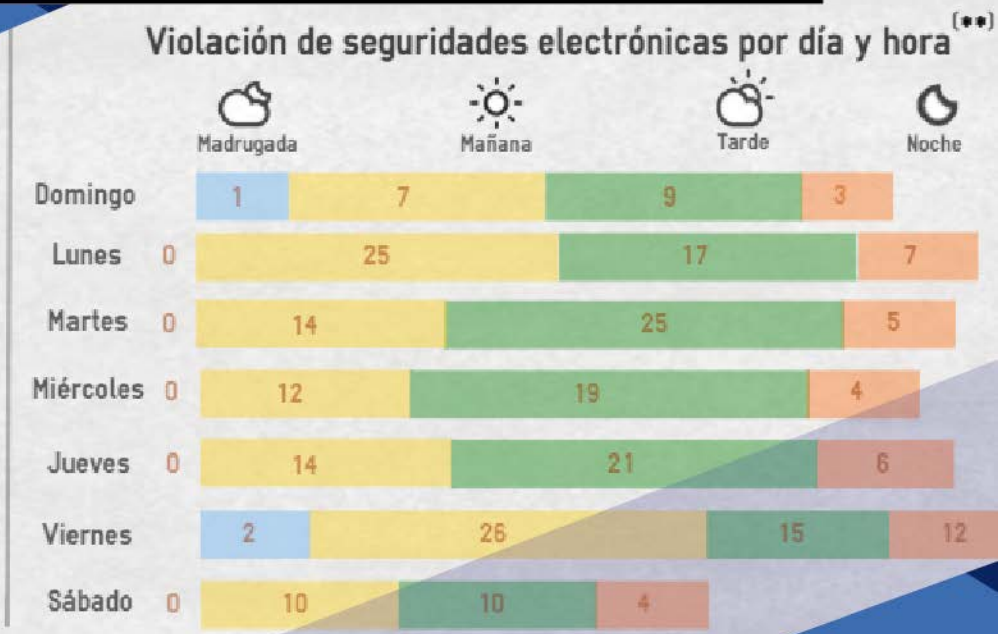
Universidad Ecotec

Análisis espacial de los delitos y aplicación de la normativa jurídica ecuatoriana



Compiladores

Carlos Esteban Alcívar Trejo, Mgs.
Juan Tarquino Calderón Cisneros, Mgs.

ANÁLISIS ESPACIAL DE LOS DELITOS Y APLICACIÓN DE LA NORMATIVA JURÍDICA ECUATORIANA

COMPILADORES:

Carlos Alcívar Trejo, Mgs.

Juan Tarquino Calderón Cisneros, Mgs.

2016

TÍTULO

Análisis Espacial de los Delitos y Aplicación de la Normativa Jurídica Ecuatoriana

COMPILADORES

Carlos Alcívar Trejo, Mgs.
Juan Tarquino Calderón Cisneros, Mgs.

AUTORES

Carlos Alcívar Trejo, Mgs.
Juan Tarquino Calderón Cisneros, Mgs.
Glenda Blanc Pihuave, Mgs.
Bolívar Duchi Ortega, Mgs.

AÑO

2016

EDICIÓN

MSc. Ángela María González Laucirica - Departamento de Publicaciones
Andrea Estefanía Agurto Tandazo - Coedición
Universidad ECOTEC

ISBN

978-9942-960-10-8

NO. PÁGINAS

86

LUGAR DE EDICIÓN

Samborondón - Ecuador

DISEÑO DE CARÁTULA

Ing. Arnaldo Oscar Sánchez González - Departamento de Marketing y Relaciones Públicas
Universidad ECOTEC

INDICE

INTRODUCCIÓN

En el presente libro se abordará una revisión actualizada de la distribución de la delincuencia en Guayaquil, mediante el uso de técnicas geoestadísticas. En el análisis espacial se determinan modelos teóricos de ajustes de los variogramas con el objetivo de estudiar los tipos de delitos que se distribuyen en cuatro jefaturas o departamentos dentro del sistema de la Policía Judicial del Guayas que son; delitos contra la propiedad, delitos a la administración y fe pública, vehículos y delitos contra las personas. Con la aplicación de los métodos geoestadísticos se puede obtener mapas de estimación y de varianza; y con este se determinan los lugares donde se concentran la mayor incidencia de delitos en la ciudad de Guayaquil.

