EL ANALFABETISMO DIGITAL Y LA SEGURIDAD INFORMATICA EN EL ECUADOR

Autor: MSc. Ing. Com. Bolivar Espinoza Santos

Ing. Com. Bolivar Espinoza Santos, Magíster en Educación Superior por la Universidad de Guayaquil.

Ingeniero Comercial Catedrático de la Universidad de Guayaquil.

bolivar.espinozas@ug.edu.ec

bol_espinoza@hotmail.com

Autor: MSc. Arq. Fernando Terán Viteri

Arq. Luis Fernando Terán Viteri, Magíster en Educación Superior por la Universidad de Guayaquil.

Arquitecto-Urbanista por la Universidad de Guayaquil.

Catedrático de la Universidad de Guayaquil.

luis.teranv@ug.edu.ec

teranluis58@gmail.com

RESUMEN:
Este artículo trata del nivel de seguridad informática existente en el Ecuador en la última década (2005-2015). El campo de interés está enmarcado en la seguridad que debe existir en el plano informático en relación a los individuos que acceden mediante el internet con diferentes medios tecnológicos. Este estudio se base en experiencias de casos ocurridos o situaciones las cuales se presentan diariamente, donde se ha podido evidenciar que los perjuicios han ocasionado pérdidas económicas significativas a personas e instituciones en general por parte de los delincuentes cibernéticos que incurren en estafas, violaciones a la integridad individual y colectiva, al robo electrónico, los cuales se cometen al acceder sin previa autorización a cuentas y bases de datos privados, aspecto donde la legislación ecuatoriana no ofrece garantías y tipificaciones correspondientes para sentenciar a los culpables y se concluye que en el país se remarca la correlación existente entre el analfabetismo digital y el delito informático.
Palabras Claves:

Internet Tecnología Seguridad Informática Delitos informáticos Analfabetismo digital

ABSTRACT

This article is the level of computer security in the Ecuador in the last decade (2005-2015). The field of interest is framed in the security that should exist in the flat computer in relation to individuals who gain access through the internet with different technological means. This study is based on experiences of cases or situations that occur daily, where it is has been able to demonstrate that the damages have resulted in significant economic losses to individuals and institutions in general by cyber criminals that are scams, individually and collectively, to electronic theft integrity violations, which are committed to access without authorization to private accounts and databases, look where Ecuadorian legislation does not offer guarantees and corresponding typifications to convict the

guilty parties and it is concluded that the country is stressed the correlation between digital illiteracy and cybercrime.

Key words:

Internet Technology Computer Security Cybercrime Digital Illiteracy

TABLA DE CONTENIDOS
INDICE DE FIGURAS

1. INTRODUCCION.

La seguridad Informática se ha convertido en un problema cada vez más creciente dentro de la sociedad ecuatoriana, desde hace algún tiempo, las instituciones y personas en general han sufrido pérdidas económicas por esta causa, sus bases de datos son el objetivo clave de los delincuentes cibernéticos, siendo muchos los que se han visto seriamente perjudicados; la gran mayoría de las amenazas se dan por internet, ya que este es el medio donde se puede acceder directamente a la información, esto conlleva a que ésta sea alterada, sustraída o utilizada para delitos.

Existen diferentes maneras de proteger la información por parte del usuario, pero también nacen nuevas formas por parte de los delincuentes informáticos para violar las seguridades del internet, y así lograr sus delitos.

1.1. Internet

Internet es una red que permite la interconexión de ordenadores mediante un conjunto de protocolos llamados TCP/IP. Sus inicios fueron en 1969, cuando una agencia del Departamento de Defensa de los Estados Unidos empezó la búsqueda de opciones ante una eventual guerra atómica que pudiera incomunicar a los seres humanos. La primera exposición oficial de aquel sistema, fue por el año 1972 ya que las universidades del estado de California lograron establecer la primera conexión conocida como ARPANET (Advanced Research Projects Agency Network).

1.2. Tecnología

La tecnología es la aplicación coordinada de un conjunto de conocimientos y habilidades con el fin de crear una solución que permita al individuo satisfacer necesidades.

Con la tecnología se pone en desarrollo un conjunto de conocimientos de orden práctico y científico que, relacionados bajo una serie de procedimientos y métodos de firmeza técnica contribuyen a solucionar problemas de orden técnico.

1.3. Seguridad Informática

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Los expertos informáticos indican que no existe un sistema 100% seguro, lo que si podemos mencionar es ciertas características que reduzca los riesgos y donde solo los usuarios autorizados ingresen y modifiquen la información, como son: la confidencialidad, Integridad, disponibilidad e irrefutabilidad.

Además la seguridad se compone de tres partes dependiendo de las fuentes de amenazas las cuales son: Seguridad lógica, Seguridad física y Seguridad ambiental.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de Internet, para no permitir que su información sea comprometida.

1.4. **Delitos informáticos**[1]

Para definir al delito informático tomamos como referencia a la ONU ya que es el organismo más idóneo, así se define al tema como los "fraudes cometidos mediante manipulación de computadoras", pero también tiene catalogados a otras acciones denominadas como delitos, entre ellos están:

Manipulación de datos de entrada: que es la acción de sustraer información ajena, convirtiéndose en el delito más expandido y amparado por la impunidad del realizador que además no requiere de mayores conocimientos técnicos para realizar su objetivo.

Manipulación de Software: esta acción delictiva si requiere conocimientos técnicos para realizarla, y se trata de alterar los datos originales del software colocando nuevos comandos orientados para adquirir fraudulentamente información ajena.

Caballo de Troya: que como su nombre lo indica acciona internamente desde la computadora ciertas instrucciones fraudulentas aparte de las suyas actuando con cierta normalidad sin que el propietario se dé cuenta del delito.

Manipulación de datos de salida: se basa en alterar la información de los chips inteligentes y las bandas de las tarjetas de crédito, que, al alterar el funcionamiento normal de los cajeros hace que su ejecutante reciba dinero que no le corresponde.

