníbal Yánez Suarez y Kléver Antonio Mendoza Jácome.

1. Los sistemas electrónicos encontrados en funcionamiento en varias agencias y empresas financieras demuestran que utilizan sistemas de Seguridad Electrónicos poco funcionales o caducos; por lo que es necesario que las autoridades pertinentes obliguen a actualizar dichos sistemas que deben estar acuerdo a los requerimientos y exigencias de niveles de seguridad internacionales.

2. La experiencia acumulada por expertos en el manejo de sistemas de Seguridad Electrónica en el ámbito financiero permite a nuestro estudio afirmar que no se obtendrán resultados exitosos, si los bancos, entidades financieras, organismos judiciales y de otra índole no asumen a cabalidad la responsabilidad social que les corresponde en la lucha que actualmente libra el mundo contra las organizaciones criminales; lo anterior se complementa con la adopción de medidas universales que superen las barreras fronterizas existentes entre los diversos países contrarrestando de formas globalizada el accionar de los la delincuencia organizada transnacional. (2005, pág. 123)

Mientras tanto, en otra tesis se pone énfasis en la implementación de seguridad, la cual fue realizada por los oficiales Edison Barrionuevo Jairo Ñacata, ellos concluyeron que

1. Los empleados que laboran en Instituto Tecnológico Superior de la Policía Nacional no han recibido capacitación para un buen manejo de la información.
2. Un alto porcentaje del personal que labora en el área administrativa del Instituto Tecnológico Superior de la Policía Nacional tienen acceso a los computadores de las distintas oficinas.
3. Existe en el Instituto Tecnológico Superior de la Policía Nacional un alto porcentaje de perdida de información a causa de apagones y virus informáticos.

4. Existe carencia en el Instituto Tecnológico Superior de la Policía Nacional de UPS (baterías de carga eléctrica) para los equipos informáticos y las instalaciones eléctricas no son óptimas para el funcionamiento. (2006, pág. 156)

Una vez analizado las fuentes investigativas realizadas por los mismos estudiantes se dará inicio a éste estudio, el cual intenta a través de enfoques sociales explicar el problema y sustentarlo teóricamente.

1.2. Fundamentación Teórica

Enfoque sociológico

Las diferencias sociales, económicas y culturales han producido una desigualdad entre los individuos de determinada sociedad, este aspecto en algunas ocasiones se ha convertido en exclusión, y son estos excluidos los que quieren vengar su situación por ser alojados de su entorno mediante actitudes delictivas, produciendo de esta manera conflictos sociales que en muchos casos han terminado en conductas desviadas, más no en actos criminales.

> El delincuente se distingue del infractor por el hecho de que es menos su acto que su vida lo pertinente para caracterizarlo… La detención provoca la reincidencia. Después de haber salido de prisión, se tienen más posibilidades de volver a ella; los condenados son, en una proporción considerable, antiguos delitos… La prisión fabrica indirectamente delincuentes al hacer caer en la miseria a la familia del detenido… Admitamos que la ley está destinada a definir infracciones, que el aparato penal tenga como función reducirlas y que la prisión sea el instrumento de esta represión. Entonces hay que levantar un acta de fracaso. (1976, pág. 12)

Según la explicación que emite Foucault, se señala que los delincuentes se dan a causa de las desigualdades que se producen dentro de una sociedad, las causas pueden variar sin embargo los efectos que produzcan serán los mismos.

Para tratar a estos individuos se han creado organismos que se encarguen de castigar su falta mediante distintos mecanismos y normas que sancionen sus desviaciones, y a partir de esto hacer respetar el orden ya establecido.

Para combatir algunos de estos casos se ha creado cuerpos policiales que controlen el orden ciudadano mediante la aplicación de castigos, de tal modo que se genere miedo hacia el resto de la población. La cárcel es la institución que

condena y vigila a los infractores y a la vez fabrica indirectamente delincuentes, debido al entorno que encierra insatisfacción.

Enfoque psicológico

Debido a los cambios producidos en las sociedades y a los aspectos culturales se ha optado por determinar un enfoque que explique las necesidades que tiene el ser humano.

> El nuevo modelo de sociedad ha hecho emerger nuevas manifestaciones de la violencia social, que imbrican en aquellas formas de violencia que están más directamente relacionadas con las condiciones estructurales del sistema social- la situación de pobreza extrema, la cesantía, la falta de viviendas, etc. Con otras formas de violencia que deterioran gravemente las condiciones de vida de la población general, como de la violencia delictual. (1996, pág. 87)

Partiendo de este enfoque se puede entender que el ser humano necesita seguridad, la cual condiciona la percepción de los deseos, es decir, cuanto mayor es la satisfacción de un deseo, menor es la necesidad de satisfacerlo.

Kotler, P.; Armstrong, G., en su texto Fundamentos del Marketing afirma

> Para Maslow las necesidades humanas forman jerarquías, desde la más urgente, que se encuentran en la parte inferior, hasta las menos urgentes, que están en la parte de arriba. Dichas necesidades incluyen las fisiológicas, de seguridad, sociales, de estima y de actualización propia. (2005, pág. 24)

La necesidad humana de tener seguridad es innata, pertenece a su naturaleza y composición psicosocial, es decir el sujeto exigirá seguridad a quien esté regularizando esta actividad, ya que ésta por ser una institución pública debe

velar por los intereses de su grupo social, provocando así legitimidad por parte de la ciudadanía ante la institución.

Enfoque socio-tecnológico

El enfoque socio-tecnológico intenta explicar la relación que existe entre la tecnología y las diferentes prácticas sociales y culturales del sujeto, ya que en los últimos años la tecnología ha intentado reemplazar algunas actividades practicadas por el ser humano.

> La mayor parte de los usos a los que se ha puesto a trabajar a la máquina son exactamente los mismos que existían antes de su invención. La única diferencia es que la máquina realiza idénticas tareas mejor, más rápido y a un Costo significativamente menor. (2004, pág. 89)

Por lo que, la tecnología se ha convertido en un recurso social que determina no sólo estatus social sino poder, ya que a través del dominio de ellas permite que varios grupos sociales establezcan las normas, reglas que legalicen y regularicen el uso de nuevas tecnologías, para facilitar la vida o brindar seguridad.

> La tecnología es legislación en estado práctico, y los modelos sociales alternativos necesitan de la implantación de tecnologías inconmensurables. Es por ello que hay que retomar el control de la tecnología. Una vez implantada, la tecnología ocupa el espacio físico y social, usufructuándolos recursos disponibles finitos (2002, pág. 98)

Se le considera como estado práctico al uso que tiene el gobierno de turno sobre el manejo de las tecnologías, ya que ellos a más de proveer artefactos que faciliten la vida, tienen la potestad de instaurar lo que se debe utilizar y lo que no se debe utilizar.

Es por ello, que la sociedad ha optado por modelos sociales donde se relacione cultura, identidad y tecnología, esto quiere decir que el uso de equipos técnicos facilitará a que un grupo social que se vincule al llamado progreso, ya que a mayor tecnología mayor desarrollo y si existe mayor desarrollo existirá mayor aceptación por parte de los Estados de poder.

> La historia del impacto social de la tecnología muestra la conexión existente entre un tipo determinado de tecnología y una forma específica de sociedad. Ni toda tecnología sirve a cualquier sociedad, ni toda sociedad puede absorber cualquier tipo de tecnología. (2003, pág. 87)

1.3. Marco conceptual

- **Seguridad**

Carlos Chiriboga “es la condición esencial para la vida y el desenvolvimiento de las naciones y de los individuos que la integran”. (2005, pág. 23). Representa la garantía de la aplicación objetiva de la Ley, de tal modo que los individuos saben en cada momento cuáles son sus derechos y sus obligaciones sin que el capricho, la torpeza o la mala voluntad de los gobernantes puedan causarles perjuicio.

Por consiguiente la seguridad debe ser definida desde estos dos ámbitos (lo jurídico y lo social), donde los seres humanos procuren gozar la protección legal del Estado. Según Luis Alcalá-Zamora y Cabanellas “la seguridad social se encuentra en la zona fronteriza de lo jurídico y lo sociológico”. (2005, pág. 17) Estas dos visiones demuestran que, en la actualidad, la seguridad es concebida como una obligación del Estado con los ciudadanos, pues es el encargado de velar y proteger.

- **Informática**

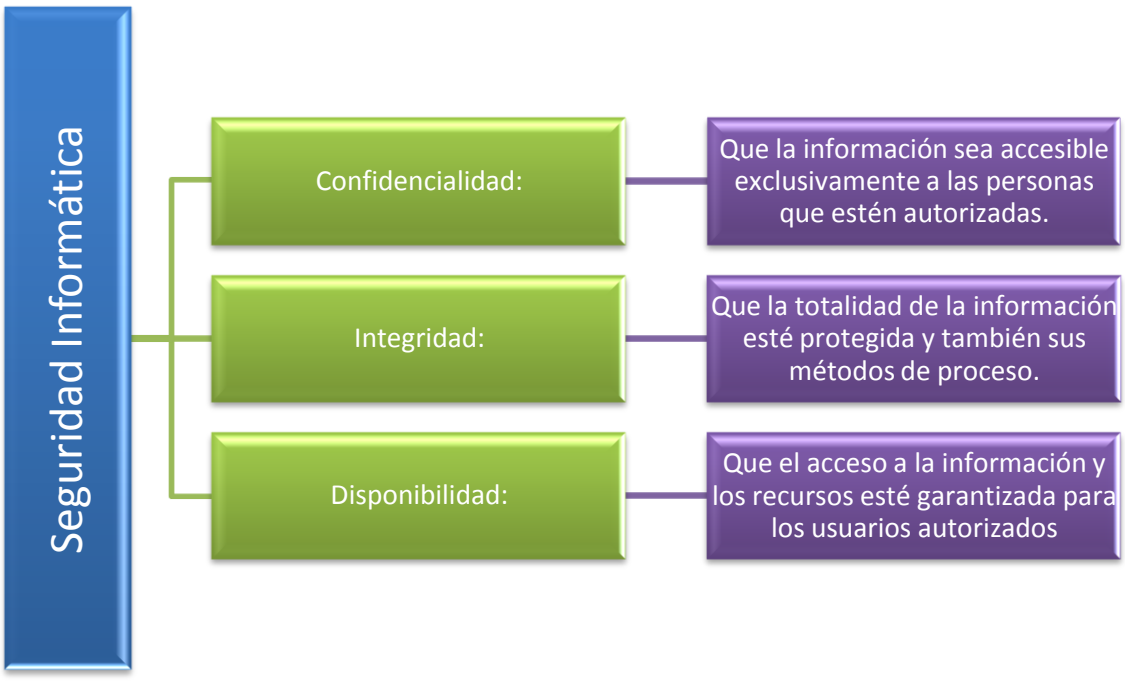
Así CALDERÓN, Luis define que

> "La informática es el tratamiento de la información utilizando sistemas electrónicos y computacionales. Consta de tres tareas básicas: entada de datos, procesamiento de la información y salida y transmisión de resultados. La informática es un amplio campo que incluye los fundamentos teóricos, el diseño, la programación y el uso de las computadoras". (2011, pág. 15)

- **Seguridad informática**

Está definida como "la característica de cualquier sistema informático, que hace que esté libre de todo peligro, daño o riesgo. Como no hay sistema infalible, se trata de que el sistema sea lo más fiable posible". (Seguridad Informática, 2010)

Gráfico Nº 1 Seguridad Informática



Fuente:(Seguridad Informática, 2010)
Elaborado por: Roberto Mejía

En contraste recomienda que “La seguridad comienza desde nuestro PC, la seguridad a nivel locales lo primero que debemos es cuidar. Un 90% de los ataques vienen por las contraseñas. Es conveniente cambiarlas cada15días o por lo menos una vez al mes, ya que por descuido del usuario se puede realizar daños irreparables al sistema informático”. (Informática, 2008)

- **Delito Informático**

Para UILCAPI, Arturo afirma que “El delito informático, o crimen electrónico, es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet”. (Derecho Ecuador, 2011)

Para Lima, L., el delito informático está definido como “cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y que en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin”. (2001, pág. 100)

De igual forma en el tercer Convenio de Cyber-delincuencia del Consejo de Europa, especifica que los delitos informáticos son “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos”. (Convenio de Cyberdelincuencia del Consejo de Europa Estados miembros de Consejo de Europa y otros, 2001)

Tipos de delitos Informáticos

Los tipos de delitos informáticos busca proteger y salvaguardar los diferente bienes jurídicos, los cuales son de alto interés para los grupos sociales, ellos definen como bienes jurídicos todo lo que tiene valor alguno para el sujeto o son dignos de ser protegidos por la protección penal, para ilustrar esto se puede observar la tipificación de delitos Informáticos

Tabla Nº 1Tipificación de Delitos Informáticos

Reconocidos por la Naciones Unidas	Abogados Especializados en Delitos Informáticos
Fraudes mediante la manipulación de computadoras (programas, datos de entrada y salida, repetición automática de procesos.	Fraudes mediante la manipulación de computadoras: 1. Delito contra elementos físicos – hardware. 2. Delitos contra elementos lógicos (daños, acceso ilícitos a sistemas, acceso ilícito a datos protección de programas)
Falsificaciones informáticas (alteraciones de documentos falsificaciones de documentos)	
Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)	Delitos cometidos a través de sistemas informáticos: 1. Estafas 2. Apoderamiento de dinero por tarjetas de cajero 3. Uso de correo electrónico con finalidad criminal 4. Utilización de internet como medio criminal
Acceso no autorizado a servicios y sistemas informáticos (piratas, reproducción no autorizada)	

Fuente: http://informatica-jurídica.com
Elaborado por: Roberto Mejía

Partiendo de este cuadro los tipos delitos también se los puede clasificar en:

- ***Fraudes:*** es todo aquel delito que por medio de la manipulación de los datos y programas informáticos se puede obtener lucro ilícito
- ***Sabotaje Informático:*** Es todo daño ocasionado por la destrucción y modificación de datos, información en documentos electrónicos o redes informáticas.
- ***Pornografía Infantil:*** es la inducción, producción venta y distribución de contenido infantil con fines pornográficos o explotación sexual.
- ***Espionaje Informático:*** es la circulación no autorizada de datos reservados

- **Delincuencia Informática**

Infracciones de Propiedad Intelectual: Son copias y reproducciones que no tienen la plena autorización por parte del creador de esa información que tienen protección legal.