El uso de las técnicas geoestadísticas en el análisis espacial de variabilidad de los delitos en la ciudad de Guayaquil es completamente nuevo. Los problemas de seguridad que se presentan en la actualidad, la delincuencia en nuestro medio y en estos tiempos, que con mucha frecuencia son descuidados por nuestra sociedad, porque es ahí donde se comienza a resquebrajar este miembro de la sociedad, sin ni siquiera darle la oportunidad de llegar a ser miembro eficaz y productivo, que contribuya a la tarea común debido sobre todo a la falta de empleo y la carencia de medios para poder subsistir.

El propósito es precisamente realizar un estudio espacial con respecto de la distribución de la delincuencia el cual se encuentra sumido nuestra ciudad, estableciendo zonas de inseguridad. El uso adecuado de mapas para establecer zonas de seguridad en la ciudad y la información que brinda el último Censo de Población y de Vivienda; lo cual es un excelente marco de referencia en el procesamiento adecuado de los datos, al efectuarse el levantamiento de información donde ocurrió el delito por parte de la policía o las autoridades del caso.

Los mapas de distribución por delitos constituyen una herramienta imprescindible para la planificación de la lucha contra la delincuencia, indicando la necesidad de un tratamiento más intenso en las áreas estudiadas. Para llegar al punto culminante de la "delincuencia" existen una serie de causas y factores que influyen en un determinado ser humano a cometer un acto punible (delinquir).

Dejando en constancia esta problemática en articulación con las normativas del Estado, frente a estos delitos, el derecho a la seguridad jurídica se traduce en la confianza que todos los ciudadanos debemos tener en el sistema jurídico ecuatoriano, la cual implica que las disposiciones normativas e instituciones jurídicas se mantengan en un periodo considerable

de tiempo, a fin de que los ciudadanos sepan bajo qué reglas tienen que actuar frente al Estado.

Esto determina que la legislación debe ser emitida de tal forma que garantice la aplicación efectiva del principio de la seguridad jurídica, más aún, si una ley tiene una determinada disposición, ésta no puede ser desconocida por resoluciones de inferior jerarquía, ni puede ser aplicada por ninguna autoridad del Estado.

CAPÍTULO I. IMPACTO SOCIAL DE LOS DELITOS EN GUAYAQUIL ECOTEC

Autores: Glenda Blanc Pihuave, Mgs.
Coordinadora de Información y Estadísticas de Vicerrectorado Académico y Docente de la Facultad de Sistemas de la Universidad Tecnológica ECOTEC

Carlos Alcívar Trejo, Mgs.
Coordinador Académico y Docente de la Facultad de Derecho de la Universidad Tecnológica

Bolívar Duchi Ortega, Mgs.
Docente de la Facultad de Sistemas de la Universidad Tecnológica

INTRODUCCIÓN

Hace unos 15.000 años (Lascaux, 2008) en las paredes de las cuevas de Lascaux (Francia) los hombres de Cro-Magnon pintaban en las paredes los animales que cazaban, asociando estos dibujos con trazas lineales que, se cree, cuadraban con las rutas de migración de esas especies (Curtis, 2006). Si bien este ejemplo es simplista en comparación con las tecnologías modernas, estos antecedentes tempranos imitan a dos elementos de los Sistemas de Información Geográfica modernos: una imagen asociada con un atributo de información. (Whitehouse, s.f.)

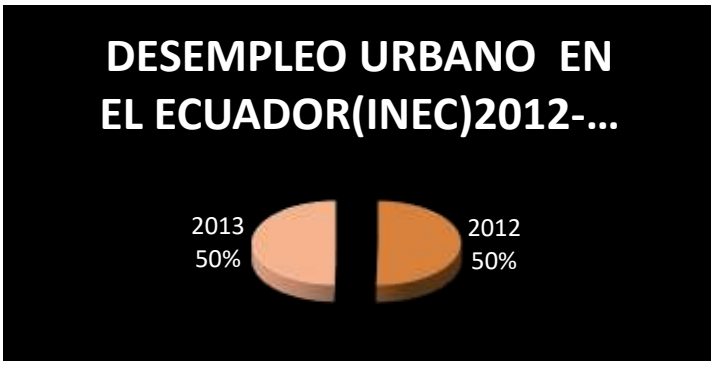
Los cambios de la política en el ecuador en estos últimos 20 años dan como conclusión una razón que tienden a degenerar la sociedad en la que se desenvuelven pues apelan al alcohol u otras drogas, así como la delincuencia. Una causa muy fuerte es la migración como factor que se ha incrementado sustantivamente en las últimas décadas, lo que ha significado serios estragos al tejido social, sobre todo por el abandono del país de miles de hombres y mujeres que dejan, no sólo el país sino también su ciudad, su barrio, su comunidad, sus hogares con niños y mujeres que sufren la consecuencia de la soledad el abandono. (Haz, 2011)