Manipulación Informática: es el fraude que permite introducirse en información bancaria e ir sacando dinero sistemáticamente hacia otra cuenta de forma casi imperceptible por parte del propietario.

Sabotaje Informático: es el acto más común de alterar el funcionamiento normal de un ordenador, entre sus métodos están los virus, gusanos, troyanos y demás elementos ajenos que el propietario ajeno a su existencia luego padece de sus indeseados resultados.

1.5. **Analfabetismo digital**[2]

---

1 **Disponible**: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

2 **Disponible**: http://www.foroconsultivo.org.mx/innovacion.gaceta/los-pi-q-2/436-brecha-y-analfabetismo-digitales-

Es la falta de conocimiento que tienen los individuos al momento de manejar las tecnologías actuales, este asunto evita que ellos puedan tener la habilidad necesaria para extraer todas las ventajas que ofrece el mundo digital que en la actualidad abarcan casi todos los conocimientos del ser humano, el desconocimiento se puede medir en varios niveles:

Manejo básico de las CPU, laptops, smartphones y sus accesorios.

Manejo del software básico para poder sacar ventaja dentro de los medios de hardware, lo cual implica ofimática y e-mail.

Manejo del diferente software en especial los de uso libre que representan ventajas frente a los pagados en especial por la captación de virus.

La idea general es que todo individuo aprenda a relacionarse digitalmente con los otros y así sacarle ventaja a las tecnologías que a diario aparecen mediante las aplicaciones actuales.

Antecedentes.

El analfabetismo informático ha sido una de las primeras razones por la cual se aprovechan los delincuentes para el cometimiento de los delitos, esto se da por la falta de una cultura digital preventiva que obstaculice a los sujetos que intenten ingresar por medio del internet a realizar daños a la información personal o privada.

Las autoridades Ecuatorianas ya han registrado 3.143 casos, de los cuales existe un subregistro que no es reportado por los perjudicados. En este país las cifras de los delitos que no son registrados asciende al 80%, esto posesiona al Ecuador en el tercer lugar seguido de México y Bolivia con el 92% y 85% respectivamente.

Las pérdidas que sufren los individuos o las instituciones privadas o públicas son en muchos de los casos en grandes escalas, donde la mayoría de los usuarios son sorprendidos sin darse cuenta por los delincuentes informáticos ya que las personas suelen navegar sin prevención.

Es frecuente que ciertos sitios webs se muestran como seguros solicitando información en forma de anuncios o banners, es así, que se aprovechan de las personas violentando su correspondencia, realizando fraudes bancarios conocidos como estafas de tipo electrónico por medio del internet y alterando o destruyendo la información.

Otra de las causas que originan los delitos informáticos son la falta de capacitación de los usuarios que usan el internet, dejando expuestas muchas ventajas aprovechas para que los delincuentes puedan cometer diversas fechorías informáticas.

Es de relevante observar que el tema de este artículo se hace hincapié sobre la variable independiente como es la seguridad informática y la variable dependiente que es el analfabetismo digital, la cual es la causa de muchos delitos informáticos que ocurren en el Ecuador.

2. CONTENIDO

2.1. Importancia de la Seguridad Informática.

La importancia de tener una cultura informática en los actuales momentos es vital ya que con una correcta disciplina permitirá al usuario mediante técnicas y diversas herramientas de seguridad proteger oportunamente la información.

Uno de los objetivos principales que tiene la Seguridad Informática es brindar una garantía y privacidad a la información del usuario.

2.2. **Particularidades de la Seguridad Informática**

Como principales particularidades de la Seguridad Informática podemos contar en primer lugar con la reserva y sigilo en el almacenamiento de los datos en especial cuando son de índole económico, y como segundo aspecto importante se menciona a la ética al entregar un servicio confiable lo cual representa para el usuario la preservación y consistencia de los datos entregados.

Para una mejor comprensión se detallan a continuación en diferentes cuadros, los tipos, amenazas y software utilizados en la seguridad informática:

Tabla : Tipos de Seguridades Informática

• SEGURIDAD INFORMÁTICA •		
Hardware	**Redes**	**Lógica**
Que son todos los elementos físicos de las computadoras (mouse, monitor, teclado, impresora, scanner.), incluyendo su mala manipulación y el sitio donde los equipos son instalados.	Son los elementos de conectividad que relacionan a una serie específica de computadoras e implica todo medio de seguridad entre ellas.	Son los elementos que hacen activar a los aparatos conectados a una computadora o a una red de comunicación siendo el usuario el responsable de su mejor manipulación.

Fuente: autores

Tabla : Las amenazas de la Seguridad Informática

LAS AMENAZAS MAS DESCUIDADAS SON:	
“Shoulder surfing”	Espiar cerca y discretamente la inserción de clave de un usuario sin su consentimiento.
Observación	Espiar de lejos y por diferentes medio (larga vistas) la inserción de claves de un usuario sin su consentimiento, también aplica para saber el movimiento cotidiano de todo el ambiente físico que rodea al lugar que se desea atacar.
“Eavesdropping”	Es el uso de técnicas que se emplean para sacar información básica de usuarios importantes (gerentes, managers) en especial con amplificadores de audio u otros medios afines.
“Dumpster diving”	No siempre la basura se debe desechar tan fácilmente, en ella de seguro hay información valiosa que el delincuente sabe detectar en los papeles, papel carbón, computadoras desechadas y todo elemento usado en oficinas donde se tramita información valiosa.