Gómez Perals afirma que:

> "como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos". (1994, pág. 24)

De igual forma Ruiz Vadillo conceptualiza a la delincuencia informática como "todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos". (1996, pág. 20)

Ley SOPA

Para el Ministerio del Poder Popular para la Educación Superior de Venezuela la Ley S.O.P.A está definida como

> La Ley S.O.P.A (Stop Online Piracy Act), por sus siglas en inglés, está principalmente enfocada en eliminar la piratería, el copyright y las violaciones de los derechos de autor en la web; es cierto, que se debe tener presente la importancia de regular este problema con la piratería, pero las medidas tomadas para ello, según ésta, provocarían más consecuencias negativas a la internet y al usuario, el cuál es el problema inicial sobre el cual fue planteada la ley. (Ministerio del Poder Popular para la Educación Superior, 2010)

Ley PIPA

El proyecto de ley PIPA fue presentado el 12 de mayo de 2011, por el senador Patrick Leahy (D-VT) y bipartidista copatrocinadores 11, donde afirmaban que

> La Ley de protección de la PI (Prevención de amenazas en línea real de creatividad económica y el robo de la Ley de Propiedad Intelectual, o PIPA) es un proyecto de ley con el objetivo declarado de dar a los titulares del gobierno de EE.UU. y los derechos de autor herramientas adicionales para restringir el acceso a "sitios web dedicados a infringir robos o falsificaciones ", especialmente los registrados fuera de los EE.UU. (Ley P.I.P.A, 2011)

1.4. Marco legal

Constitución de la República del Ecuador
Sección tercera
Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:
1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.
2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

Sección octava
Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.
3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.
2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kawsay.
3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.
4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.
5. Reconocer la condición de investigador de acuerdo con la Ley.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursable. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

Ley Orgánica de Transparencia y Acceso a la Información Pública

Art. 7.-Difusión de la Información Pública.

Por la transparencia en la gestión administrativa que están obligadas a observar todas las instituciones del Estado que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República y demás entes señalados en el artículo 1 de la presente Ley, difundirán a través de un portal de información o página web, así como de los medios necesarios a disposición del público, implementados en la misma institución, la siguiente información mínima actualizada, que para efectos de esta Ley, se la considera de naturaleza obligatoria:

a) Estructura orgánica funcional, base legal que la rige, regulaciones y procedimientos internos aplicables a la entidad; las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos.

b) El directorio completo de la institución, así como su distributivo de personal;

d) Los servicios que ofrece y las formas de acceder a ellos, horarios de atención y demás indicaciones necesarias, para que la ciudadanía pueda ejercer sus derechos y cumplir sus obligaciones;

g) Información total sobre el presupuesto anual que administra la institución, especificando ingresos, gastos, financiamiento y resultados operativos de conformidad con los clasificadores presupuestales, así como liquidación del presupuesto, especificando destinatarios de la entrega de recursos públicos; i) Información completa y detallada sobre los procesos precontractuales, contractuales, de adjudicación y liquidación, de las contrataciones de obras, adquisición de bienes, prestación de servicios, arrendamientos mercantiles, etc., celebrados por la institución con personas

1.5. Hipótesis

La informática es herramienta para la prevención del delito en el Distrito Metropolitano de Quito en el año 2012

Variable Independiente

Informática

Variable dependiente

Prevención del delito

CAPÍTULO II

2. METODOLOGÍA DE LA INVESTIGACIÓN

2.1. Tipo de investigación

Correlacional

La investigación es de tipo es correlacional, porque la investigación busca entender las relaciones entre las variables, es decir pretende comprender si la informática es una herramienta que facilite para prevenir los delitos en el Distrito Metropolitano de Quito en el año 2012, para así desarrollar un plan donde se especifique los fraudes y delitos tecnológicos.

Para Consuelo Sandoval en su sitio web determina que: "Los estudios correlacionales miden las dos o más variables que se pretende ver si están o no relacionadas en los mismos sujetos y después se analiza la correlación". (Sandoval, S/F)

Por consiguiente un estudio correlacionar se puede distinguir de otros tipos de investigación

Los estudios correlacionales se distinguen de los descriptivos principalmente en que, mientras estos últimos se centran en medir con precisión las variables individuales (varias de las cuales se pueden medir con independencia e n una sola investigación), los estudios correlaciónales evalúan el grado de relación entre dos variables —pudiéndose incluir varios pares de evaluaciones de esta naturaleza en una única investigación (comúnmente se incluye más de una correlación).

2.2. Enfoque

El enfoque de la investigación es mixto es decir es cuantitativo y cualitativo, ya que estos proveerán de mayor información para verificar la hipótesis planteada.

Cuantitativo.- se utiliza este enfoque porque a través de cuadros estadísticos se puede explicar la incidencia del problema y tener datos más concisos sobre los beneficios que tiene la informática sobre la detección de delitos.

Cualitativo.- Partiendo de la observación y la experimentación se puede interpretar el desarrollo del problema, ya que el investigador tiene un estrecho vínculo con la investigación, es decir éste trabaja en el Área de Seguridad Ciudadana, por lo que es más fácil conseguir datos e información.

2.3. Técnicas y herramientas de la investigación

Técnica de la Investigación

La metodología que se va a utilizar es la observación y bibliográfico.
La observación identifica las estrategias informáticas utilizadas para realizar delitos y cómo a través de la experimentación se puede crear un sistema para evitar estos fraudes tecnológicos

Por otro lado es bibliográfico, porque a través de antecedentes investigativos se puede verificar estudios preliminares del tema y partiendo de esos resultados se puede fortalecer esta investigación

Herramientas de la Investigación

La finalidad de las herramientas de la investigación son de verificar la hipótesis y resolver el problema para proveer de resultados y así evaluar si se lograron o no los objetivos.

Encuesta: está dirigida a un sector específico el cual será elegido al azar para que exista objetividad en la investigación está herramienta otorgará información, para verificar la variable independiente y dependiente

2.4. Recolección de Datos

La recolección de datos se realizará por medio de encuestas y los cuadros estadísticos. Estas cuadros condescenderán distinguirán y valorarán la información adquirida para comprender la incidencia de la informática como herramienta para la prevención del delito.

2.5. Procesamiento de la Información

Una vez obtenido los resultados de la investigación, los datos serán procesados, por medio del programa de Office Excel, el cual a través de su exactitud, medirá el rango del problema y ayudará a la interpretación de la información.

2.6. Población y Muestra

Población

Partiendo desde la concepción que población es un conjunto de los individuos o cosas sometido a una evaluación estadística mediante muestreo. La actual población fue seleccionada al azar, es decir la Avenida “Amazonas” se ha convertido en lugar muy comercial, tanto para personas extranjeras como nacionales, por lo que en el tramo entre la Av. Patria y Colón se ha localizado varias instituciones financieras, como:

Tabla Nº 2 Población

INFORMANTES	FRECUENCIA
Habitantes del sector de “La Mariscal”	300
Usuarios de los Bancos	200
Total	**500**

Elaborado por: Roberto Mejía

Muestra

De la población de 500 se procede a calcular el tamaño de la muestra o número de personas a ser encuestada a lo cual, se aplica un nivel de confianza de 95% y un margen de error del 5%, reflejado en la siguiente fórmula:

Dónde:

n: Tamaño de la muestra

Z2: Nivel de confianza 95% (1.96)

N: Universo o población

e: Margen de error 5%

p: probabilidad de ocurrencia = 0.5

q: probabilidad de no ocurrencia 1- 0.5 **=** 0.5

N =		500
z =	95%	1.96
e =	5 %	0.05

Tabla Nº 3 Muestra

INFORMANTES	**PORCENTAJES**
Habitantes y Usuarios	217
Total	217

Elaborado por: Roberto Mejía

2.7. Análisis e Interpretación

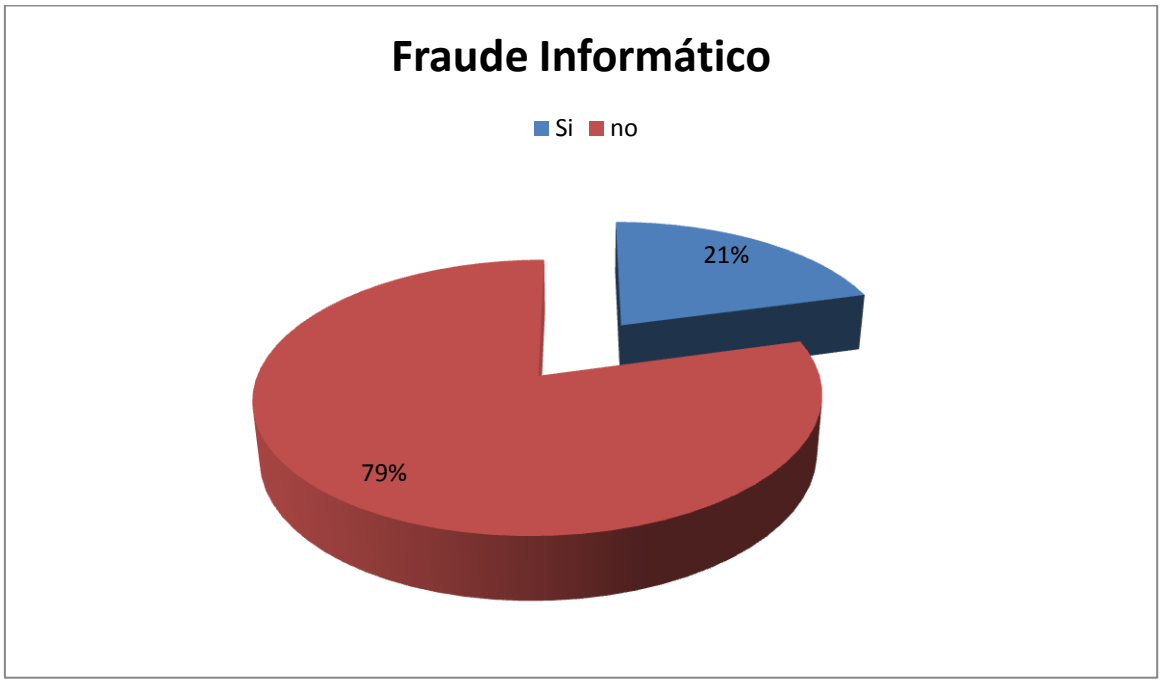
1. ¿Ha sido víctima de fraude informático?

Tabla Nº 4Víctima de fraude informático

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	47	21%
NO	180	79%
TOTAL	**217**	**100%**

Elaborado por:

Gráfico Nº 2 Víctima de fraude informático



Elaborado por: Roberto Mejía

El 21% de los encuestados afirma que si ha sufrido algún delito informático mientras el 79% no ha padecido este problema, por lo que estos datos permiten entender que aún en la ciudad de Quito, no es latente la existencia de fraude informático, ya que las medidas de seguridad que les brindan los bancos, las redes sociales han sido las adecuadas para proteger sus datos personales.

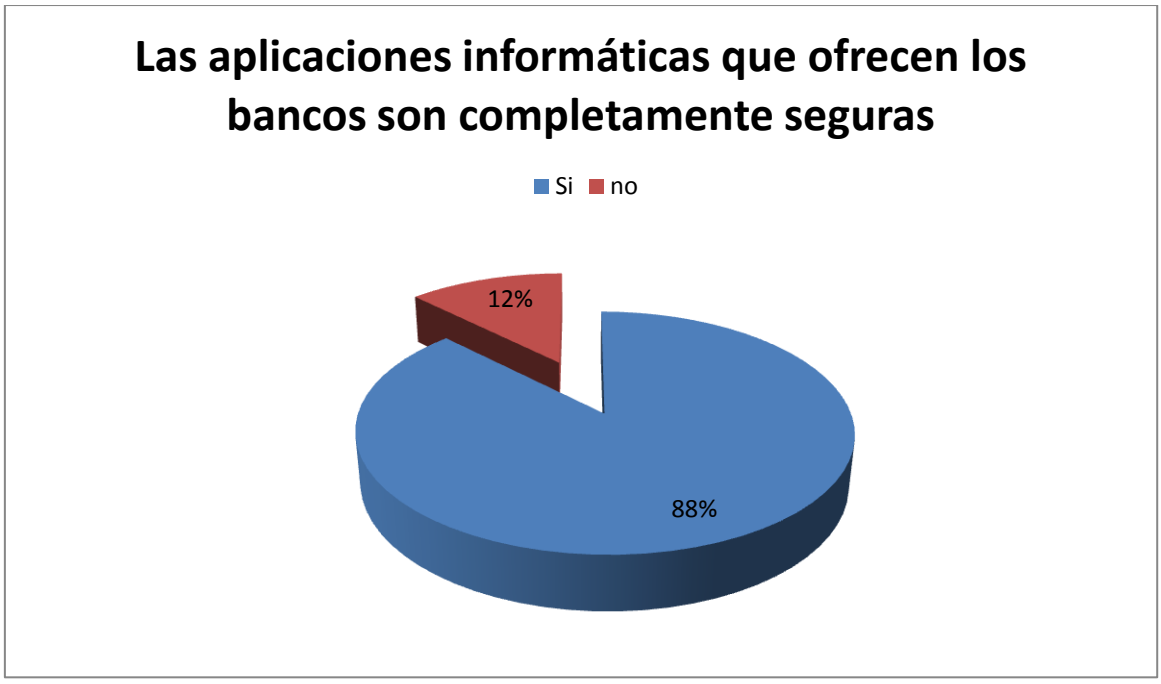
2. **¿Cree usted que las aplicaciones informáticas que ofrecen los bancos son completamente seguras?**

Tabla Nº 5 Seguridad en las aplicaciones informáticas que ofrecen los bancos

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	190	88
NO	27	12
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 3 Seguridad en las aplicaciones informáticas que ofrecen los bancos



Elaborado por: Roberto Mejía

El 88% de los encuestados afirman que las aplicaciones informáticas que ofrecen los bancos son completamente seguras, mientras que el 22% no confía en las seguridades que tienen los bancos, por lo que prefieren hacer sus transacciones y retiros bancarios manualmente, o de forma personalizada.

La confiabilidad que tienen los clientes con sus bancos todavía no es segura, por lo que los bancos han optado por brindar todas las seguridades para no perder clientes y sobre todo, para que su prestigio no sea afectado.

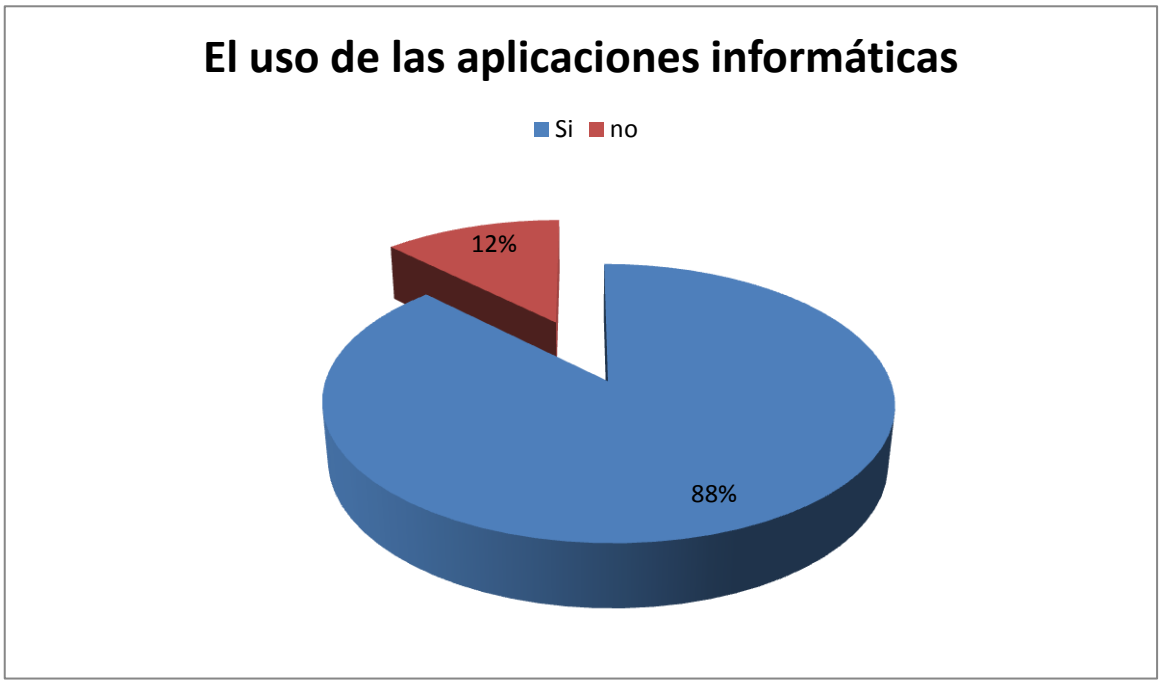
3. **¿usa normalmente las aplicaciones informáticas que su entidad financiera le ofrece?**

Tabla Nº 6 Uso de las aplicaciones informáticas que su entidad financiera oferta

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	190	88
NO	27	12
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 4Uso de las aplicaciones informáticas que la entidad financiera oferta



Elaborado por: Roberto Mejía

Con respecto a la normalidad que utilizan los usuarios las aplicaciones informáticas que su entidad financiera, el 88% de encuestados hacen uso, ya sea por la facilidad que tienen o porque confían en ello. Pero existe un 12% que no hace uso de las mismas, por lo que las instituciones bancarias pueden proveer de capacitaciones, para que dichas personas conozcan de los beneficios, tanto por tiempo como por comodidad.