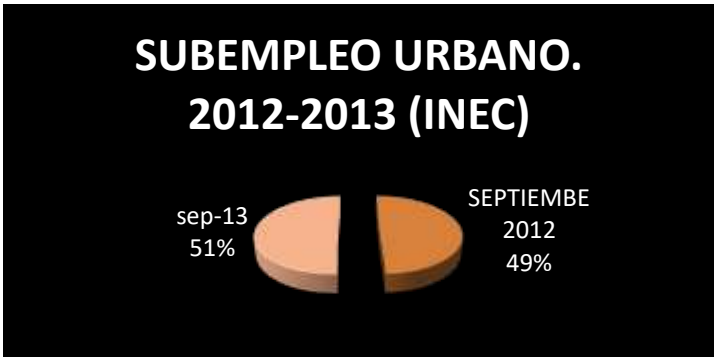
1. El Desempleo en el Ecuador

El desempleo urbano en Ecuador se ubicó en 4,57% en septiembre de 2013 frente al 4,63% del mismo mes del año anterior, según datos publicados hoy 16 de octubre del 2103 por el Instituto Nacional de Estadística y Censos (INEC). Según el INEC, el subempleo en el área urbana llegó a 42,69% en comparación con el 41,88% de septiembre del año pasado. Asimismo, la ocupación plena se ubicó en 50,53% versus el 51,48% de septiembre del 2012. La encuesta revela que aproximadamente 8 de cada 10 empleos en el área urbana son generados por el sector privado, tendencia que se ha mantenido en los últimos años. La

pobreza urbana en septiembre del 2013 afectó el 15,74% de la población, es decir, de cada 100 habitantes 16 son pobres, cifra similar a la registrada un año antes. Mientras que la extrema pobreza urbana se ubicó en 4,08% frente al 4,68% del mismo mes del 2012. (INEC, 2013)

Gráfico 1.1. Desempleo en el Ecuador





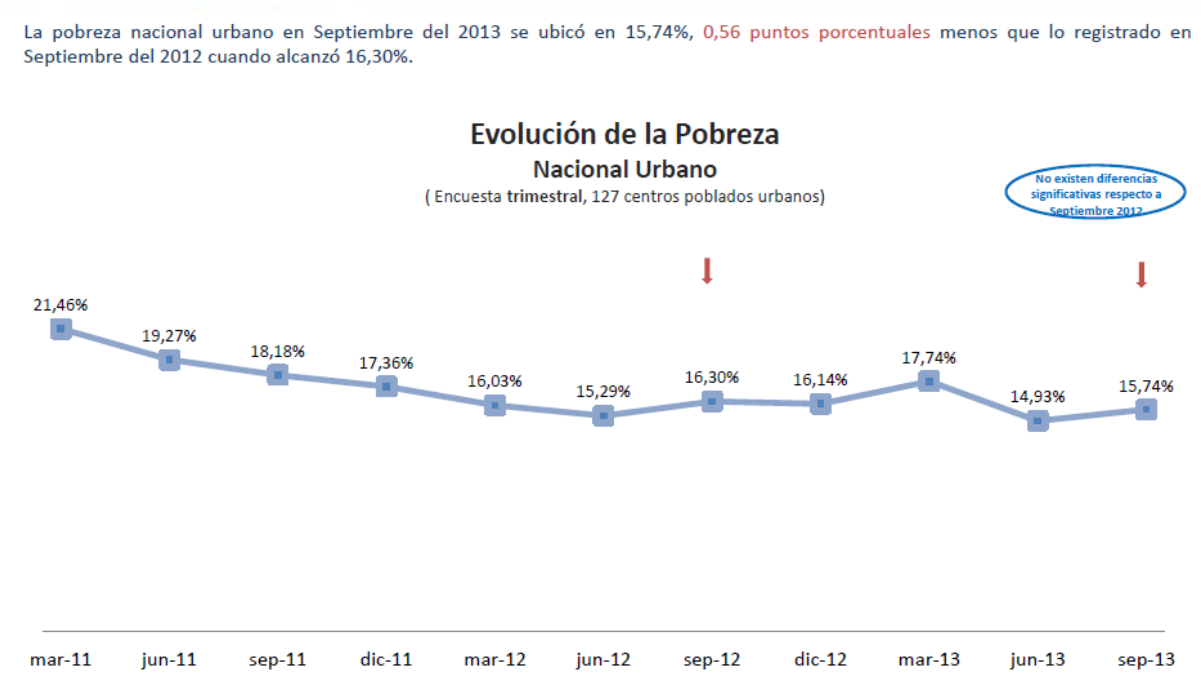
Fuente: INEC. Recuperado de http://www.elcomercio.com.ec/negocios/Desempleo-Ecuador-septiembre-INEC_0_1012098884.html