Dispositivos móviles perdidos	La información contenida en tabletas, iPads, Smartphone y otros gadgets portátiles si es sustraída e interpretada por manos inescrupulosas es otro delito que se usa en contra del propietario
Prensa	Muchas veces la instauración de nuevos equipos o software instalados en compañías o instituciones puede ser arma de doble filo ya que el delincuente con la instrucción necesaria se entera por medios de prensa y puede usar esa información para realizar sus delitos.
Foros online:	La ingenuidad y la poca experiencia puede jugar una mala pasada a los usuarios que en grupos y foros de discusión en Internet exponen todas las características de sus sistemas y por querer subsanar un daño presentado exponen toda su información (incluyendo # de IP) a cualquier persona que maliciosamente puede usar esos datos técnicos básicos para realizar delitos informáticos.
Sitios Web	El motor de búsqueda puede ser utilizado para acceder a la información y se ha convertido en uno de los métodos más utilizados para penetrar a la información personal, mediante el navegador. Esto se da por las constantes mejoras que presentan los navegadores y conllevan al usuario inexperto a ser víctimas del espionaje.
Herramientas en línea	La imaginación y tecnicidad del ciber-delincuente no tiene límites, en este caso el empleo de programas en línea pueden ser usados para capturar información importante del usuario.
Ingeniería social	La ingenuidad y el morbo del usuario también es un elemento que se puede usar como carnada para que al momento de acceder en busca de la promoción ofrecida, sean incrustados en sus equipos programas adicionales que sirven también para manipularlas y extraer información valiosa.

Disponible en: http://www.diginota.com/las-10-amenazas-a-la-seguridad-informatica-mas-descuidadas/

Tabla : Software utilizados para la Seguridad Informática

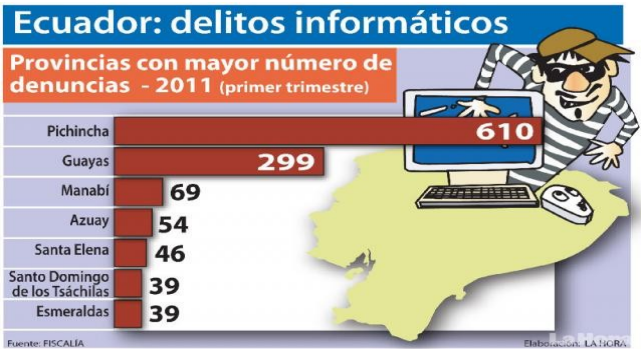
ANTIVIRUS:	ANTISPYWARES:	FIREWALLS
Programas primordiales que protegen los ordenadores contra los virus informáticos	Programas que han sido creados para combatir el espionaje delincuencial, dentro de ellos están:	Protegen el ordenador contra todas las conexiones dañinas.
• Antivirus NOD32 • Avira AntiVir Kaspersky Anti-Virus • Avast! Home • AVG Antivirus	• Spyware Terminator • SpyBot Search & Destroy • Ad-Aware SE Personal	• ZoneAlarm • McAfee Personal Firewall

Fuente: http://www.bloginformatico.com/seguridad-informatica-principios-basicos-y-software.php

2.3. **Delitos informáticos por provincias**

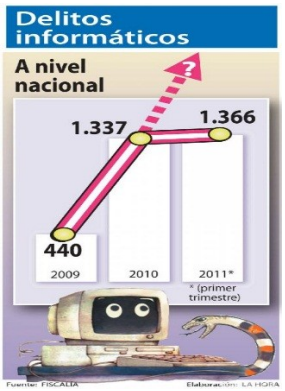
Según las denuncias reportadas de manera oficial ante la Fiscalía, en el Ecuador año 2011, las provincias con mayor incidencias de delitos informáticos, fueron Pichincha y Guayas, siendo la primera que ventaja en forma significativa al resto de provincias por el número mayor de usuarios que esta tiene.

Figura : Delitos Informáticos



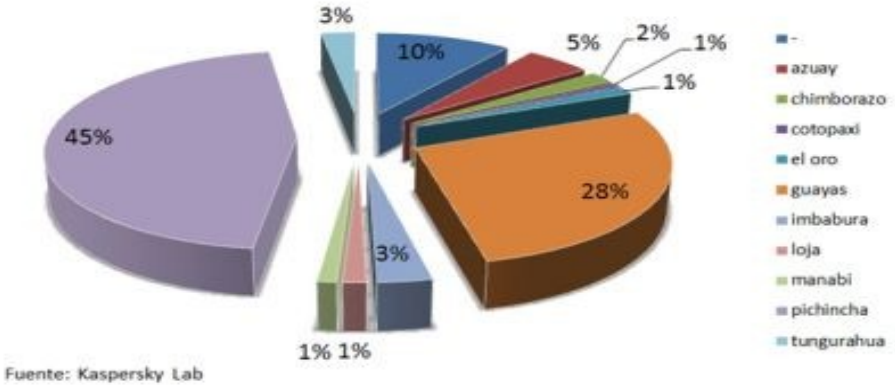
Fuente: http://www.lahora.com.ec/index.php/noticias/show/1101191943/-1/Se_disparan_los_delitos_inform%C3%A1ticos_.html#.VPX_pouG8YE

Figura : Incremento de los delitos informáticos en el Ecuador



Fuente: http://www.lahora.com.ec/index.php/noticias/show/1101191943/-1/Se_disparan_los_delitos_inform%C3%A1ticos_.html#.VPX_pouG8YE

Gráfico : Provincias con mayor infección en máquinas de los usuarios, año 2011



Fuente: http://www.canal-tecnologico.com/index.php?option=com_content&view=article&id=622:robar-lo-que-sea-y-a-quien-sea-delitos-informaticos-en-el-ecuador&catid=25:soft&Itemid=54

2.4. **Estadísticas del Analfabetismo Digital en Ecuador.**[3]

En el 2013, el 20% de las personas en el Ecuador son analfabetas digitales, lo que representa un 9.2 menos que en el 2010.

Para elaborar el cuadro estadístico se ha considerado como Analfabeta Digital a la persona que cumple simultáneamente estas tres características como son:

3 http://www.ecuadorencifras.gob.ec/12-millones-de-ecuatorianos-tienen-un-telefono-inteligente-smartphone/

a) No tener celular activado.
b) No haber tenido acceso a una computadora en los últimos 12 meses.
c) No haber tenido acceso al internet en los últimos 12 meses.