4. **¿Cree usted que los bancos cuentan con personal especializado para fortalecer los sistemas informáticos?**

Tabla Nº 7Bancos cuenta con personal especializado

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	210	97%
NO	7	3%
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 5 Bancos cuenta con personal especializado

Elaborado por: Roberto Mejía

Según la población encuestada el 97% afirman que los bancos si cuentan con personal especializado para fortalecer los sistemas informáticos, mientras que un 3% desconocen de estas personas.

Tener personas capacitadas sobre el uso de las aplicaciones informáticas permite brindar un servicio de calidad para que sus usuarios confíen en las instituciones bancarias y así evitar que ellos sufran fraude informático.

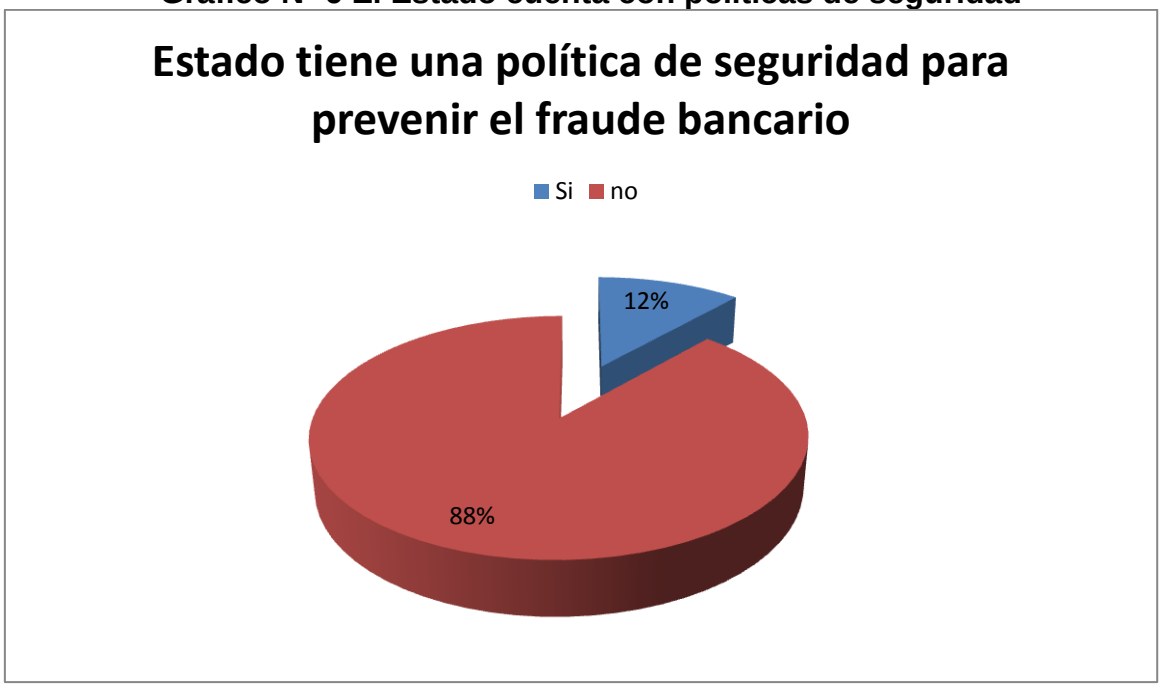
5. **¿Sabe si el Estado tiene una política de seguridad para prevenir el fraude bancario?**

Tabla Nº 8El Estado cuenta con políticas de seguridad

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	25	12
NO	192	88
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 6 El Estado cuenta con políticas de seguridad



Elaborado por: Roberto Mejía

De 217 personas encuestadas el 88% afirman que desconocen de las normas, leyes y estatus que velen por las seguridades para prevenir o evitar el fraude bancario, mientras que el 12% de la población total si conoce dichas políticas, ya sea por conocimiento propio, por la difusión en los medios de comunicación o porque la instituciones bancarias han brindado información útil para sus clientes.

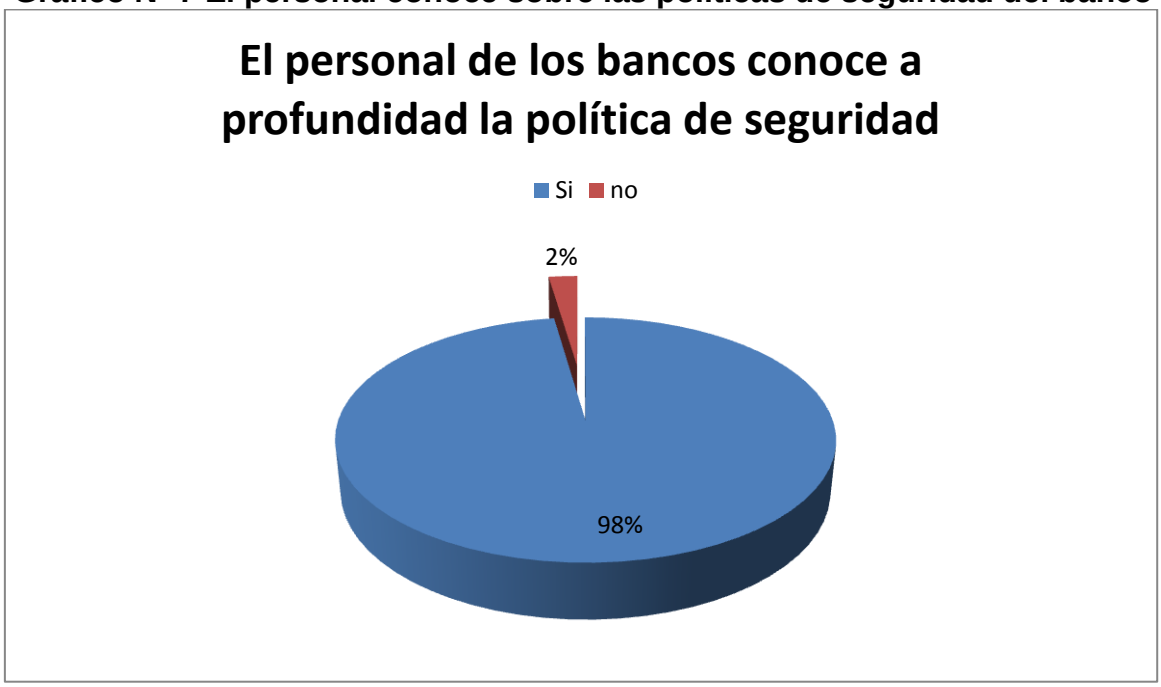
6. **¿Cree usted que el personal de los bancos conoce a profundidad la política de seguridad contra el robo informático?**

Tabla Nº 9 El personal conoce sobre las políticas de seguridad del banco

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	212	78
NO	5	22
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 7 El personal conoce sobre las políticas de seguridad del banco



Elaborado por: Roberto Mejía

El 98% de las personas encuestadas afirma que confía en que el personal de los bancos conozcan sobre ello, ya que ellos conocen a profundidad la política de seguridad contra el robo informático, por otro lado un 2% cree que el personal de las instituciones desconocen de las políticas de seguridad que tiene cada banco. Esta desconfianza que tiene los clientes por los conocimientos de los empleados de las instituciones bancarias, se da, porque los usuarios no han recibido una atención de calidad, por lo que muchos usufructuarios han optado por cambiar de banco o por realizar sus transacciones manualmente.

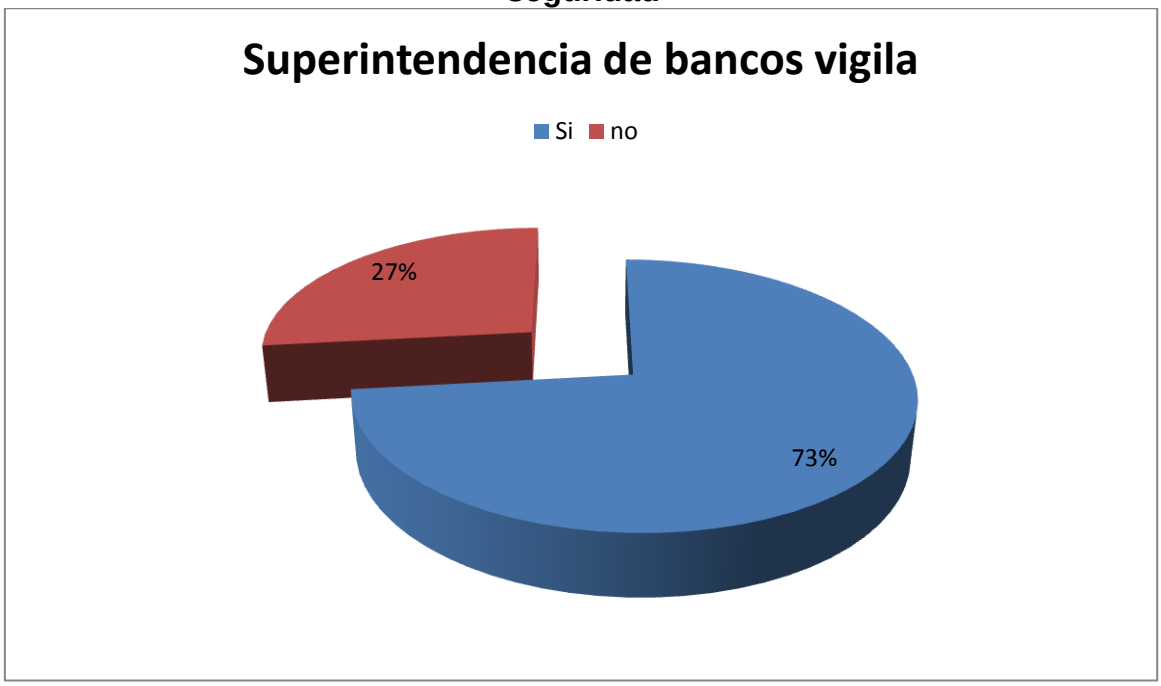
7. **¿cree usted que la Superintendencia de Bancos y Seguros vigila que las políticas de seguridad se cumplan en las instituciones financieras?**

Tabla Nº 10 Superintendencia de Bancos y Seguros y políticas de seguridad

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	159	73
NO	58	27
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 8 Superintendencia de Bancos y Seguros y las políticas de seguridad



Elaborado por: Roberto Mejía

El porcentaje de legitimación que tiene entre clientes y Superintendencia de Bancos y Seguros es alto, ya que según el grupo encuestado el 73% afirma que dicha institución vigila que las políticas de seguridad se cumplan en las diferentes instituciones financieras. El 27% de desconfianza radica en que las personas encuestadas no conocen del trabajo que tiene la Superintendencia de Bancos y Seguros, ya que ha preferido difundir el trabajo de la institución antes que proyectos que velen por la brindar seguridad sobre los delitos informáticos.

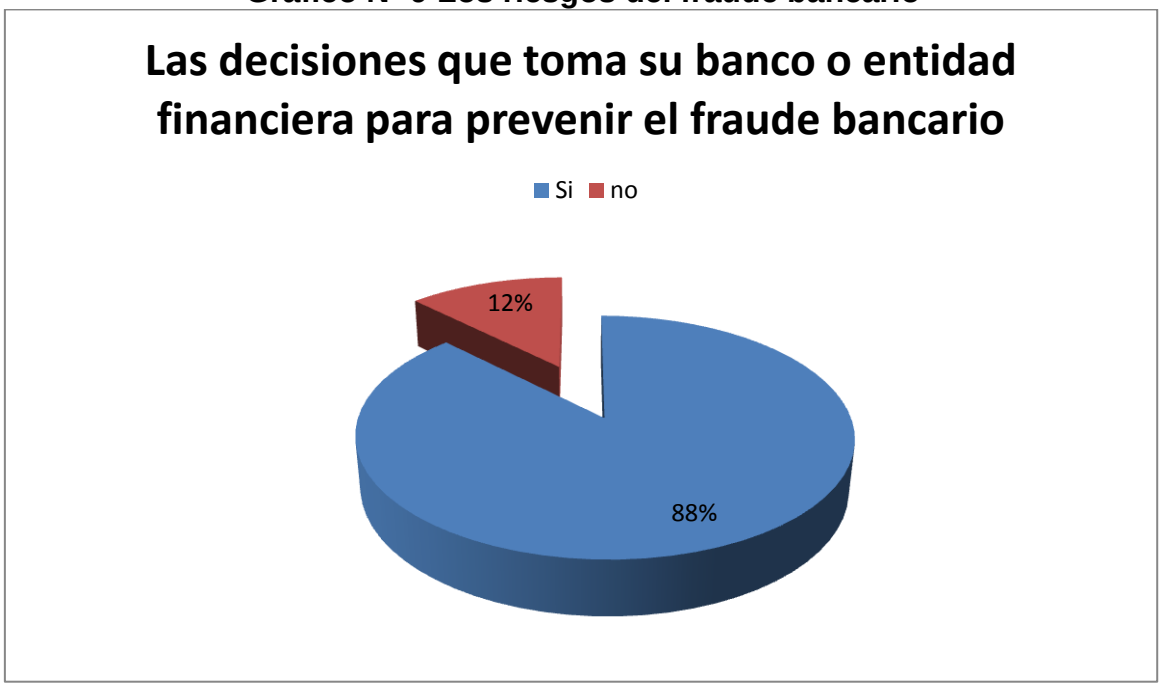
8. **Su banco o institución financiera ¿le ha explicado los riesgos del fraude bancario?**

Tabla Nº 11 Los riesgos del fraude bancario

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	25	12
NO	192	88
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 9 Los riesgos del fraude bancario



Elaborado por: Roberto Mejía

El 88% de la población encuestada nos dice que su Banco o Institución Financiera no le ha explicado los riesgos del fraude, y tan solo 25 personas encuestadas afirman lo contrario es decir solo un 25%.