ECUADOR - TASA DE DESEMPLEO

REAL	ANTERIOR	MAYOR	MENOR	PRONÓSTICO	FECHAS	UNIDAD	FRECUENCIA
4.86	4.60	12.05	4.60	4.30 | 2013/12	2003 - 2013	POR CIENTO	TRIMESTRAL

El coeficiente de GINI, índice que mide la desigualdad de los ingresos entre la población, en un intervalo de 0 a 1 (el 0 corresponde a la perfecta igualdad), actualmente se sitúa en 0,46 en zonas urbanas (INEC, 2013). En septiembre 2013, la línea de pobreza se ubicó en 2,57 dólares per cápita diarios. Los individuos cuyo ingreso per cápita es menor a la línea de pobreza son considerados pobres.

Gráfico 1.2. Evolución de la Pobreza Nacional Urbano



Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo-INEC

2. Causas del Desempleo

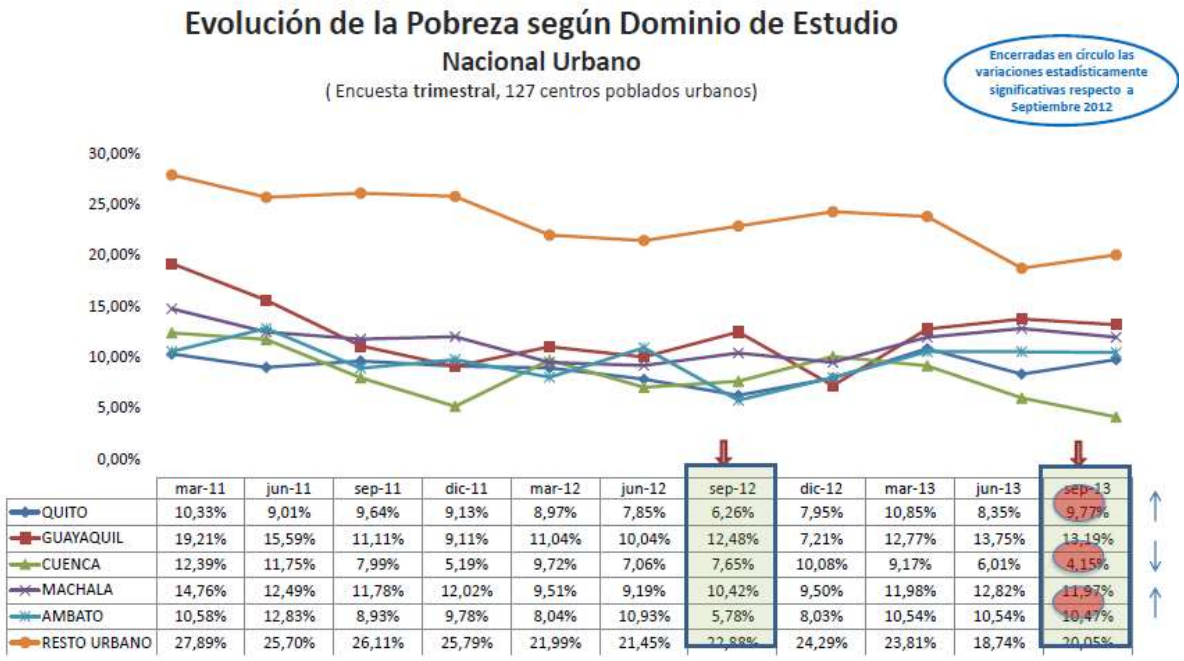
El desempleo es el ocio involuntario de una persona que desea encontrar trabajo, esta afirmación común a la que se llega puede deberse a varias causas. Cuando existe un descenso temporal que experimenta el crecimiento económico caracterizado por la disminución de la demanda, de la inversión y de la productividad y por el aumento de la inflación. La actividad económica tiene un comportamiento cíclico, de forma que los períodos de auge en la economía van seguidos de una recesión o desaceleración del crecimiento. (INEC, 2013)

Pobreza en nuestro país

La pobreza es un fenómeno que tiene muchas dimensiones, por lo que no existe una única manera de definirla, la mayor parte de las veces, la pobreza se ha definido como la incapacidad de una familia de cubrir con su gasto familiar una canasta básica de subsistencia. Este enfoque metodológico clasifica a las personas como pobres o no pobres. Similarmente,

en el caso de que el gasto familiar no logre cubrir los requerimientos de una canasta alimentaria, se identifica a la familia como pobre extrema.