Gráfico : Analfabetos digitales

Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2010-2013)

2.4.1. **El 20% de los ecuatorianos es analfabeto digital.**[4]

El conocimiento básico de lectura y escritura dejó de ser lo más elemental en conocimientos que debe tener una persona, en la actualidad es una prioridad que los habitantes del Ecuador se instruyan y adapten con los términos digitales a tal punto que ese saber esté a la par de la educación básica que se imparte normalmente.

En el año 2013 el INEC decidió hacer una encuesta al respecto, el resultado fue que el 20% de la población tenía desconocimiento absoluto de términos computacionales, de ese porcentaje una leve diferencia le daba mayoría a las mujeres en cuanto al analfabetismo digital, también la variable edad influía de manera significativa ya que de los mayores de 55 años solo el 19% había usado la computadora.

Las academias de computación son las encargadas de brindar ese conocimiento, lo mismo que algunos municipios como el de Guayaquil: http://guayaquil.gov.ec/content/centros-municipales-multimedia-iniciaron-cursos-de-capacitaci%C3%B3n-

En el resto del país existen muchos centros de educación digital como el centro de desarrollo comunitario de Tumbaco cerca de Quito, incluso algunos son totalmente gratuitos como los infocentros del gobierno que según el ministerio de comunicaciones existen 489 sitios en todo el país los cuales han permitido disminuir el analfabetismo digital, en especial a nivel rural donde se cubre un 78% de esa región. Pero de ese conocimiento no se sabe si el nivel es básico o avanzado lo que hace dudoso dar un resultado certero de ese tema.

Lamentablemente debe existir la voluntad, la necesidad e iniciativa de la persona para que comience a estudiar y eso no se aplica en todos los casos a tal punto que muchos encargan esa labor a terceros y es ahí donde el riesgo se produce con mayor incidencia.

Adicional a este analfabetismo absoluto también existe el desconocimiento parcial, es decir una gran cantidad de personas tan solo saben manejar recursos de las redes sociales y tipiar, al saber poco, lógicamente surgen problemas al momento de accionar recursos que impliquen mayor experiencia, es que en la actualidad una gran mayoría de trámites que se realizan por internet.

2.5. **Equipamiento tecnológico y acceso al internet**

El 18,1% de los hogares tiene al menos un computador portátil, 9,1 puntos más que lo registrado en 2010. Mientras el 27,5% de los hogares tiene computadora de escritorio, 3,5 puntos más que en 2010.

---

4 Disponible:http://www.elcomercio.com.ec/tendencias/ecuatorianos-analfabeto-digital-cifras-tecnologia.html-

¿Tiene este HOGAR: televisión a color, Equipo de sonido, DVD-VHS, computadora de escritorio, Computadora portátil?

Según fuente GSMA, en Ecuador las conexiones a internet a través del celular crecerán en un 67% en el año 2020, esto se dará gracias a los teléfonos inteligentes, lo que significa que en ese año sus empleo se duplicará tomando en cuenta que en el 2014 era la mitad.

Hay que tomar en cuenta que Ecuador está en la posición intermedia con el 35% en el uso de celulares inteligentes, según la lista aportada por GSMA en un comunicado:

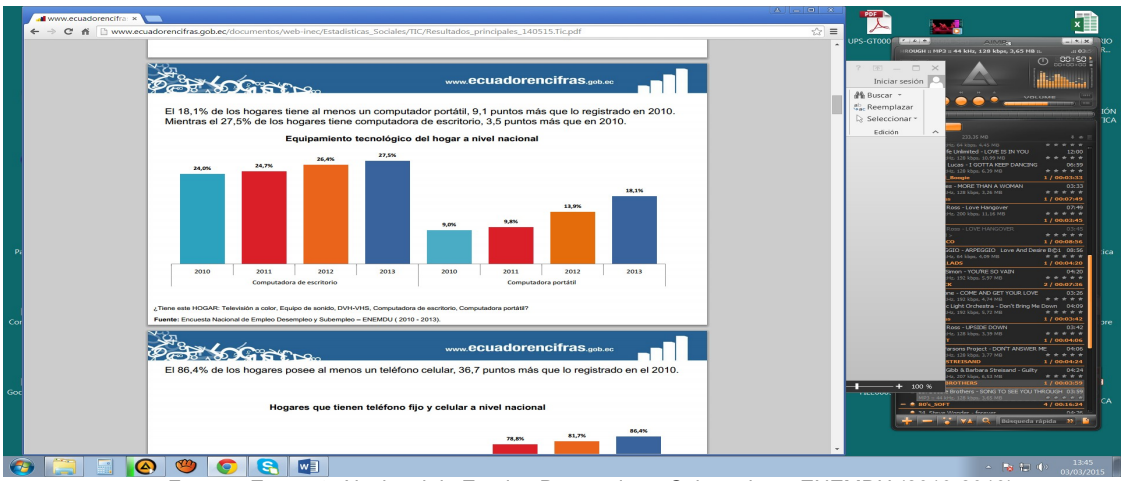
Tabla : Posición de Ecuador con el uso de celulares inteligentes

Conexiones mediante celulares inteligentes									
Venezuela	República Dominicana	Brasil	Chile	Ecuador	Argentina	Colombia	Guatemala	México	Perú
47%	39%	38%	36%	35%	34%	31%	25%	20%	19%

Fuente: GSMA Intelligence

En la actualidad, la tecnología móvil es uno de los modos mayormente utilizados para acceder al internet, empezando con la población latinoamericana, y especial en las áreas rurales. Esto se corrobora por el anuncio de la compañía GSMA que dice: "Las conexiones de banda ancha móvil superaron a las conexiones de banda ancha fija en América Latina durante 2011. Esto se da en toda la región, incluyendo los cinco mercados más grandes entre ellos Brasil donde hay cinco veces más conexiones de banda ancha móvil que de banda ancha fija". GSMA Intelligence (2014).