Después de haber realizado el análisis podemos decir que la mayor parte de las personas encuestadas desconocen las decisiones que toma su Banco o Entidad Financiera para prevenir el fraude bancario, es decir que si su banco sufre un fraude los únicos perjudicados serían los cuenta ahorrista y cuenta corrientista, probablemente por las malas decisiones de los directivos de las instituciones financieras.

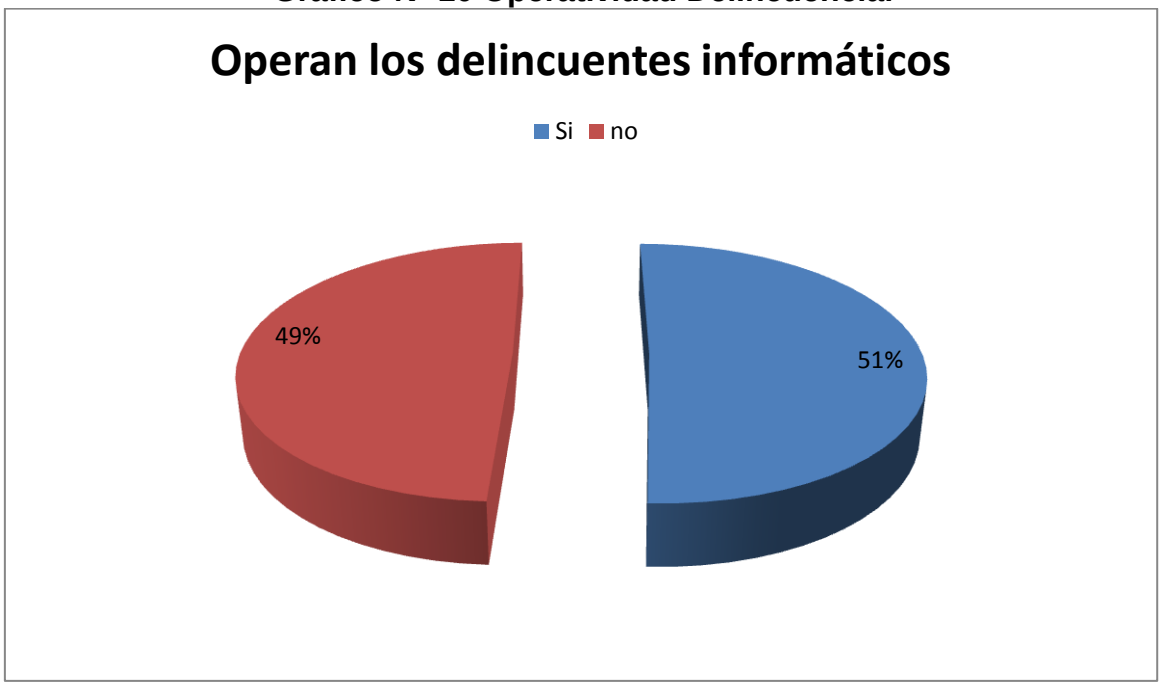
9. ¿sabe usted cómo operan los delincuentes informáticos?

Tabla Nº 12 Operatividad Delincuencial

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	110	51
NO	107	49
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 10 Operatividad Delincuencial



Elaborado por: Roberto Mejía

De 217 personas encuestadas el 51% afirman que conocen el modo operandi de los delincuentes informáticos y que el 49% desconocen

La mayor parte conoce cómo operan los delincuentes informáticos, de cierta manera porque algún familiar, amigo o ellos mismos fueron víctimas de esta nueva forma de delincuencia, lo cual afecta gravemente a la economía del ecuatoriano.

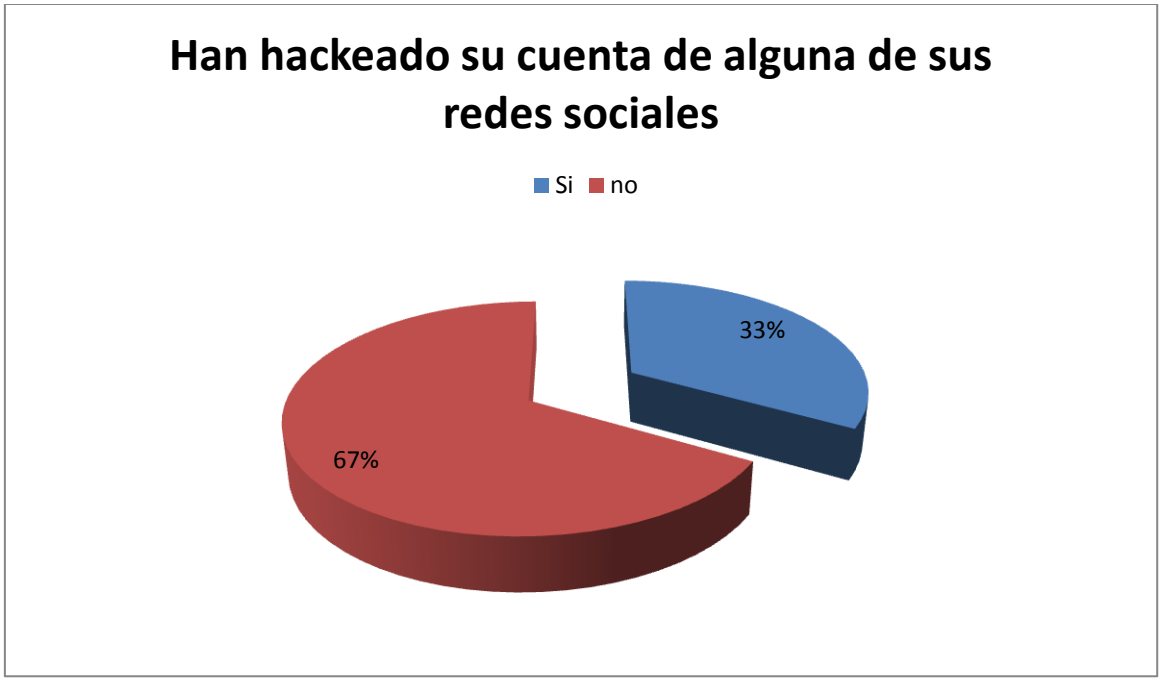
10. ¿alguna vez han hackeado su cuenta de alguna de sus redes sociales?

Tabla Nº 13 Hackeo en las cuentas de las redes sociales

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	72	33
NO	145	67
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 11Hackeo en las cuentas de las redes sociales



Elaborado por: Roberto Mejía

El 33 % de la población encuestada dice que en algún momento le han hackeado su cuenta en alguna red social mientras que el 67% dice lo contrario.

Hackear cuentas en las redes sociales antes era considerado como algo no tan significativo, pero con el paso de los años, el plagio de información en las redes sociales se ha convertido en algo sumamente peligroso. Por lo que cada res social, como Facebook han buscado formas de controlar el ingreso a estas formas de comunicación.

11. ¿ha sentido que las políticas de seguridad de algunas páginas son suficientes para evitar ser víctima de los delincuentes informáticos?

Tabla Nº 14 Seguridad en los sitios en web

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	34	16
NO	183	84
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 12 Seguridad en los Sitios Web

Elaborado por: Roberto Mejía

El 16% de las personas q fueron encuestadas nos dice que si ha sentido que las políticas de seguridad de algunas páginas son suficientes para evitar ser víctima de los delincuentes informáticos mientras que el 84% consideran que deberían incrementar los niveles de seguridad

La mayor parte de las personas encuestadas considera que no son suficientes los niveles de seguridad que existen hoy en día en las páginas de internet y que se debería aumentar los niveles de seguridad para evitar futuras estafas.

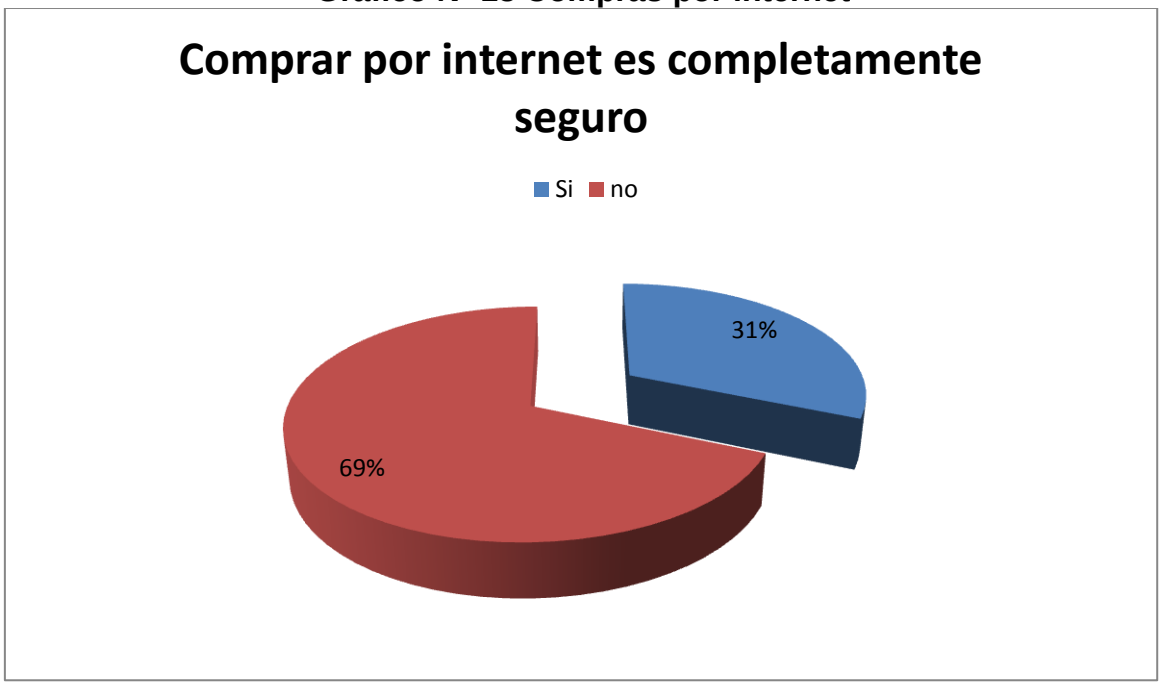
12. ¿cree usted que comprar por internet es completamente seguro?

Tabla Nº 15 Compras por internet

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	68	31
NO	149	69
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 13 Compras por internet



Elaborado por: Roberto Mejía

El 31% de las personas encuestadas afirman que comprar por internet es seguro mientras que el 69% dice lo contrario.

La mayor parte de las personas encuestadas dicen que no son seguras las compras por internet, lo que se oferta en la web resulta una pérdida de tiempo y dinero, en ocasiones una completa estafa, porque se pierde el dinero invertido o porque el bien adquirido no cumple con las características que se menciona en la web.

13. ¿consideras que los pagos por internet manejan una política eficaz para evitar falsificaciones?

Tabla Nº 16 Pagos por Internet

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	75	35
NO	142	65
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 14 Pagos por Internet

Elaborado por: Roberto Mejía

El 35% de la población encuestada manifiesta que los pagos por internet manejan una política eficaz para evitar falsificaciones mientras que la mayoría que corresponde a un 65% dice lo contrario.

La mayor parte de la población encuestada quisiera que las políticas de los pagos por internet sea más eficaces y seguras para evitar las falsificaciones, desviaciones de fondos, fraudes, etc., y de estar manera tener una confiabilidad alta al momento de realizar las transacciones por internet, la cual resulta una herramienta muy útil que ayuda a ahorrar tiempo.

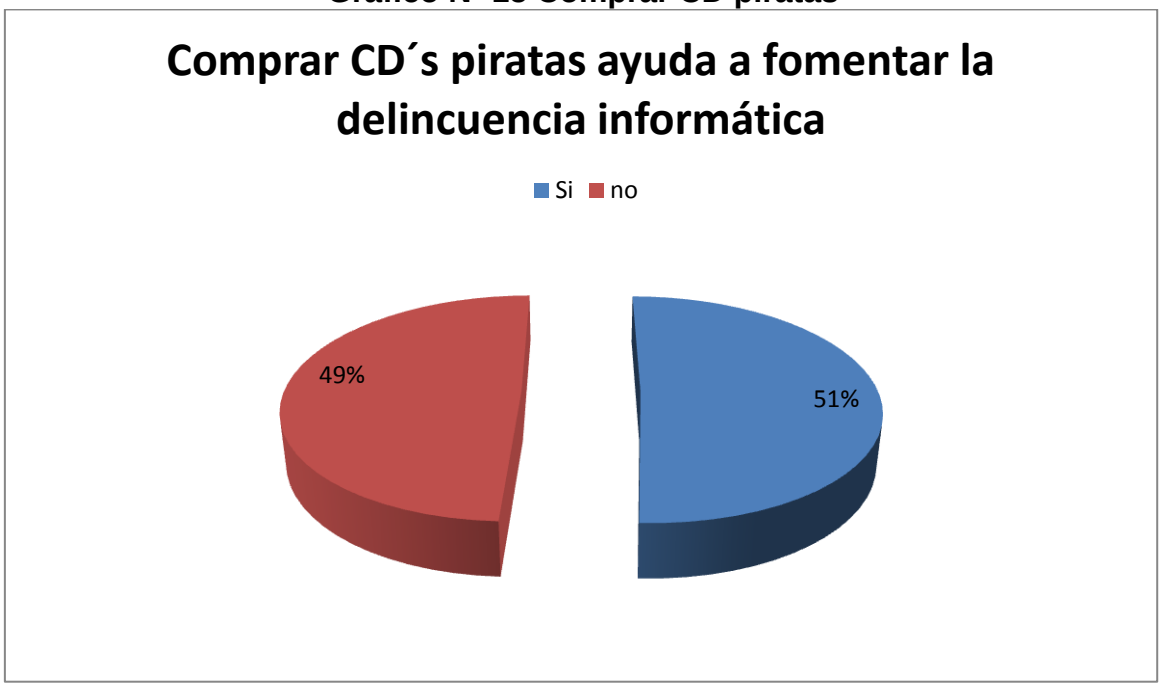
14. ¿considera que comprar CD piratas ayuda a fomentar la delincuencia informática?

Tabla Nº 17 Comprar CD piratas

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	110	51
NO	107	49
TOTAL	**217**	**100%**

Elaborado por: Roberto Mejía

Gráfico Nº 15 Comprar CD piratas



Elaborado por: Roberto Mejía

El 51% de las personas encuestadas afirma que los cd piratas fomentan la delincuencia informática este dato no está exento de una igualdad ya que el 49% asevera que no fomenta la delincuencia.

Según la población encuestada los artistas ecuatorianos conocen al mercado nacional, y saben que sus cd serán copiados, por lo que miran en la piratería como algo natural. De manera que, las copias ilícitas sostienen la microeconomía de algunas familias, por consiguiente el Estado creo una ley que regularice esta forma de negocio.

CAPITULO III

3. PROPUESTA

3.1. Tema:

Guía para prevenir Delitos Informáticos

3.2. Antecedentes

Los delitos informáticos en los últimos años han sido los que más han afectado la economía de la ciudad de Quito, en especial a sus familias, ya que éstos no sólo están definidos como robos bancarios, sino que varias cuentas en las redes sociales han sido plagiadas, por lo que muchas de las identidades de las ciudadanos han sido afectadas o desprestigiadas.