Gráfico 1.3. Evolución de la Pobreza según Dominio de Estudio



	mar-11	jun-11	sep-11	dic-11	mar-12	jun-12	sep-12	dic-12	mar-13	jun-13	sep-13
QUITO	10,33%	9,01%	9,64%	9,13%	8,97%	7,85%	6,26%	7,95%	10,85%	8,35%	9,77%
GUAYAQUIL	19,21%	15,59%	11,11%	9,11%	11,04%	10,04%	12,48%	7,21%	12,77%	13,75%	13,19%
CUENCA	12,39%	11,75%	7,99%	5,19%	9,72%	7,06%	7,65%	10,08%	9,17%	6,01%	4,15%
MACHALA	14,76%	12,49%	11,78%	12,02%	9,51%	9,19%	10,42%	9,50%	11,98%	12,82%	11,97%
AMBATO	10,58%	12,83%	8,93%	9,78%	8,04%	10,93%	5,78%	8,03%	10,54%	10,54%	10,47%
RESTO URBANO	27,89%	25,70%	26,11%	25,79%	21,99%	21,45%	22,88%	24,29%	23,81%	18,74%	20,05%

Fuente: Encuesta Nacional de Empleo Desempleo y Subempleo-INEC

Cuando en ciertas regiones o industrias donde la demanda de mano de obra fluctúa dependiendo de la época del año en que se encuentren. Cuando se dan cambios en la estructura de la economía, como aumentos de la demanda de mano de obra en unas industrias y disminuciones en otras, impidiendo que la oferta de empleo se ajuste a la velocidad adecuada.

Adicionalmente esta situación se puede evidenciar en determinadas zonas geográficas, por la implantación de nuevas tecnologías que sustituyen a la mano de obra. Cuando por causas ajenas a la voluntad del trabajador impide su incorporación al mundo laboral.

3. Efectos del Desempleo

Efectos Económicos. - El desempleo impone un costo en la economía como un todo, debido a que se producen menos bienes y servicios. Cuando la economía no genera suficientes empleos para contratar a aquellos trabajadores que están dispuestos y en posibilidades de trabajar, ese servicio de la mano de obra desempleada se pierde para siempre. (Acosta, 2010)

En un sistema económico, uno de los factores fundamentales es el suministro de recursos humanos (trabajo), la actividad productiva: unidades familiares que incluyen a todos los individuos que, directa o indirectamente, participan de las actividades productivas y consumen los bienes y servicios finales elaborados y las unidades de producción que están representadas por las empresas y son las encargadas de dinamizar la actividad económica de un país.

Adicionalmente, el desempleo trae consigo una pérdida en el nivel de ingresos en los gobiernos; por cuanto, deja de percibir impuestos que el trabajador y la empresa aportaba normalmente mientras este desempeñaba su trabajo. Además, los egresos que realiza la administración pública por concepto de subsidiar a los desempleados.

Gráfico 1.4. Índice de desempleo

Fuente: Recuperado de http://es.tradingeconomics.com/ecuador/unemployment-rate

Esta relación existente se deteriora, cuando el número de unidades familiares que participan de las actividades productivas es menor (desempleo), lo que conlleva a que la presencia de compradores que están dispuestos y pueden comprar algún producto o servicio al precio que se les ofrece no dispongan de ingresos suficientes por cuanto no tienen empleo, esto ocasiona que las unidades productivas bajen sus niveles de producción y no se pueda continuar con el ciclo económico normal por cuanto se evidencia una brecha en la demanda.

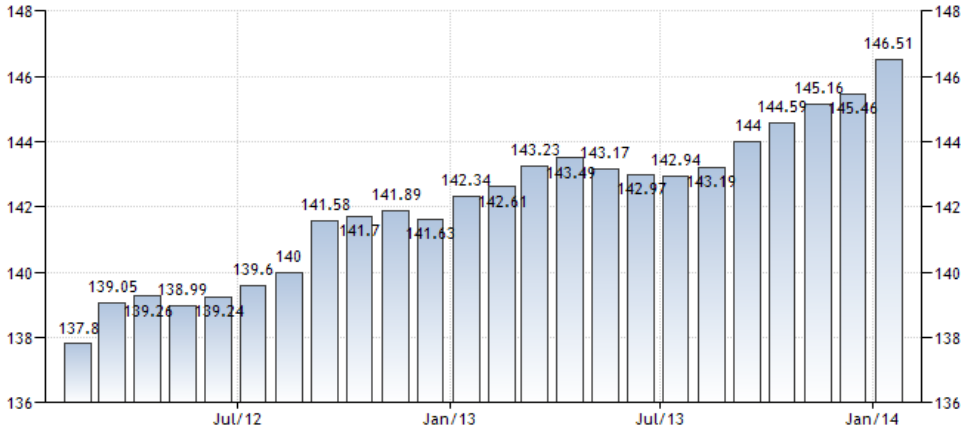
Efectos Sociales. - El costo económico del desempleo es, ciertamente, alto, pero el social es enorme. Ninguna cifra monetaria refleja satisfactoriamente la carga humana y psicológica de los largos períodos de persistente desempleo involuntario. La tragedia personal del desempleo ha quedado demostrada una y otra vez" (Laaz et al., 2013).