Gráfico : Equipamiento tecnológico a nivel nacional

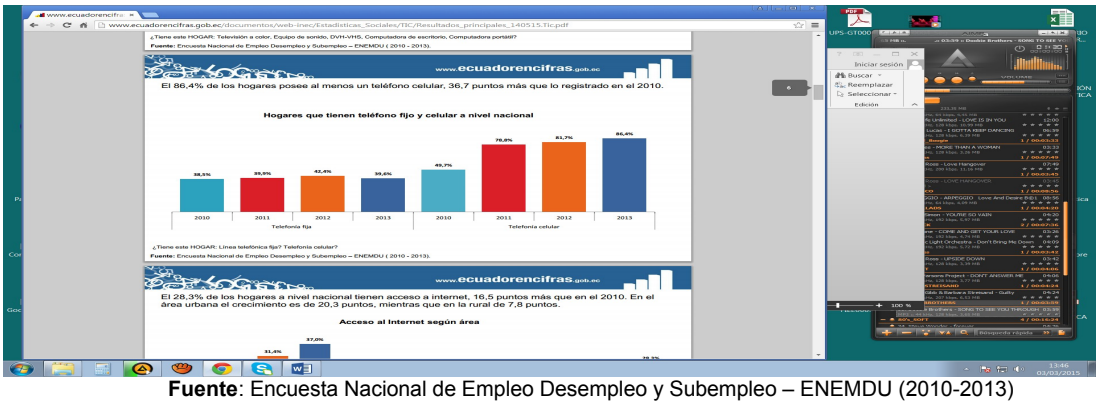


Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2010-2013)

El 86,4 % de los hogares posee al menos un teléfono celular, 36,7 puntos más que lo registrado en el 2010.

¿Tiene este HOGAR: Línea telefónica fija? Telefonía celular?

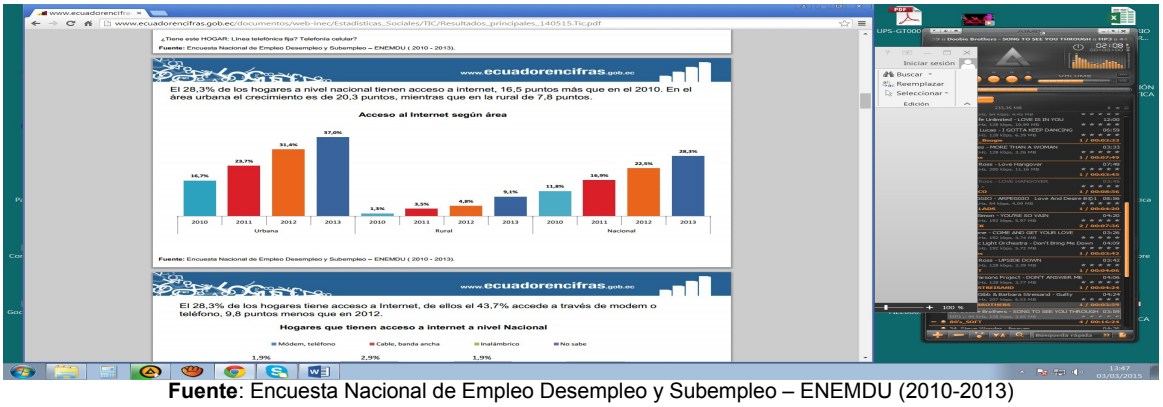
Gráfico : Hogares con teléfono fijo y celular



Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2010-2013)

El 28,3% de los hogares a nivel nacional tienen acceso a internet, 16,5 puntos más que en el 2010. El área urbana el crecimiento es de 20,3 puntos, mientras que en la rural de 7,8 puntos.

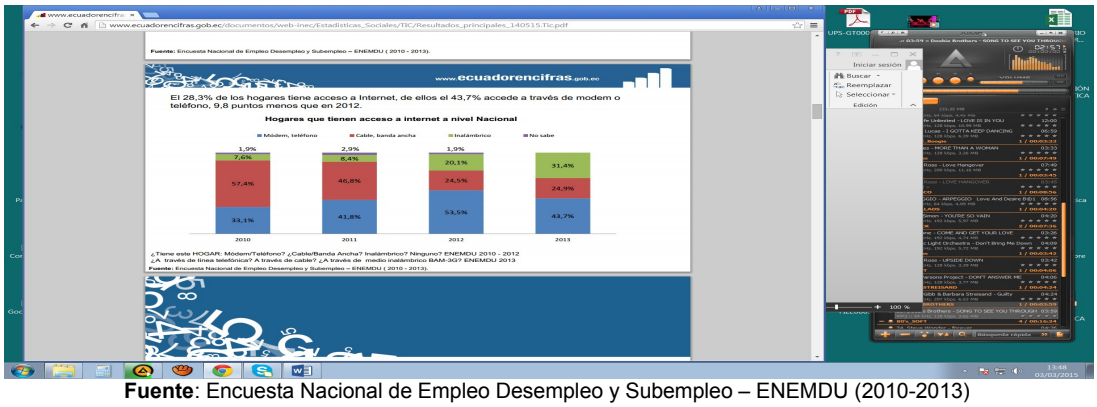
Gráfico : Acceso del internet.



Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2010-2013)

El 28,3% de los hogares tiene acceso a internet, de ellos el 43,7% accede a través de modem o teléfono, 9,8 puntos menos que en 2012.
¿Tiene este HOGAR: Módem/Teléfono? ¿Cable/Banda Ancha? Inalámbrico? Ninguno? ENEMDU 2010 – 2012
¿A través de línea telefónica? ¿A través de Cable? ¿A través de medio inalámbrico BAM-3G? ENEMDU 2013.

Gráfico : Gráfico de porcentajes de hogares con acceso al internet en Ecuador.



Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2010-2013)

La provincia con mayor número de personas que utilizan computadora es Pichincha con el 56,2%, seguido por Azuay con el 54,3%; mientas que Los Ríos es la provincia que menos usa el 28,4%.

Gráfico : Grafico porcentual de uso de computadoras por provincia en el Ecuador.

Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU 2013

2.6. **Ataques de crimen cibernético vía web año 2012**

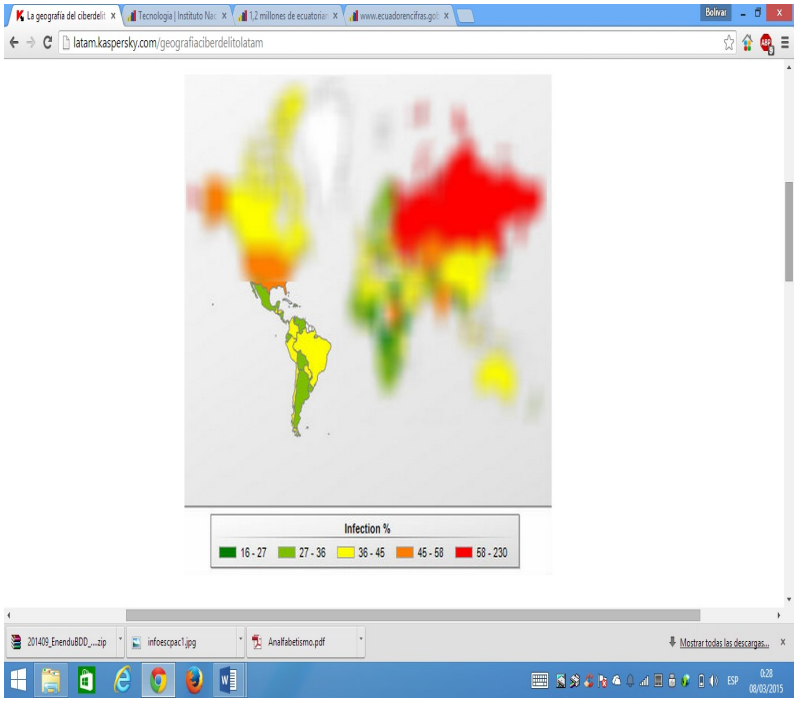
Tabla : Porcentajes de ataques por País

País	% Usuarios atacados vía Web
Chile	39%
Colombia	39%
Panamá	38%
Brasil	37%
Honduras	37%
Paraguay	37%
Perú	37%

Guatemala	36%
México	35%
Argentina	35%
Uruguay	35%
Costa Rica	34%
Bolivia	34%
Ecuador	34%
Nicaragua	34%
El Salvador	33%
Venezuela	32%
República Dominicana	30%

Fuente: http://latam.kaspersky.com/geografiaciberdelitolatam

Gráfico : Mapa de ataques por País.



Fuente: http://latam.kaspersky.com/geografiaciberdelitolatam

2.7. **El crecimiento del cibercrimen en Ecuador es del 130%**[5]

La importante empresa internacional de tecnología Kaspersky Lab siempre ha tratado de estar informada del tema del cibercrimen en especial en américa latina, haciendo énfasis en países como Brasil, Ecuador, México y Argentina, en esta ocasión el tema fue de las formas de ataque cibernéticos más actuales y la forma de protegerse de las mismas, tratando de plantear soluciones contra dichas amenazas y la manera de difundir su protección.

La persona encargada de dirigir esos estudios en Latinoamérica es Dmitry Bestuzhev quien es el jefe del equipo de analistas, de ese estudio se detalla que Brasil(37%), Colombia(39%), Panamá (38%) y Chile(39%) son los países que mayor ataques reciben debido a su creciente economía lo que demuestra que el objetivo del delincuente es el dinero, en el caso de Brasil de cada 100 reales robados 95 se lo hace por la web, lo cual crea una alarma cada vez más creciente.

no.com/noticia/crecimiento-del-cibercrimen-ecuador-es-130

Hablando de Ecuador, este experto ha señalado que en el país el delincuente es nativo y aprende técnicas modernas del extranjero y las aplica inmediatamente y de manera contundente, lo cual ha determinado que haya un crecimiento del 130% para el 2013 con una tendencia a mantenerse en esa proporción para el 2014, como en casi toda la región los principales víctimas son relacionados a la banca, pero el agravante es que esas grandes compañías no hacen trascender esa información para no perder clientela por ese motivo.
Los factores que según el experto inciden en el ataque a esas instituciones bancarias son: el monto a ser usurpado que es casi ilimitado y que la culpabilidad cae en la impunidad, todo esto apoyado por la falta de leyes apropiadas y la escasez de personal técnico especializado.

2.8. **Aspectos relativos ocurridos en el Ecuador**

2.8.1. **El fraude bancario.**[6]

Desde el 2011 se tienen datos oficiales que el fraude bancario es el delito cibernético más frecuente en el Ecuador, este informe lo elaboró la compañía dueña de un antivirus llamada Kaspersky Lab, esta empresa no dejó estadísticas exactas, pero se estima que en ese año (2011) la banca perdió 5 millones de dólares lo que era más del doble que el año anterior, en ese año se dice existieron 1179 ataques al IPS (Instructions of Prevention System), o en español los sistemas de prevención de intrusiones, estas cifras demuestran el aumento del cibercrimen y además la ignorancia informática del cliente cuando hace transacciones bancarias vía Internet. Las compañías que tienen a su cargo ese tipo de giros electrónicos han tratado de realizar diferentes campañas educativas para hacer conciencia y precaución en el cliente al momento de accionar en la web, en especial si usan cybers o no controlan sus claves personales.

2.8.2. **El celular es nuevo objetivo del cibercrimen.**[7]

Ya es un hecho probado por muchas personas, el nuevo objetivo de los delincuentes cibernéticos son los smartphones o celulares de tecnología avanzada, este problema surge con la aparición de las nuevas aplicaciones complementarias a los ya múltiples servicios de los celulares modernos, actúan como elementos infiltrados y su objetivo es apropiarse de fotos o contraseñas privadas del usuario, el asunto es que el usuario no relaciona al celular como elemento portador de un malware. Ya que la evolución del celular lo convierte cada día en un componente multimedia estamos hablando de una minicomputadora que como todas, al menor contacto con el internet se enfrenta a todos los riesgos propios de cualquier pc, según costos y garantías, la compañía Apple reporta menos infiltración de datos que otras; aquí interviene también el desconocimiento digital cuando el portador del celular se conecta con redes wifi ilegítimas lo que las convierte en vínculos o partes del sistema de redes delictivas. Estas aplicaciones alertan sobre cualquier tipo de información en especial actual y puede ser adquirida desde cualquier lugar del mundo.