De la misma manera, Las compras por internet no tienen políticas de seguridad que garanticen el servicio, por lo que muchos compradores han sido estafados y según sus testimonios, es porque las personas no tienen el conocimiento, ni la experiencia para identificar quienes son vendedores confiables. Además el Ecuador no tiene las políticas de seguridad en comparación con otros países, por ejemplo en Estados Unidos en 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030) donde se contempla la regulación de los virus. Además afirman que

> Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

La encuesta dirigida a los habitantes del Sector de la Mariscal, en especial los usuarios que utilizan los servicios bancarios de: Produbanco, Pacífico, Bolivariano, Guayaquil, Pichincha fueron quienes facilitaron de información adecuada para realizar esta propuesta.

En dicha encuesta se reafirma el desconocimiento que tienen los usuarios por el peligro que tiene el delito informático, de manera que la siguiente propuesta está enfocada para brindar información a aquellas personas que recién se involucran en el manejo de los servicios digitales que tiene cada institución bancaria.

3.3. Justificación

La razón de hacer una guía de prevención de delitos informáticos es fundamental, ya que el robo bancario, el plagio de identidades en las redes sociales y la piratería se ha vuelto parte diario vivir, es decir se ha naturalizado en las mentes de los habitantes de la ciudad de Quito y en especial en las personas que utilizan los servicios de las instituciones bancarias que se encuentran en el sector de la Mariscal.

Por consiguiente esta propuesta no busca solucionar un problema sino evitar que ésta se reproduzca y afecte a más habitantes del sector, porque si este problema persiste el prestigio de muchas instituciones bancarias privadas decaerán y sus clientes optarán por utilizar los servicios bancarios estatales.

3.4. Objetivo

3.4.1. Objetivo General

Desarrollar una guía para prevenir delitos informáticos en el sector de La Mariscal

3.4.2. Objetivo Específico

- Enlistar los delitos informáticos más comunes en el sector de la Mariscal
- Explicar en qué consiste los delitos bancarios.
- Definir los delitos informáticos que afectan a la población del Distrito Metropolitano de Quito para organizar procesos y propuestas de seguridad.

GUÍA PARA PREVENIR DELITOS INFORMÁTICOS

Autor: Roberto Mejía

Delimitación del Fenómeno de la Delincuencia Informática

Vivir con armonía en el Estado nación es el ideal de todo individuo, ya que la convivencia pacífica se ha convertido en el objetivo principal de toda organización social, aunque existen formas de relación social en que los conflictos que le son inherentes, puedan ser procesados de modo violento.

Esta convivencia pacífica está vinculada, por un lado, al poder económico, y por otro al desarrollo institucional y cultural que asuman a la organización civil y política como forma de convivencia civil, es decir a la lógica social que se plantea en un grupo social establecido.

De manera que el Estado tiene como obligación garantizar la seguridad de sus miembros. Pero fundamentalmente, es la misma sociedad la que debe asentar la bases de sus propia seguridad, a esto se lo denomina seguridad ciudadana.

Hay que entender que la seguridad ciudadana no le exime al estado de su compromiso, sino que es todo lo contrario, es decir que la seguridad ciudadana establece capacidades de interacción autónomas de los sujetos sociales y el guía por los senderos de la reforma permanente de su cultura institucional.

Por consiguiente las Tecnología de la Información y Comunicación (TIC), según Castells afirma

> Las TICS son probablemente uno de los fenómenos tecnológicos, sociales, económicos, políticos y culturales cuya magnitud y complejidad no acaba todavía de ser dimensionados, así como sus efectos. Los cambios que ha ocasionado y ocasionarán en todos los órdenes de la vida cotidiana, confrontan nuevas geografías de responsabilidad y de poder. (2010, pág. 451)

Relacionar las TICS con la seguridad, en especial con la seguridad ciudadana es la función que tiene esta propuesta, para así evitar los fraudes económicos, amenazas a la privacidad, daños técnicos, acecho o agresión coercitiva del ciudadano y manipulación de información

De manera que, el desarrollo de las tecnologías de la información ha afectado a muchas personas, lo cual ofrece un aspecto negativo, es decir ha abierto la puerta a conductas antisociales y delictivas. Donde los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

> El aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después (1999, pág. 34)

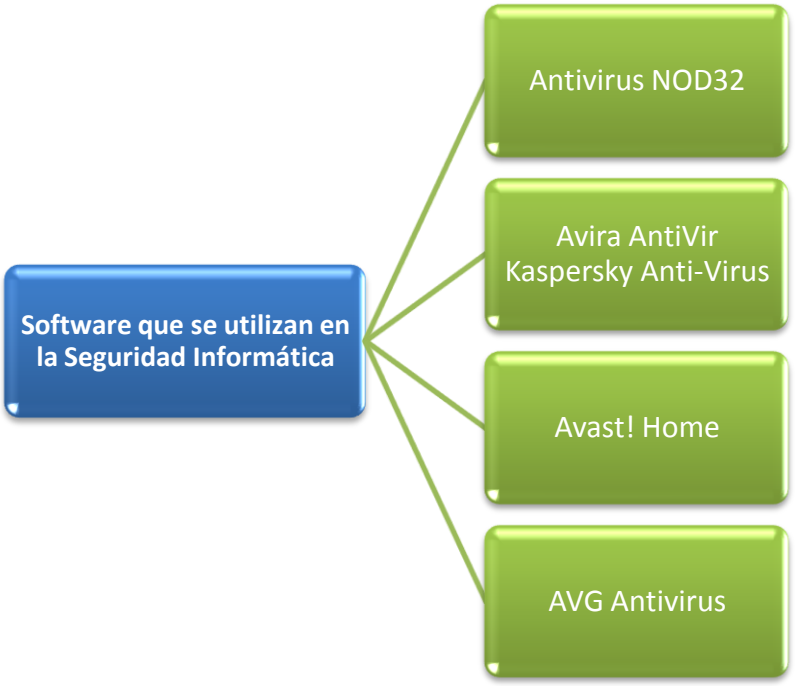
Delito Informático

Las amenazas de la Seguridad Informática

Existen distintas amenazas para la seguridad informática en la actualidad como son el Shouldersurfing, Eavesdropping, Dumpsterdiving, observación, dispositivos móviles perdidos, prensa, foros online, sitios web, herramientas en línea. Ingeniería social. Todos estas amenazas tiene un solo factor común obtener información para posteriormente ser usada para causar delitos y estafas informáticas.(http://diginota.com/, 2008)

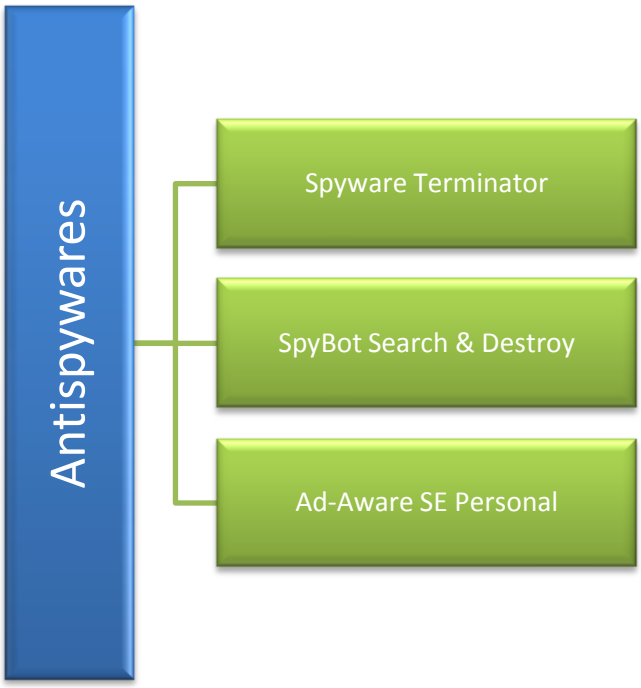
Software que se utilizan en la Seguridad Informática

Los antivirus son los mejores programas fundamentales para proteger nuestras computadoras contra los virus informáticos son los antivirus los cuales son:



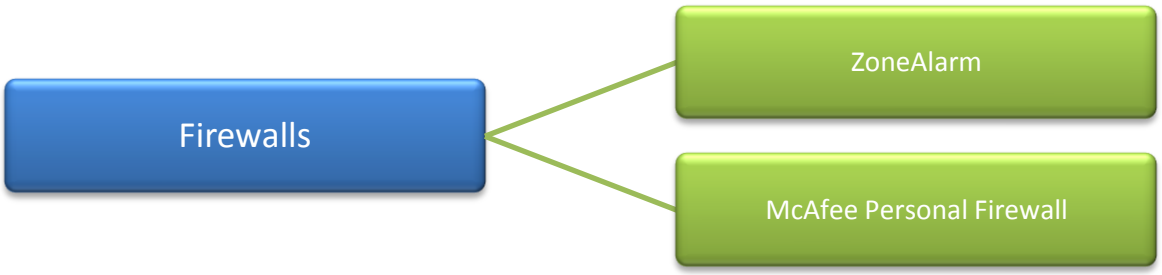
Fuente: (http://www.bloginformatico.com/, 2008)

Además de esto existen programas que han sido creados combatir programas especialmente espías los cuales se los conoce como los antispywareslos cuales son:



Fuente: (http://www.bloginformatico.com/, 2008)

Por otra parte, están los firewalls o cortafuegos que protegen tu computadora contra todas aquellas conexiones dañinas para tu computador los cuales son:



Fuente: (http://www.bloginformatico.com/, 2008)

Consejos para la Seguridad Informática

Se debe tomar en cuenta estos consejos de la Seguridad Informática para proteger su información:

Fuente: (http://www.mundofranquicia.com/, 2008)

Medidas preventivas en la Seguridad Informática

Debemos tomar en consideración estos aspectos preventivos de la Seguridad Informática para evitar los delitos informáticos:

- Mantener las máquinas actualizadas y seguras físicamente.
- Mantener personal especializado en cuestiones de seguridad.
- Administra bien las redes y configurar adecuadamente los routers.
- Mantenerse informado constantemente sobre cada una de las vulnerabilidades encontradas y parches lanzados.
- Utilizar protocolos seguros como http, ssh.
- Encriptación de mails mediante GPG.
- Migrar a otros sistemas operativos como GNU/Linux, Solaris, BSD. (José Antonio Martínez Torres, 2005)

Importancia de la Seguridad Informática

Es importante la Seguridad Informática en la actualidad porque esta nos protege de muchas amenazas informáticas como el software pirata, hackers, crackers, virus y otro software maliciosos del ciberespacio que nos rodea. (Daniel Werner Berrio, 2006)

Marco Conceptual

El marco conceptual a utilizar, está determinado por conceptos que se utilizarán en la presente propuesta, por lo que fue necesario utilizar varios a los términos, los cuales guiarán este proceso de investigación.

Privacidad.- Se define como el derecho de mantener de forma reservada o confidencial los datos de la computadora y los que intercambia con su red.

Software.- Es todo el conjunto intangible de datos y programas de la computadora

Cortafuegos.- Es un sistema que previene el uso y el acceso desautorizados a tu ordenador.

Hackers.- Son personas que entra de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo.

Crackers.-Se utiliza para referirse a las personas que rompen algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.

Virus.- Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora.

Antivirus.- Es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio.

Anti-spyware.- Es un programa que detecta y elimina y bloquea toda clase de spyware, adware, troyanos spyware, keyloggers, suplantación de identidad, secuestradores de navegador, amenazas de rastreo, anti-spyware maligno, software no .

Internet.- Es una red de redes de millones de ordenadores en todo el mundo.

Firewall.-Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet.

El Cloud computing.- Es una tecnología que utiliza el Internet y servidores centrales remotos para mantener datos y aplicaciones. Esta tecnología permite una computación mucho más eficiente por el almacenamiento de datos centralizar el procesamiento y ancho de banda.

Shouldersurfing- Un término usado para describir a una persona que mira por encima del hombro de otra persona a medida que entran los datos en una computadora u otro dispositivo.

Eavesdropping.- Es una técnica para capturar información escuchando las conversaciones privadas.

Dumpsterdiving.- La búsqueda de información valiosa en la basura es una práctica que puede resultar riesgosa para una empresa.

Firewall personal

El término firewall personal se utiliza para los casos en que el área protegida se limita al ordenador en el que el firewall está instalado.
Un firewall personal permite controlar el acceso a la red de aplicaciones instaladas en el ordenador y prevenir notablemente los ataques de programas como los troyanos, es decir, programas dañinos que penetran en el sistema para permitir que un hacker controle el ordenador en forma remota. Los firewalls personales permiten subsanar y prevenir intrusiones de aplicaciones no autorizadas a conectarse a su ordenador.

Limitaciones del Firewall

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante un módem o cualquier otro medio de conexión que evite el firewall.

Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.

Para garantizar un nivel máximo de protección, debe ejecutarse un firewall en el ordenador y su registro de actividad debe controlarse para poder detectar intentos de intrusión o anomalías. Además, se recomienda controlar la seguridad (por ejemplo, inscribiéndose para recibir alertas de seguridad de CERT) a fin de modificar los parámetros del dispositivo de firewall en función de las alertas publicadas.

Fundamentación Legal

Un modelo propuesto según la norma ISO 17799 la cual recomienda la aplicación de estándares encaminados a la seguridad informática plantea tres grandes secciones:

• Las directrices son un conjunto de reglas generales de nivel estratégico donde se expresan los valores de la seguridad de la organización.
Es propuesta por el líder empresarial de la organización y tiene como su base la misión y visión para abarcar toda la filosofía de la seguridad de la información.

• Las normas son un conjunto de reglas generales y específicas de la seguridad de la información que deben ser usadas por todos los segmentos involucrados en todos los procesos de negocio de la institución, y que deben ser elaboradas por activo, área, tecnología, proceso de negocio, público a que se destina, etc. Las normas de seguridad para usuarios son dirigidas para el uso de ambientes informatizados, basadas en aspectos genéricos como el cuidado con las claves de acceso, manejo de equipos o estaciones de trabajo, inclusión y exclusión de usuarios, administración de sistemas operativos, etc.

• Los procedimientos e instrucciones de trabajo son un conjunto de orientaciones para realizar las actividades operativas, que representa las relaciones interpersonales e interdepartamentales y sus respectivas etapas de trabajo para su implementación y mantenimiento de la seguridad de la información.

Conclusiones

Las redes sociales online son servicios prestados a través de internet que autorizan a los usuarios a generar un perfil público, en el que plasmar datos personales e información de uno mismo, suministran de herramientas para interactuar con el resto de usuarios afines o no al perfil publicado. Un perfil virtual es la representación del sujeto en ausencia de él, es decir que cuando un individuo dice lo que es en la red social, está comunicando lo que desea o anhela ser, ya que lo beneficioso del mundo virtual es alejarse de la realidad para internarse en una nueva realidad.

Es así como las realidades cambian, lo que se percibe en la web se convierte en un acto real, por lo que comprender la importancia del mundo *online* en las relaciones intrapersonales será fundamental para comprender el agravio que tiene los delitos informáticos en el sistema que tiene cada ser humano.