Interpretación Económica del Desempleo. - Interpretar económicamente el desempleo es buscar las diferentes razones que implica el estar desempleado, para ello consideraremos los tipos de desempleo existentes, también distinguiremos entre desempleo voluntario e involuntario, así como las razones de rigidez de los sueldos y salarios. (Camones, C., & María, C., 2013).

ECUADOR - ÍNDICE DE PRECIOS AL CONSUMIDOR (IPC)

REAL	ANTERIOR	MAYOR	MENOR	PRONÓSTICO	FECHAS	UNIDAD	FRECUENCIA	
146.51	145.46	146.51	0.02	147.10 | 2014/02	1969 - 2014	PUNTOS DE INDEXACIÓN	MENSUAL	2004=100 , NSA

Gráfico 1.5.



Fuente: http://es.tradingeconomics.com/ecuador/unemployment-rate

PRECIOS	ÚLTIMO		ANTERIOR	MAYOR	MENOR	PRONÓSTICO		UNIDAD	TENDENCIA
ÍNDICE DE PRECIOS AL CONSUMIDOR (IPC)	146.51	2014-01-15	145.46	146.51	0.02	147.10	2014-02-28	PUNTOS DE INDEXACIÓN	
TASA DE INFLACIÓN	2.92	2014-01-31	2.70	107.87	-2.67	3.36	2014-02-28	POR CIENTO	
LOS PRECIOS AL PRODUCTOR	2734.23	2014-01-15	2795.06	2982.72	199.07	2729.08	2014-02-28	PUNTOS DE INDEXACIÓN	

[+]

En un país tan inestable como es el Ecuador que siempre está en permanentes fluctuaciones, esto por la inestabilidad económica que sufrió el país por la crisis mundial en los años 2009 y 2010; así como también la inestabilidad política interna y externa. Históricamente, los precios de los productos tienen tendencia a subir, lo que afecta al consumidor en su poder adquisitivo;

sin embargo, actualmente con las nuevas políticas de gobierno el salario es incrementado conforme la inflación para compensar y aliviar de alguna manera los costos de los productos.

Los problemas de seguridad que se presentan en la actualidad, la delincuencia en nuestro medio y en estos tiempos, que con mucha frecuencia son descuidados por nuestra sociedad, porque es ahí donde se comienza a resquebrajar este miembro de la sociedad, sin ni siquiera darle la oportunidad de llegar a ser miembro eficaz y productivo, que contribuya a la tarea común debido sobre todo a la falta de empleo y la carencia de medios para poder subsistir. (Álava, 2013)

El propósito es precisamente realizar un estudio espacial con respecto a la distribución de la delincuencia el cual se encuentra sumido la ciudad, estableciendo zonas de inseguridad. El uso adecuado de mapas para establecer zonas de seguridad en la ciudad y la información que brinda el último Censo de Población y de Vivienda da un excelente marco de referencia en el procesamiento adecuado de los datos al efectuarse el levantamiento de información donde ocurrió el delito por parte de la policía o las autoridades del caso.

Los mapas de distribución por delitos constituyen una herramienta imprescindible para la planificación de la lucha contra la delincuencia, indicando la necesidad de un tratamiento más intenso en las áreas estudiadas.

CAPÍTULO II.- COMPONENTES CONSTITUTIVOS DEL DELITO. FUNDAMENTOS TEÓRICOS Y NORMATIVOS.