Por otro lado, existen los trolls (siente placer al sembrar discordia en Internet) que roban la identidad mediante el **internet**[8], hemos escuchado casos donde tú mejor amigo te llama, agitado y furioso, “¿Por qué escribes eso tan horrible sobre mí?”. Cosa que ni siquiera sabes a que se refiere. “Lo que colocaste en tu muro de Facebook”, te dice. No recuerdas haber escrito nada ofensivo en la red social, menos que hiciera referencia a tu amigo donde se observa lo siguiente:

---

6 Fuente: http://www.elcomercio.com/actualidad/negocios/hoy-se-analizo-delito-informatico.html

7 Fuente: http://www.elcomercio.com/actualidad/celular-nuevo-blanco-cibercrimen.html

8 http://www.ecuavisa.com

Frases ofensivas, El perfil parece tuyo, Tiene tus fotografías, El año en que naciste, Tu estado, todos los datos que incluirías en uno propio. No recuerdas haber escrito nada ofensivo de tu amigo, pero la frase está ahí. En el muro de un perfil parece tuyo.
La cuenta es tan verosímil que hasta tu mejor amiga le aceptó una solicitud de amistad.

Sin embargo, no tienes el mínimo control sobre este; ni, por supuesto, lo que se publica en él.

2.8.3. **Solo el 63% de ciberdelitos se penaliza en ecuador.**[9]

En el país no hay información verídica en estadística sobre cuánto es la afectación económica relacionada al delito informático, el único organismo encargado del asunto es la Dirección Nacional de la Policía Judicial, donde se indica que un buen número de personas denunciaron usurpación de datos personales en general.
El único proyecto donde se espera que penalicen estas actividades es el nuevo Código Integral Penal, pero según datos relacionados a su contenido estas sanciones solo cubrirían el 63% de los delitos informáticos y todas sus modalidades, a diferencia por ejemplo de una ley similar de Republica Dominicana que cubre el 100% de delitos, esa ley es especial "contra crímenes y delitos de alta tecnología", en realidad se nota que en el país hay un vacío legal que hace que los criminales cibernéticos tengan bastante impunidad amparándose en el anonimato, muchas veces basados en la "ignorancia tecnológica" del usuario.
En el Ecuador existen varias leyes que penalizan el cibercrimen, el problema es que éstas requieren una continua actualización lo que hace que día a día estas leyes queden rezagadas ya que la innovación tecnológica va más rápido que la conformación de leyes de penalización, a continuación se ofrece un link donde se pueden apreciar las principales leyes referentes al tema:
http://delitosinformaticosloja.blogspot.com/2010/07/constitucion-del-ecuador.html

2.8.4. **Evitar delitos informáticos**[10]

la VII Cumbre de Comunidad de Policías de América (Ameripol) se reunió en Quito el 6 de agosto del 2014, en esta reunión estaban los jefes policiales de toda América y se llegó, dentro de varias conclusiones a la necesidad de ayudarse mutuamente en el campo de la seguridad informática así como la lucha contra la trata de las personas y la corrupción en general, también se llevó a la necesidad de crear un Centro de ciberseguridad para evaluar a ese nivel tanto el fraude como el abuso sexual en menores, adicionalmente se llegaron a conclusiones de los errores comunes del usuario como los siguientes:

1. No subir fotos personales en especial en las redes sociales.
2. Evitar los amigos desconocidos en redes sociales.
3. Denunciar a la policía acosos de desconocidos.
4. Realizar comunes cambios de claves de puntos de acceso importantes.
5. No exponga esa clave a personas desconocidas.

También se dieron a conocer términos actualizados que tienen que ver con el tema por ejemplo el "grooming" el "sexting" y la "pornovenganza" todos ellos relacionados con grabaciones intimas en especial de niños y jóvenes.

Según el sitio oficial http://www.odila.org/ ODILA (observatorio de delitos informáticos en Latinoamérica) [11]

---

9 Fuente: http://www.elcomercio.com/actualidad/63-delitos-cometidos-internet-sancion-penal.html

10 Fuente: http://www.elcomercio.com/actualidad/delitos-informaticos-internet-pornografia-fraude.html

11 "*El usuario puede reportar el incidente sufrido a través de un sencillo formulario y de forma totalmente anónima. Los datos son procesados por ODILA y se informa el resultado de la legislación aplicable en su país y la información sobre los organismos competentes oficiales, donde la víctima podrá realizar su denuncia formal para que dicho hecho sea investigado*

Tabla : Tipificación de delitos informáticos

DELITOS RECONOCIDOS POR LAS NACIONES UNIDAS	TIPIFICACIÓN DE DELITOS INFORMÁTICOS
Fraudes mediante la manipulación de computadoras (programas, datos de entrada y salida, repetición automática de procesos.	Fraudes mediante la manipulación de computadoras: a) Delitos contra elementos físicos – Hardware (robo, estafa) b) Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas, acceso ilícito a datos, protección de programas.
Falsificaciones informáticas (alteración de documentos, falsificación de documentos.	
Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)	Delitos cometidos a través de sistemas informáticos: a) Estafas b) Apoderamiento de dinero por tarjetas de cajero c) Uso de correo electrónico con finalidad criminal d) Utilización de internet como medio criminal.
Acceso no autorizado a servicios y sistemas informáticos (piratas, reproducción no autorizada).	