Presupuesto

Actividad	Costo USD
1. Revisión bibliográfica	$150.00
2. Movilización, transporte y comunicaciones	$50.00
3. Impresiones (borradores y trabajo final)	$150.00
4. Encuestas	$30.00
5. Instrumentos para la recolección de información (diario de campo, grabadora)	$150.00
6. Imprevistos	$130.00
Subtotal	**$660.00**
Inflación estimada para 2014 (5%)	**+(5%) $36,50**
Total	**$696,50**

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Una vez realizado esta investigación, se llegó a muchas conclusiones las cuales fueron plasmadas en el capítulo de Análisis e Interpretación, de todas ellas se tomaran a las más representativas y se intentará acoplarlas a los objetivos planteados y verificar la hipótesis propuesta.

El delito informático en el Distrito Metropolitano de Quito en el año 2012 es alto, ya que varios usuarios que utilizan el servicio bancario han sufrido algún tipo de robo de contraseñas, de igual forma sucede cuando hacen comprar por internet, ya que el servidor como Mercado Libre, EBay, Amazon, etc., no proveen de seguridad en las compras.

La principal razón para que exista delito informático, es que el internet se ha convertido en una forma más de interrelacionarse entre los seres humanos por lo que, es primordial crear un marco legal que controle, proteja y ampare a los ciudadanos

Se pudo definir los delitos informáticos que más afectan a la población del Distrito Metropolitano de Quito, entre ellos están plagios de contraseñas ya sea de sus cuentas bancarias como en las redes sociales, este tipo de delito es el más común en nuestro país, ya que con ello se ha creado cuentas fantasmas y la apropiación de la identidad del ciudadano

Es primordial plantear una propuesta de solución que disminuya el impacto que provocan los fraudes informáticos, ya que la única solución que se tiene, por el momento, es enseñar a las personas sobre la gravedad del problema, ya que si ellos conocen serán menos propensos a padecer delito informático.

Esta solución no va sola, es decir que el Estado ecuatoriano debe tener un marco legal que vele por la seguridad ciudadana, además los policías y los empleados

de los diferentes bancos de la ciudad deben brindar toda la información que puedan, ya que trabajando en conjunto como un sistema se puede prevenir, para luego erradicar el problema de delito informático.

4.2. Recomendaciones

El estado Ecuatoriano debe involucrarse más en al tema desde instituciones nacionales, como la fiscalía o las cortes de justicia y otros organismos de protección y poder estatal tradicionalmente ligados a la construcción y sustento de las ideas de ciudadanía y seguridad.

Las instituciones financieras, tanto estatales como privadas deben proveer de información a sus clientes sobre el manejo y el riesgo que tienen las aplicaciones *online,* ya que estas a más ahorrar tiempo generan una cultura digital que va a la par con el sistema económico de turno, donde la tecnología ha cubierto en gran parte de la vida diaria.

La guía que se pretende implementar debe estar sostenida por cursos de capacitación para que los usuarios conozcan de los beneficios que tiene la web en la vida diaria.

Finalmente un trabajo en conjunto fortalecerá la implementación de esta guía de seguridad, donde la primera fase está informar, para luego prevenir y al final poder erradicar. Por ello es necesario estar en constante capacitación ya que, la tecnología no espera a que el ser humano se habitué a ella, la tecnología con el paso de los años es mejorada y por ende ciudadanos, policía nacional, empleados de las instituciones financieras y servidores públicos deben estar en arduo proceso de aprendizaje.

5. GLOSARIO DE TÉRMINOS

Seguridad Informática-
Es el área de la informática que se enfoca en la protección de la infraestructura computacional.

Estafas.-
El sujeto activo del delito se hace entregar un bien patrimonial, por medio del engaño; es decir, haciendo creer la existencia de algo que en realidad no existe.

Tecnología.-
Es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de las personas.

Información.-
Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Fraudes.-
Es todo aquel delito que por medio de la manipulación de los datos y programas informáticos se puede obtener lucro ilícito

Sabotaje Informático.-
Es todo daño ocasionado por la destrucción y modificación de datos, información en documentos electrónicos o redes informáticas.

Pornografía Infantil
Es la inducción, producción venta y distribución de contenido infantil con fines pornográficos o explotación sexual.

Espionaje Informático.-
Es la circulación no autorizada de datos reservados

Hackear.-

Es la capacidad de explorar un sistema hasta sus lugares más recónditos, en busca del conocimiento. Es aquel que no se conforma con lo obvio, que tiene una visión de las cosas que pasa desapercibida al resto de mortales. Es aquel que puede tener una comprensión de la totalidad, que no está mutilada por el conocimiento específico. Es aquel que puede ver lo que otros no han podido imaginar, ni tan siquiera soñar.

Antispyware.-

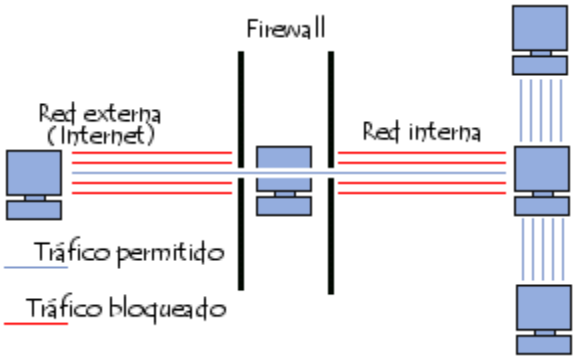
El software anti spyware ayuda a proteger su equipo contra ventanas emergentes, rendimiento lento y amenazas de seguridad provocadas por spyware y otro software no deseado. Para estar al día con las últimas formas de spyware, debe mantener actualizado su software anti spyware.

Muchos tipos de software no deseado, incluyendo el spyware, están diseñados para ser difíciles de eliminar. Si trata de desinstalar este software de la misma forma que desinstala cualquier otro programa, es posible que descubra que el programa vuelve a aparecer en cuanto reinicia el equipo.

Firewalls.-

Un **firewall** es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- una interfaz para la red protegida (red interna)
- una interfaz para la red externa.



El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

En caso de que el sistema de firewall venga en una caja negra (llave en mano), se aplica el término "aparato".

Filtrado de paquetes Stateless.-

Un sistema de firewall opera según el principio del filtrado simple de paquetes, o *filtrado de paquetes stateless*. Analiza el encabezado de cada paquete de datos (*datagrama*) que se ha intercambiado entre un ordenador de red interna y un ordenador externo.

Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP del ordenador que envía los paquetes
- La dirección IP del ordenador que recibe los paquetes
- El tipo de paquete (TCP, UDP, etc.)
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Las direcciones IP que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza.

BIBLIOGRAFÍA

- Almendáriz, J. (2011). *LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE IMBABURA.* Imbabura: Universidad Técnica del Norte.
- Balkin, M. (2003). *Cultural software. A theory of ideology.* New York: Yale University.
- Bordieu, P. (1999). *Malestares Sociales .* Barcelona.
- Calderón, J. (2011). *Seguridad informática.* Buenos Aires.
- Carlos Emilio Quinapanta Narvaéz. (2010). *La explotación infantil por parte de los padres tiende a contribuir con la economía familiar y vulnera los derechos de los niños, niñas y adolescente, establecidos en la Constitución del Ecuador.* Ambato.
- Carrión, F. (2007). Percepción de Inseguridad. *Programa Estudios de la Ciudad FLACSO*, 10.
- Castells, T. (2010). *Comunicación y Poder.* Madrid: Alianza .
- Chaves, C. (1996). *Publicado en revista Reflexión Nº 25.* Santiago de Chile: CINTRAS.
- Chiriboga, C. M. (2005). *Democracia y seguridad ciodadana en el Ecuador.* Quito.
- Edison Barrionuevo Jairo Ñacata. (2006). *Implementación de Seguridades Lógicas Informática en el Instituto Tecnológico Superior de la Policía Nacional.* Quito: ITSPN.
- Foucault, M. (1976). *Vigilar y castigar.* México: Siglo XXI.
- García, R. (1980). *Seguridad Social en el Ecuador .* Quito.
- Jorge Aníbal Yánez Suarez, Kléver Antonio Mendoza Jacome. (2005). *Diagnóstico De Los Sistemas De Seguridad Electrónica De La Cooperativa De Ahorro Y Crédito "Fundesarrollo" Agencia Matriz De La Ciudad De Quito.* Quito: ITSPN.
- Kotler, P.; Armstrong, G. (2005). *Fundamentos del Marketing.* México.
- Lima, M. d. (2001). *Delitos Electrónicos.* México: Porrua.
- Magliona Markovicth, Claudio Paúl, LÓPEZ MEDEL Macarena. (1999). *Delincuencia y Fraude Informático.* Santiago de Chile: Jurídica de Chile.
- McNally, P. (2002). *The rights of robots.* Estados Unidos: Labor.

- Miguel Gómez Perals. (1994). *Los Delitos Informáticos en el Derecho Español.* Mérida: Aranzadi.
- Ministerio del Poder Popular para la Educación Superior. (2010). *Ley S.O.P.A.* Venezuela.
- Pico, E. (2012). *Análisis de los fraudes informáticos y su incidencia en el acceso a la información .* UNIVERSIDAD TÉCNICA DE AMBATO : Ambato.
- Piscitelli, A. (2004). *Las Ciberculturas.* Madrid: Anagrama.
- Ruiz Vadillo, E. (1996). *Responsabilidad Penal en materia de informática.* Mérida.

NETGRAFÍA

- *http://diginota.com/*. (2008). Recuperado el 22 de Diciembre de 2013, de http://diginota.com/: http://diginota.com/las-10-amenazas-a-la-seguridad-informatica-mas-descuidadas/
- *http://www.bloginformatico.com/*. (2008). Recuperado el 22 de Diciembre de 2013, de http://www.bloginformatico.com/: http://www.bloginformatico.com/seguridad-informatica-principios-basicos-y-software.php
- *http://www.mundofranquicia.com/*. (2008). Recuperado el 22 de Diciembre de 2013, de http://www.mundofranquicia.com: http://www.mundofranquicia.com/reportaje.php?num=520
- *Ley P.I.P.A*. (2011). Recuperado el 27 de Diciembre de 2013, de http://skyblue.com.mx/home/index.php/noticias/662-ley-pipa
- Daniel Werner Berrio. (2006). *Seguridad Informática*. Recuperado el 22 de Diciembre de 2013, de http://www.slideshare.net/danielwernerberrio/seguridad-informatica-11978683
- Ecuador, D. (03 de Octubre de 2011). Recuperado el 5 de Noviembre de 2013, de http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426

- Estados, C. d. (24 de Febrero de 2001). Recuperado el 6 de Noviembre de 2013, de http://hub.coe.int/
- Hoy, D. E. (26 de Junio de 2013). Recuperado el 6 de Noviembre de 2013, de http://www.hoy.com.ec/noticias-ecuador/solo-1-de-cada-600-delitos-informaticos-se-denuncia-584518.html
- Informática, I. a. (1 de Mayo de 2008). *Introducción a la seguridad Informática*. Recuperado el 5 de 11 de 2013, de http://www.sisman.utm.edu.ec/libros/FACULTAD%20DE%20CIENCIAS%20INFORM%C3%81TICAS/CARRERA%20DE%20INGENIER%C3%8DA%20DE%20SISTEMAS%20INFORMATICOS/ELECTIVAS/COMPUTACION%20FORENSE/Introducci%C3%B3n%20a%20la%20Seguridad%20Inform%C3%A1tica%20Parte%20I.pdf
- José Antonio Martínez Torres. (2005). Recuperado el 22 de Diciembre de 2013, de http://www.antoniomtz.org
- Sandoval, C. (S/F). *www.csandoval.net*. Recuperado el 17 de Diciembre de 2013, de Proceso de Investigación: http://www.csandoval.net/files/Definicion%20del%20tipo%20de%20investigacion%20a%20realizar.pdf
- Seguridad Informática. (13 de junio de 2010). Recuperado el 6 de Noviembre de 2013, de http://80.32.206.136/Tecnologia_LCP/Documentos/SEGURIDAD%20INFORMATICA.pdf
- SIB. (23 de Enero de 2012). *Superintendecia de Bancos*. Recuperado el 5 de Noviembre de 2013, de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=531&vp_tip=2
- www.aulapc.es. (2010). *www.aulapc.es.* Recuperado el 27 de Diciembre de 2013, de http://www.aulapc.es/dibujo_photoshop_texto.html