Autor: Carlos Alcívar Trejo, Mgs.
Coordinador Académico y Docente de la Facultad de Derecho de la Universidad Tecnológica ECOTEC

INTRODUCCIÓN

Los problemas de la sociedad se dimensionan con más fuerza. Harry Godland, indicó que "las incapacidades mentales es la principal causa de la criminalidad". (Godland citado en Pérez, 1986, p. 54)

Los postulados de esta Teoría son:

a) El débil mental sería un tipo de delincuente.
b) Las personas nacen débil mental o con una inteligencia anormal.
c) En la mayoría de las ocasiones estas personas conocen los delitos peligrosos de asalto, robo y otros enmarcados en el código de Defensa de nuestro Estado.
d) Los débiles mentales comenten estos delitos por falta de los factores inhibitorios sociales; sobre todo este no puede exteriorizar los que están descritos como buenos o malos.
e) No tienen la capacidad de prever la consecuencia de sus actos y por lo tanto la amenaza penal no tiene efecto sobre esta clase de individuo.
f) Son personas muy sugestionables y cualquier criminal más inteligente que él lo puede llevar a cometer un delito.
g) Por ser débil mental en los barrios donde existe una criminalidad alta, o hacer por imitación.
h) Los inteligentes tienen la capacidad de ocultar la criminalidad, pero los débiles mentales carecen de ella.

Guillermo Cabanellas, expresa que "la seguridad jurídica 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, al tiempo que la seguridad jurídica limita y determina las facultades y los derechos de los poderes públicos".

El artículo 82 de la Carta Fundamental del Estado, señala que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicables para las autoridades competentes, lo cual significa que

todos los ecuatorianos debemos vivir bajo el mandato de las leyes y su aplicación uniforme, siendo resumida por Jesucristo, cuando dijo: “No penséis que he venido para abrogar la ley o los profetas, no he venido para abrogarla, sino para cumplirla”. (Mt.5.17).

Uno de los pilares del derecho constitucional es la seguridad jurídica y en nuestro ordenamiento jurídico constituye uno de los deberes fundamentales del Estado. La seguridad jurídica es el elemento esencial y patrimonio común del Estado de Derecho; implica la convivencia jurídicamente ordenada, la certeza sobre el derecho escrito y vigente, en suma, es la confiabilidad en el orden jurídico.

El derecho a la seguridad jurídica se traduce en la confianza que todos los ciudadanos debemos tener en el sistema jurídico ecuatoriano, la cual implica que las disposiciones normativas e instituciones jurídicas se mantengan en un periodo considerable de tiempo, a fin de que los ciudadanos sepan bajo qué reglas tienen que actuar frente al Estado.

Esto determina que la legislación debe ser emitida de tal forma que garantice la aplicación efectiva del principio de la seguridad jurídica, más aún, si una ley tiene una determinada disposición, ésta no puede ser desconocida por resoluciones de inferior jerarquía, ni puede ser dejada de aplicar por ninguna autoridad del Estado.

Se pueden numerar un sinnúmero de problemas, por muy pequeños que sean, pero problemas son, y por lo tanto afectan a toda persona, y por ende a la sociedad. El desempleo, la delincuencia, la Prostitución, las violaciones, los asaltos, los asesinatos, el alcoholismo; y, la pobreza.

Para llegar al punto culminante de la "delincuencia" existen una serie de causas y factores que influyen en un determinado ser humano a cometer un acto punible (delinquir); puede decirse que estas causas son el "conjunto de infracciones punibles clasificadas con fines sociológicos y estadísticos, según sea el lugar, tiempo y especialidad que se señale a la totalidad de transgresiones penadas".

Estas causas se dan cuando los niños han sido separados del medio familiar durante su infancia, no han tenido hogares estables, ellos se verán relegados, perdiendo el punto de equilibrio entre la realidad y el placer, y caerán en actividades delictivas o perversas, son hijos de padres delincuentes, y sus preceptos morales y formación son antisociales; éstas se manifiestan a los seis o siete años de edad; además, el maltrato físico, lo que hace que ellos huyan de sus hogares y emigren a las calles; donde la calle es la escuela de toda clase de

cosas malas, de aprendizaje rápido para ellos, porque de una u otra forma tienen que aprender a defenderse de todos los peligros que se les presenten en el camino.

La ciudad de Guayaquil tiene un incremento diario en los diferentes tipos de delitos, por la situación que se encuentra atravesando el país, debido entre otras cosas a aspectos como los que se detallan a continuación: La pérdida de valores éticos y morales; La mala administración de los gobiernos; La falta de aplicación de las Leyes y corrupción de la Función Judicial; La falta de Legislación a favor de la sociedad; La generalizada corrupción que se encuentra en todos los estratos sociales; La crisis económica; El desempleo masivo; La migración campesina; La inflación de los últimos años; La falta de alimentación, vivienda, salud, educación, entre otras.

Con los datos proporcionados por la Fiscalía representa a la sociedad en la investigación y persecución del delito y en la acusación penal de los presuntos infractores. Y su clasificación, la institución donde se judicializan los hechos delictivos ocurridos.