Fuente: Organización de Naciones Unidas

3. CONCLUSIONES.

Los delitos informáticos son de orden virtual y se hace difícil tipificarlos en especial por parte de la legislación del país y la creación o modificación de esas leyes puede generar circunstancias inesperadas con el agravante que la evolución y renovación constante de los mecanismos cibernéticos obliga que las leyes vayan acordes a ese mismo ritmo evolutivo y no siempre se dará esa posibilidad en especial en casos muy particulares.

El analfabetismo digital también es otro factor a tomar en cuenta ya que los conocimientos que en otrora se consideraban actualizados en estas épocas son caducos con lo que además de la necesidad de captar el conocimiento básico también se debe dar una cultura de actualización constante que no siempre está en la iniciativa de todas las personas.

Las transacciones comerciales son las que más sufren ataques maliciosos, por lo tanto se vuelve vital la existencia de un marco legal actualizado y efectivo que regularice y sirva de apoyo al comercio electrónico tanto en los usuarios como en las empresas vinculadas.

Los auditores informáticos tienen la responsabilidad de ejercer control para la verificación y evaluación del origen del delito, sin embargo su función se limita a dar las recomendaciones a las empresas para que ellas no vuelvan a incurrir en problemas de delitos informáticos.

Los profesionales de la informática tienen el compromiso de fortalecer los mecanismos de seguridad, los controles y demás aspectos de seguridad de las empresas su función no debe limitarse a su acción individual con un resultado hasta cierto punto satisfactorio sino también a

por las autoridades correspondientes. Además, el usuario recibirá recomendaciones básicas a tener en cuenta en todo incidente informático, con el objeto de no perjudicar las tareas de investigación y recolección de evidencia digital".

educar a la gran mayoría de usuarios para que el delito se vea cada vez más limitado en sus fechorías.[12]

4. RECOMENDACIONES.

Aunque no existe un método 100 por ciento efectivo, se sugiere tomar en cuenta los siguientes sencillos consejos para evitar ser víctima del cibercrimen:

Modificar los ajustes por defecto del navegador, así se elimina la opción de seguimiento y este anunciará la fuente Web indeseable.

Deshabilitar la instalación automática para bloquear los sitios web sospechosos y pop-ups.

Usar la navegación privada que ofrece el navegador ya que al cerrarlo todos los datos se eliminan.

Limpiar la caché de la computadora

Evitar los paneles de búsqueda

Otra recomendación valedera y preventiva es la que el estado Ecuatoriano está contratando a la compañía Spamina, la cual dará seguridad informática y protección de correo electrónico contra el spa, de uso en empresas y entidades bancarias que son los blancos más asediados por los delincuentes informáticos. Además de esto se está implementando las "billeteras móviles' en los bancos del Ecuador.

Como recomendación final que se haga una restructuración de las leyes en nuestro país contra los robos informáticos esto ayudaría a minimizar los delitos.

5. REFERENCIAS BIBLIOGRAFICAS

Almazan, R. S. (09 de septiembre de 2011). *Gaceta Electronica Innovación.* Obtenido de Gaceta Electronica Innovación.: http://www.foroconsultivo.org.mx/innovacion.gaceta/los-pi-q-2/436-brecha-y-analfabetismo-digitales-

Cevallos, J. (03 de marzo de 2015). *El UNiverso.com.* Obtenido de El UNiverso.com: http://www.eluniverso.com/noticias/2015/03/03/nota/4616526/67-conexiones-internet-ecuador-se-hara-traves-celular-2020

Computer Forensic. (01 de enero de 2015). *Delitos Informaticos.info.* Obtenido de Delitos Informaticos.info: http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

David Salazar. (10 de octubre de 2012). *Hackers and Crackers*. Obtenido de Hackers and Crackers: http://davidsalaza.blogspot.com/2012/10/seguridad-informatica.html

Diario_El_Comercio. (07 de marzo de 2012). *Diario El comercio*. Obtenido de Diario El comercio: http://www.elcomercio.com/actualidad/negocios/hoy-se-analizo-delito-informatico.html

12 fuente: http://delitosinformaticosiutlv.blogspot.com/p/conclusiones_25.html

Diario_El_Comercio. (29 de noviembre de 2014). *Diario El comercio*. Obtenido de Diario El comercio: http://www.elcomercio.com/actualidad/celular-nuevo-blanco-cibercrimen.html

Diario_El_Comercio. (06 de agosto de 2014). *Diario El Comercio*. Obtenido de Diario El Comercio: http://www.elcomercio.com/actualidad/delitos-informaticos-internet-pornografia-fraude.html

Ecuavisa. (27 de febrero de 2015). *Ecuavisa.com.* Obtenido de Ecuavisa.com: http://www.ecuavisa.com/articulo/noticias/tecnologia/100655-quien-observa-lo-que-consultas-internet

Freire, J. (01 de julio de 2013). *Diario ElUniverso*. Obtenido de Diario ElUniverso: http://www.doctortecno.com/noticia/crecimiento-del-cibercrimen-ecuador-es-130

Hyttu. (04 de agosto de 2012). *Seguridad Informatica*. Obtenido de Seguridad Informatica: http://seguridadinformatica-ezequielgarcia.blogspot.com/2012/08/para-que-sirve-la-seguridad-informatica.html

INEC. (01 de enero de 2014). *Ecuador en cifras*. Obtenido de Ecuador en cifras: http://www.ecuadorencifras.gob.ec/

Jaramillo, D. V. (08 de septiembre de 2014). *Diario El Comercio.* Obtenido de Diario El Comercio: http://www.elcomercio.com.ec/tendencias/ecuatorianos-analfabeto-digital-cifras-tecnologia.html

Naciones UNidas. (19 de abril de 2010). *12. Congreso de las Naciones UNidas sobre prevención del delito y justicia penal.* Obtenido de 12. Congreso de las Naciones UNidas sobre prevención del delito y justicia penal: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

Ortiz, S. (28 de junio de 2014). *Diario El Comercio*. Obtenido de Diario El Comercio: http://www.elcomercio.com/actualidad/63-delitos-cometidos-internet-sancion-penal.html