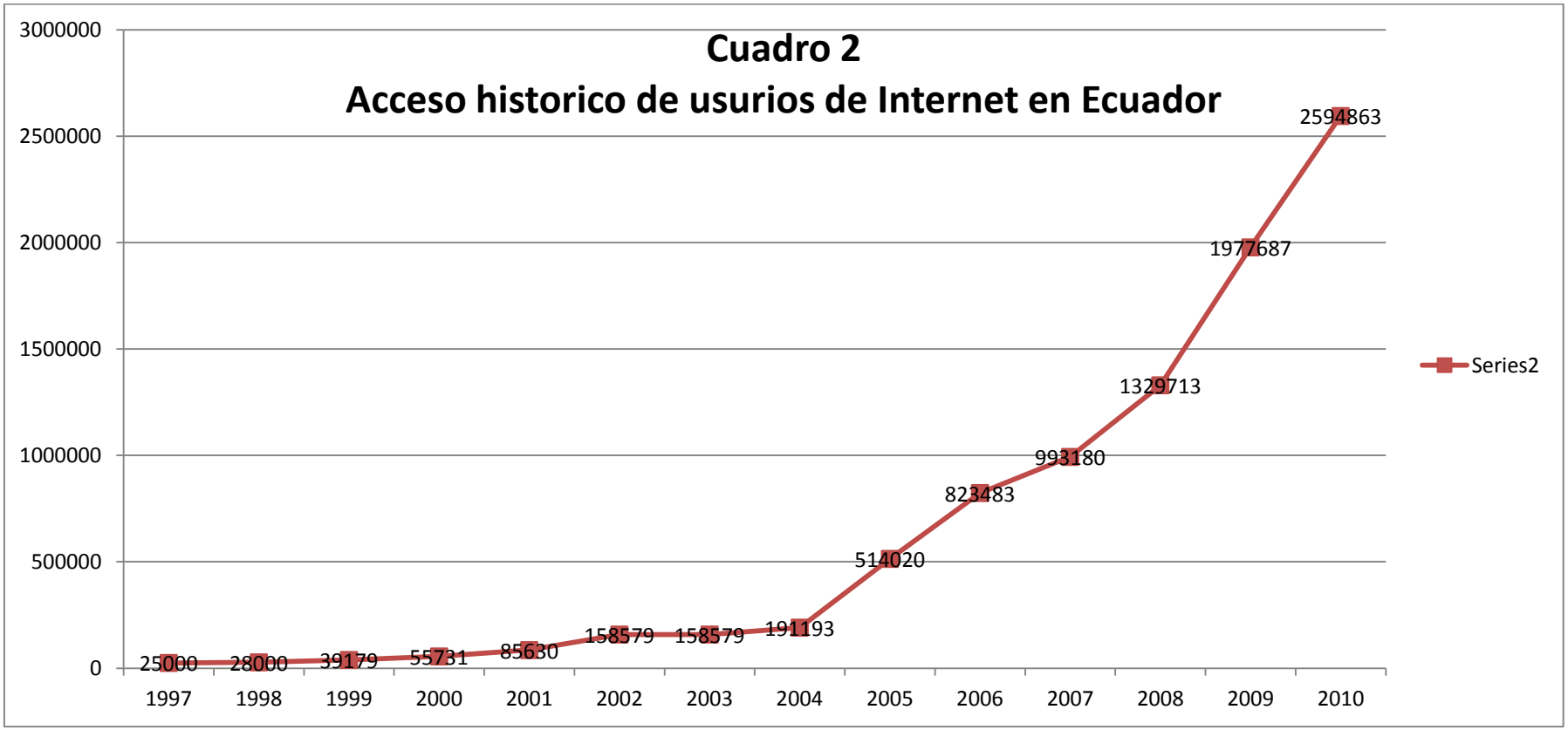
ANEXOS

Cuadro 1 Uso de Internet y Población en Sudamérica						
PAÍS	Población (est.2011)	% Población (Sudamericana)	Población en acceso	% de Población en acceso	Crecimiento (2000-2011)	% usuarios en Sudamérica
Argentina	41 769 726	10,4%	27 568 000	66,0%	1 003%	16,9%
Bolivia	10 118 683	2,5%	1 102 500	10,9%	819%	0,7%
Brasil	203 429 773	50,8%	75 982 000	37,4%	1 419%	46,7%
Chile	16 888 760	4,2%	9 254 423	54,4%	426%	5,7%
Colombia	44 725 543	11,2%	22 538 000	50,4%	2 467%	13,8%
Ecuador	**14 007 343**	**3,8%**	**3 352 000**	**29,5%**	**1 762%**	**2,1%**
Guyana Francesa	235 690	0,1%	58 000	24,6%	2 800%	0,0%
Guyana	744 768	0,2%	220 000	29,5%	7 233%	0,1%
Paraguay	6 459 058	1,6%	1 104 700	17,1%	5 423%	0,7%
Perú	29 248 943	7,3%	9 157 800	31,3%	266%	5,6%
Surinam	491 989	0,1%	163 000	33,1%	1 293%	0,1%
Uruguay	3 308 535	0,8%	1 855 000	56,1%	401%	1,1%
Venezuela	27 635 743	6,9%	10 421 557	37,7%	997%	6,4%
Total Sudamérica	**400 067 694**	**100%**	**162 779 880**	**40,7%**	**1,039%**	**100%**

Fuente: Internet World stats

CUADRO 2

Años	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Usuarios	25000	28000	39179	55731	85630	158579	158579	191193	514020	823483	993180	1329713	1977687	2594863



Fuente: Elaboración personal con datos de la Superintendencia

CUADRO 3

	Obtener Información			Comunicación en General			Comprar / ordenar productos o servicios		
	2008	2009	2010	2008	2009	2010	2008	2009	2010
Quintil 1	18,9%	19,2%	13,3%	14,2%	14,2%	16,6%	0,2%	0,2%	0,2%
Quintil 2	23,0%	21,2%	17,7%	17,4%	19,4%	18,0%	0,4%	0,2%	0,7%
Quintil 3	19,6%	26,2%	18,2%	19,3%	16,5%	24,6%	0,5%	0,3%	0,5%
Quintil 4	20,9%	31,0%	27,4%	28,4%	19,0%	25,4%	0,5%	0,7%	0,2%
Quintil 5	27,1%	34,3%	36,9%	25,8%	20,7%	22,5%	1,2%	0,6%	0,6%

	Banca Electrónica y otros Servicios Financieros			Educación y Aprendizaje			Transacciones con Organismos Gubernamentales		
	2008	2009	2010	2008	2009	2010	2008	2009	2010
Quintil 1	0,4%	1,7%	0,7%	62,0%	61,6%	66,1%	0,0%	0,2%	0,0%
Quintil 2	1,7%	0,1%	0,4%	52,8%	51,6%	56,8%	0,3%	0,1%	0,7%
Quintil 3	0,5%	0,9%	1,1%	51,4%	48,8%	49,2%	0,3%	0,2%	0,3%
Quintil 4	1,1%	0,9%	0,9%	40,0%	38,8%	38,0%	0,4%	0,2%	0,5%
Quintil 5	1,7%	1,4%	1,5%	29,9%	28,3%	26,4%	0,4%	0,5%	0,6%

	Actividades de Entretenimiento			Obtener películas, música o software			Leer / Descargar Libros Electrónicos		
	2008	2009	2010	2008	2009	2010	2008	2009	2010
Quintil 1	1,8%	1,1%	1,1%	0,9%	0,2%	0,6%	0,1%	0,3%	0,3%
Quintil 2	0,7%	2,2%	1,8%	1,0%	1,1%	0,7%	0,7%	0,5%	0,5%
Quintil 3	1,6%	2,1%	1,7%	1,0%	0,7%	1,3%	1,1%	0,4%	0,4%
Quintil 4	1,3%	1,1%	1,3%	1,0%	0,8%	0,8%	0,7%	0,5%	1,0%
Quintil 5	1,1%	0,9%	1,2%	0,5%	0,6%	0,5%	0,9%	0,9%	0,7%

	Por razones de trabajo			Otro, Cual		
	2008	2009	2010	2008	2009	2010
Quintil 1	1,5%	1,2%	0,9%	0,0%	0,0%	0,1%
Quintil 2	1,9%	3,3%	2,2%	0,1%	0,3%	0,4%
Quintil 3	4,6%	4,1%	2,4%	0,1%	0,0%	0,4%
Quintil 4	5,6%	6,8%	4,6%	0,2%	0,2%	0,1%
Quintil 5	11,3%	11,7%	9,0%	0,1%	0,1%	0,2%

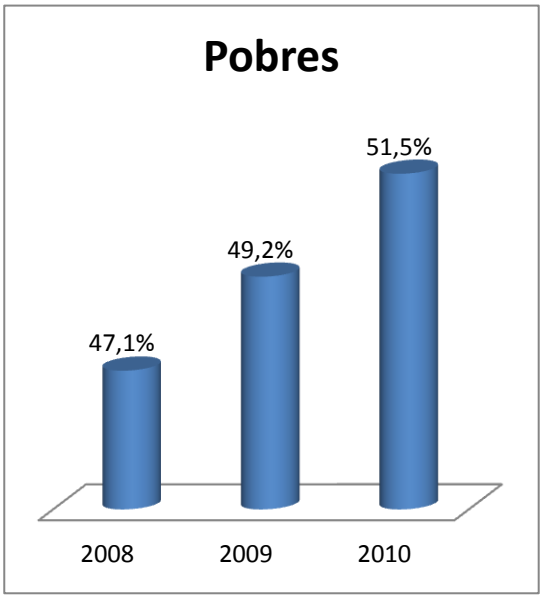
Fuente: INEC, Censo de Población 2010

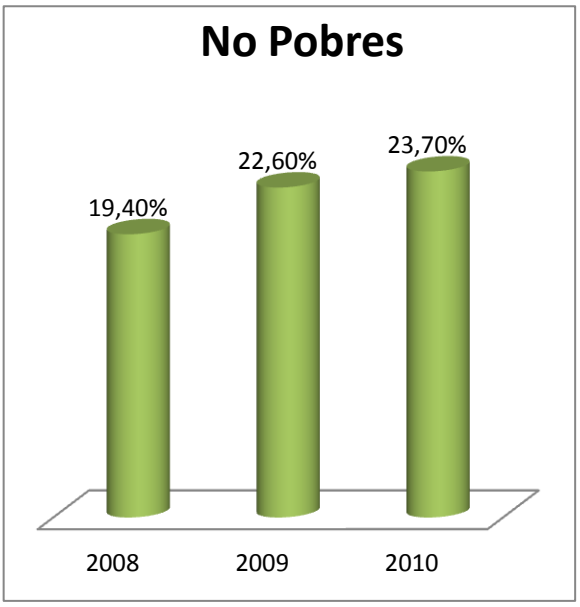
CUADRO 4

Tenencia de celular y uso de Internet

Pobres y no Pobres con celular

	Pobres	No Pobres
2008	47,1%	19,40%
2009	49,2%	22,60%
2010	51,5%	23,70%

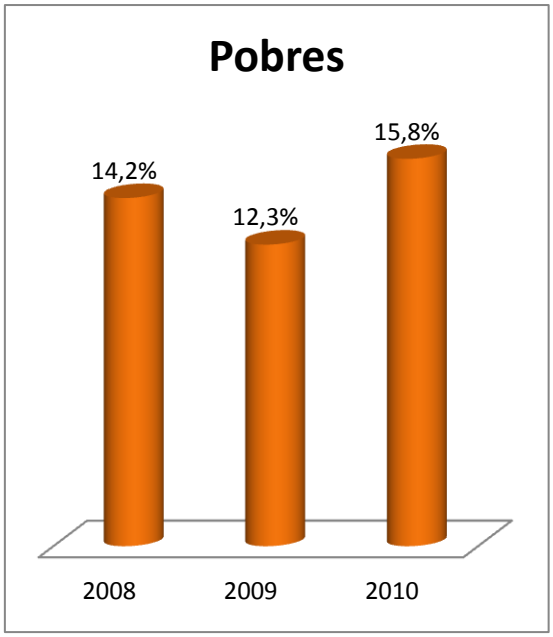


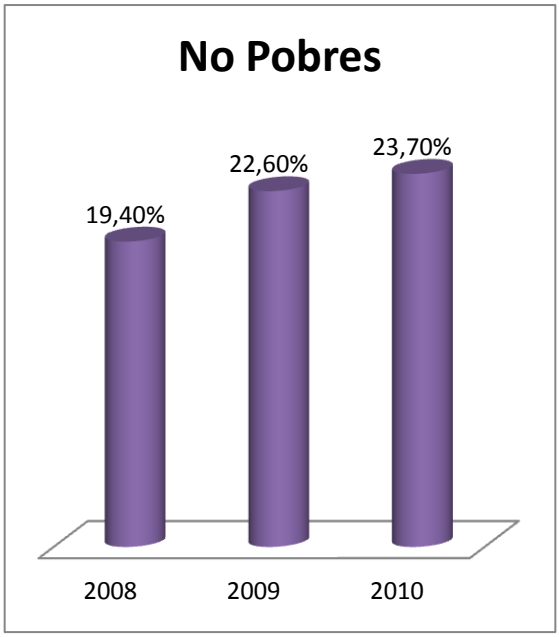


Fuente: NEC, Censo de Población 2010

Pobres y no pobres que usan internet

	Pobres	No Pobres
2008	14,2%	19,40%
2009	12,3%	22,60%
2010	15,8%	23,70%



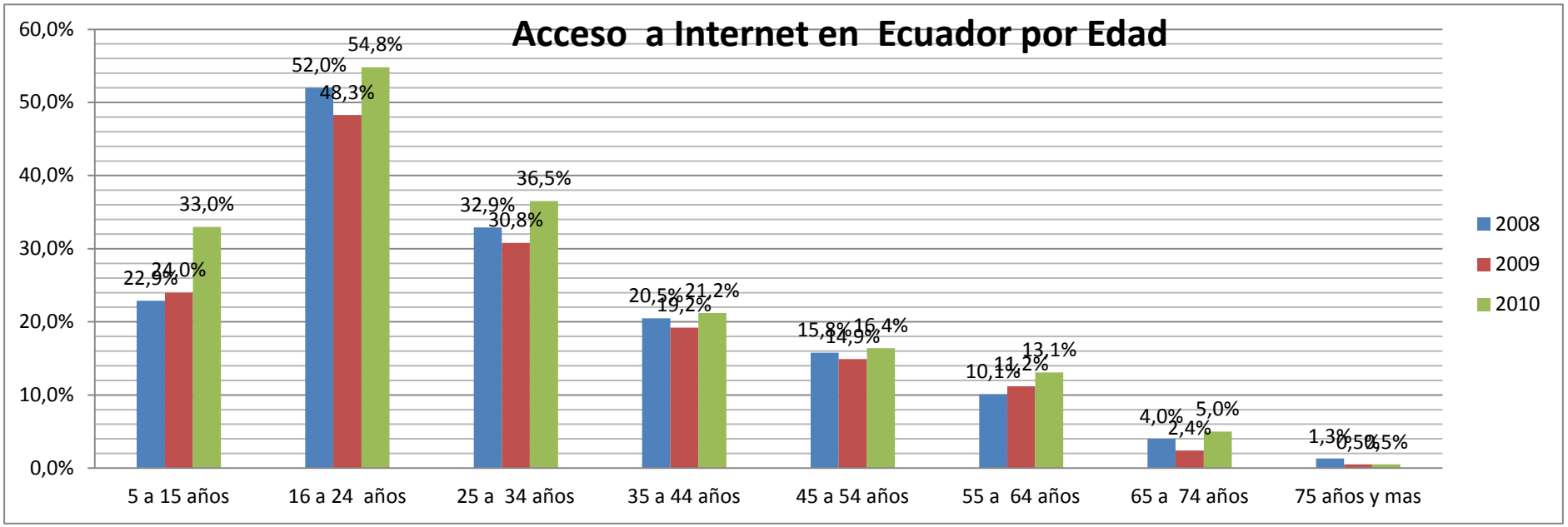


Fuente: INEC, Censo de Población 2010

CUADRO 5

Acceso a Internet en Ecuador por Edad

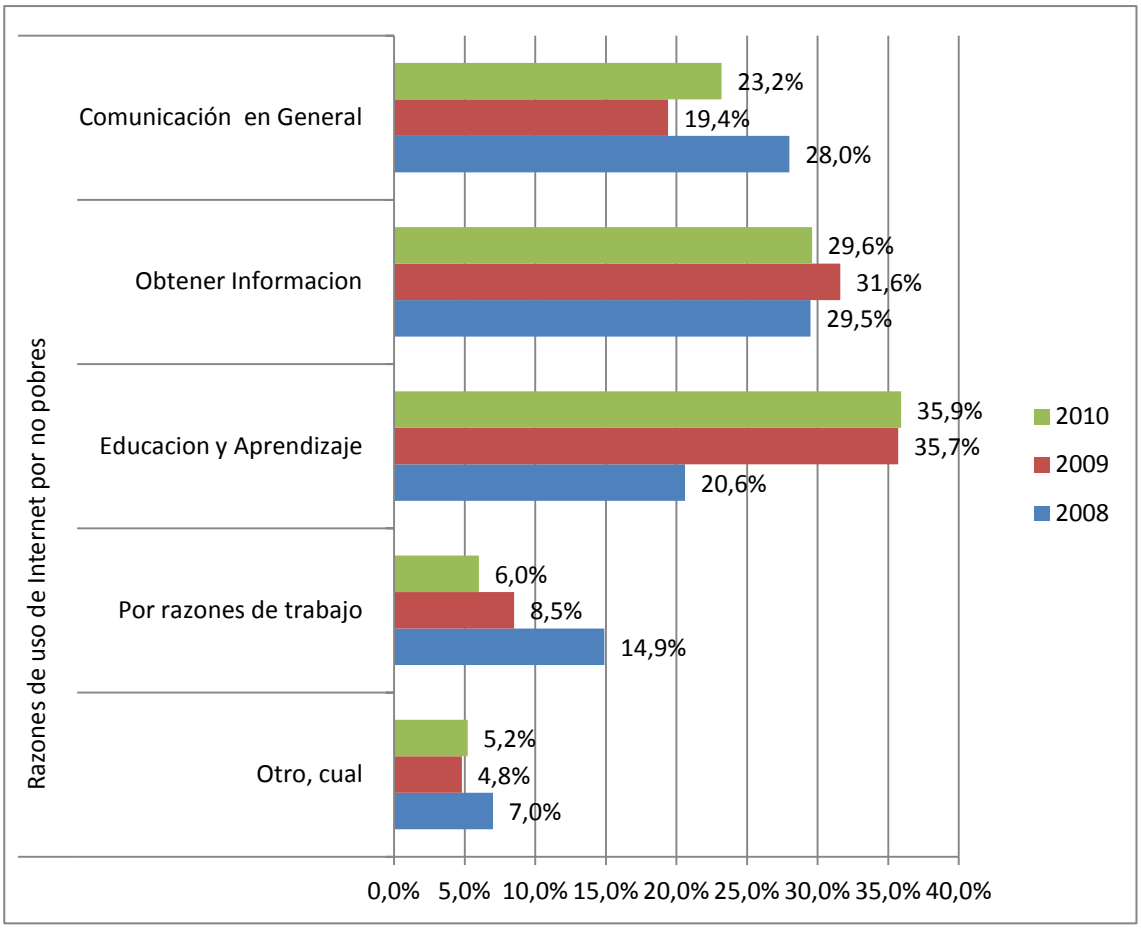
	5 a 15 años	16 a 24 años	25 a 34 años	35 a 44 años	45 a 54 años	55 a 64 años	65 a 74 años	75 años y mas
2008	22,9%	52,0%	32,9%	20,5%	15,8%	10,1%	4,0%	1,3%
2009	24,0%	48,3%	30,8%	19,2%	14,9%	11,2%	2,4%	0,5%
2010	33,0%	54,8%	36,5%	21,2%	16,4%	13,1%	5,0%	0,5%



Fuente: INEC, Censo de Población 2010

Cuadro 6
Razones de uso de Internet

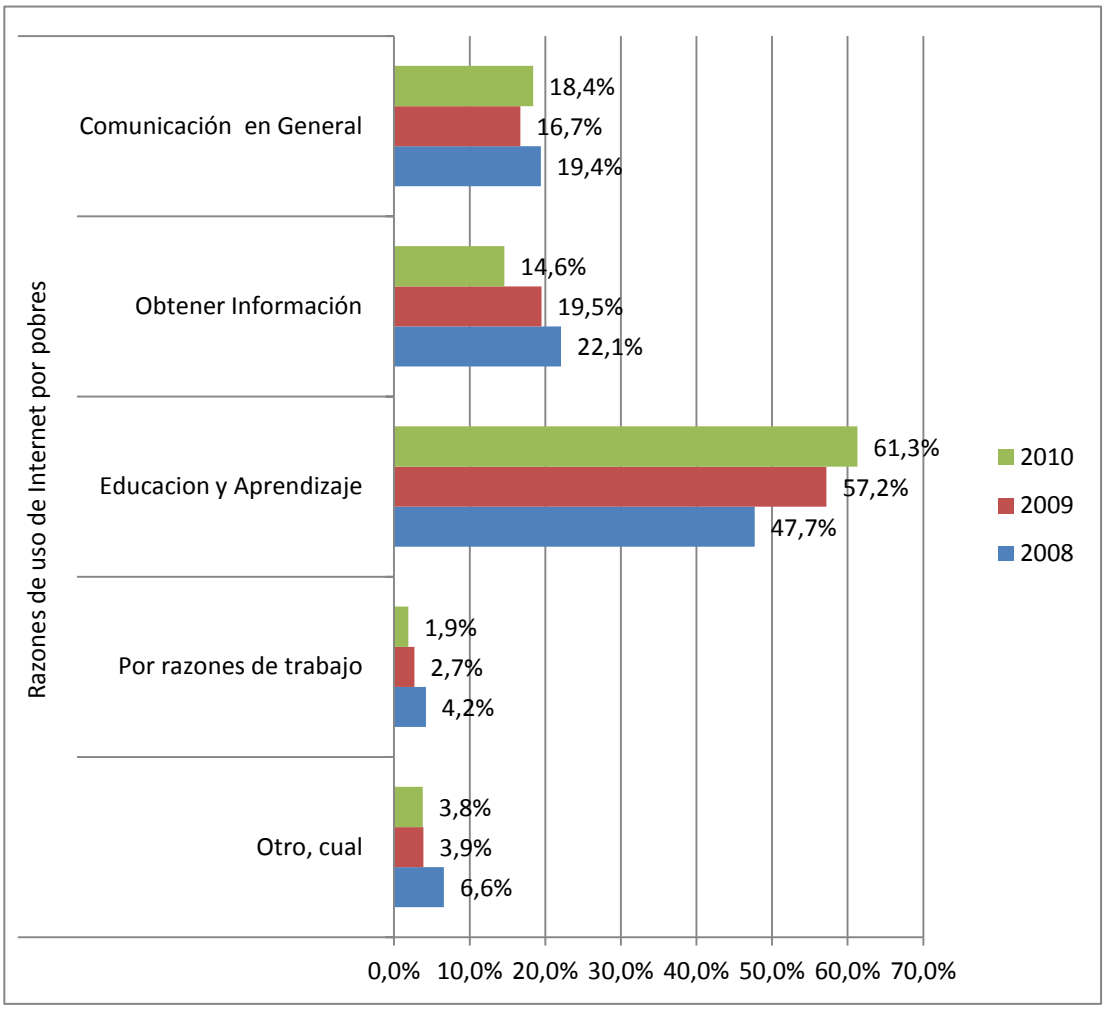
Razones de uso de Internet por no pobres					
	Otro, cual	**Por razones de trabajo**	**Educación y Aprendizaje**	**Obtener Información**	**Comunicación en General**
2008	7,0%	14,9%	20,6%	29,5%	28,0%
2009	4,8%	8,5%	35,7%	31,6%	19,4%
2010	5,2%	6,0%	35,9%	29,6%	23,2%



Fuente: INEC, Censo de Población 2010

Razones de uso de Internet por pobres

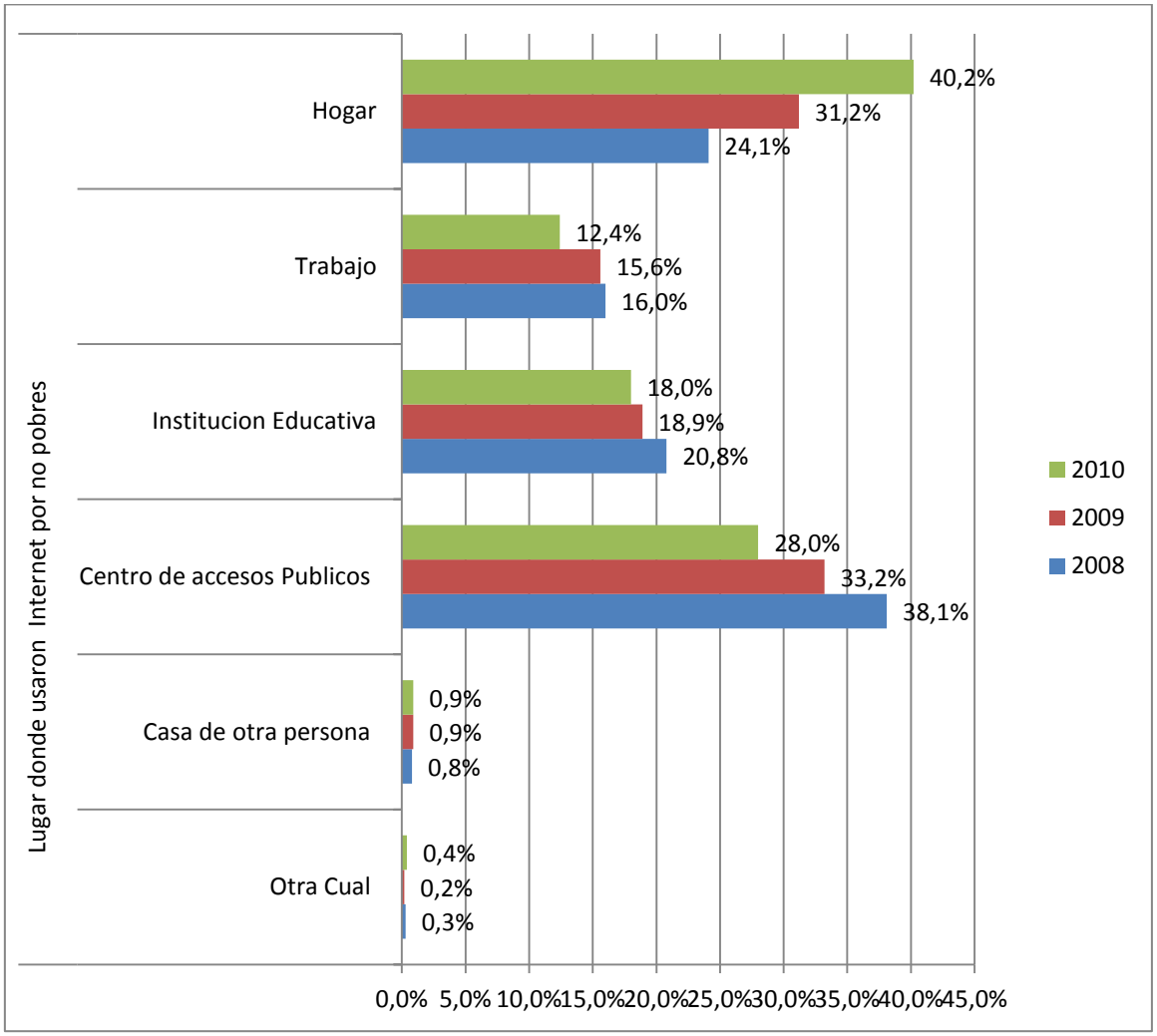
	Otro, cual	Por razones de trabajo	Educación y Aprendizaje	Obtener Información	Comunicación en General
2008	6,6%	4,2%	47,7%	22,1%	19,4%
2009	3,9%	2,7%	57,2%	19,5%	16,7%
2010	3,8%	1,9%	61,3%	14,6%	18,4%



Fuente: INEC, Censo de Población 2010

CUADRO 7
Acceso a Internet en Ecuador por lugar

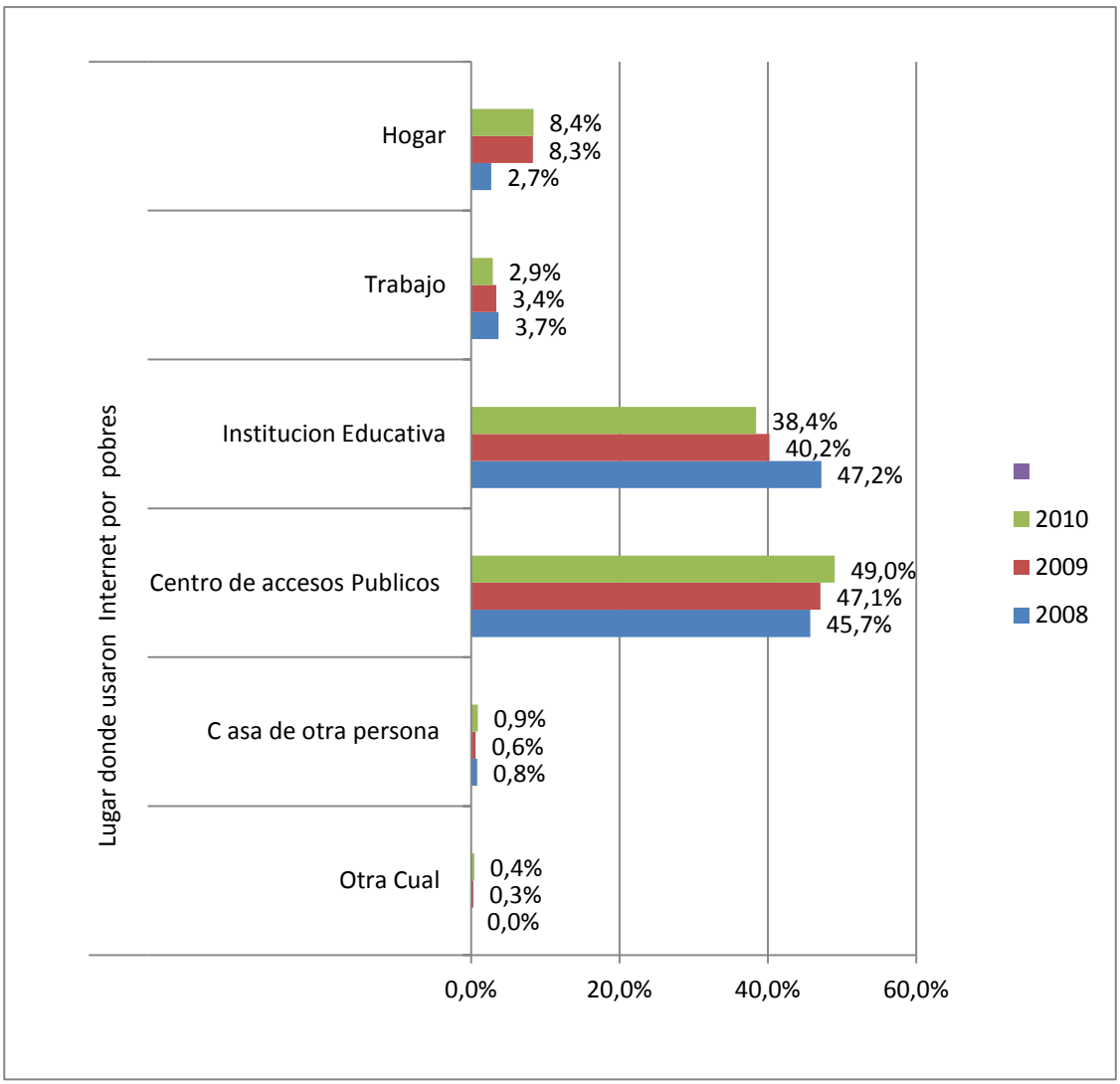
Lugar donde usaron Internet por no pobres						
	Otra Cual	**Casa de otra persona**	**Centro de accesos Públicos**	**Institución Educativa**	**Trabajo**	**Hogar**
2008	0,3%	0,8%	38,1%	20,8%	16,0%	24,1%
2009	0,2%	0,9%	33,2%	18,9%	15,6%	31,2%
2010	0,4%	0,9%	28,0%	18,0%	12,4%	40,2%



Fuente: INEC, Censo de Población 2010

Lugar donde usaron Internet por pobres

	Otra Cual	C asa de otra persona	Centro de accesos Públicos	Institución Educativa	Trabajo	Hogar
2008	0,0%	0,8%	45,7%	47,2%	3,7%	2,7%
2009	0,3%	0,6%	47,1%	40,2%	3,4%	8,3%
2010	0,4%	0,9%	49,0%	38,4%	2,9%	8,4%



Fuente: INEC, Censo de Población 2010