Cada acta de denuncia que se recepta en las dependencias de la Fiscalía de Guayaquil reporta al menos una acción delictiva, en los casos en que en el acta se denuncie más de un delito, ésta es rotulada con el delito más “grave” reportado. En este informe los delitos están agrupados en tres categorías, principales delitos contra las personas, principales delitos contra la propiedad y otras denuncias. Los principales delitos contra las personas son: Homicidio, Plagio, Robo Agravado, Secuestro Express y Violación; conforman el conjunto de los principales delitos contra la propiedad el Robo simple, Robo en domicilio, Robo de vehículos, Robo de motocicletas, Robo en local comercial y Robo en banco; en tanto que entre las “otras denuncias” están Estafa, Abuso de confianza, Agresión, Amenaza, etc., podremos observar las tendencias de cada uno de los delitos empleando tratamientos matemáticos adecuados para el análisis (INDEX, 2015).

TABLA 1

Denuncias receptadas en las Oficinas de Ministerio Público en Guayaquil

DENUNCIAS RECEPTADAS DURANTE EL AÑO 2013

Totales Generales

CATEGORÍA DE DELITO	NÚMERO DE DENUNCIAS	PORCENTAJE
Principales Delitos Contra las Personas	7324(8129)	24,99%
Principales Delitos Contra la Propiedad	7167(7118)	24,45%
Suma de Principales Delitos	14491(15247)	49,44%
Otras Denuncias	14822(15434)	50,56%
GRAN TOTAL DE DENUNCIAS RECEPTADAS EN 2011	***29313(30681)***	***100,00%***

NOTA: El total de "principales delitos" representa el 49,44% de todos los delitos denunciados durante el año 2013

Fuente: Recuperado de **http://www.icm.espol.edu.ec/delitos**

1. ÁMBITOS DE APLICACIÓN (CÓDIGO ORGÁNICO INTEGRAL PENAL)

Artículo 14.- Ámbito espacial de aplicación. - Las normas de este Código se aplicarán a:

1. Toda infracción cometida dentro del territorio nacional.
2. Las infracciones cometidas fuera del territorio ecuatoriano, en los siguientes casos:

a) Cuando la infracción produzca efectos en el Ecuador o en los lugares sometidos a su jurisdicción.

b) Cuando la infracción penal es cometida en el extranjero, contra una o varias personas ecuatorianas y no ha sido juzgada en el país donde se la cometió.

c) Cuando la infracción penal es cometida por las o los servidores públicos mientras desempeñan sus funciones o gestiones oficiales.

TABLA 2

Denuncias receptadas en las Oficinas de Ministerio Público en Guayaquil

DENUNCIAS RECEPTADAS DURANTE EL AÑO 2013

Principales Delitos contra las Personas

DELITO	FRECUENCIA ABSOLUTA	PORCENTAJE RESPECTO A ESTA CATEGORÍA DE DELITO	PORCENTAJE RESPECTO A LA SUMA DE PRINCIPALES DELITOS	PORCENTAJE RESPECTO AL "GRAN TOTAL"
Homicidio	130(178)	1,77%	0,90%	0,44%
Plagio	176(275)	2,40%	1,21%	0,60%
Robo Agravado	6384(7056)	87,17%	44,05%	21,78%
Secuestro Express	177(221)	2,42%	1,22%	0,60%
Violación	457(399)	6,24%	3,15%	1,56%
SUMA DE LOS PRINCIPALES DELITOS CONTRA LAS PERSONAS	***7324(8129)***	***100,00%***	***50,54%***	***24,99%***

NOTA: Los "delitos contra las personas" representan el 50,54% de los "principales delitos" denunciados y el 24,99% del "gran total

Fuente: Recuperado de **http://www.icm.espol.edu.ec/delitos**

¿Qué tipo de delitos puedo denunciar en la Fiscalía más cercana?

Delitos de Acción Pública

Homicidio

Asesinato (homicio agravado)

Delitos sexuales y atentado al pudor

Secuestro

Robo

Narcotráfico

Peculado, concusión, cohecho, enriquecimiento ilícito

Trata de Personas

Estafa u otras defraudaciones (cuando existan 15 o más ofendidos)

Delitos de Tránsito

Lavado de activos

Usura, entré otros

Nota importante: Estos delitos no requieren de denuncia escrita, basta con informar a la Fiscalía o Policía Judicial. La Fiscalía está obligada a investigar de oficio, sin necesidad de la intervención de las partes interesadas, ni reconocimientos de firmas.

De instancia Particular

Revelación de secretos de fábrica

Hurto

Estupro en mayores de 16 años

Rapto

Muerte de animales

Usurpación

Nota importante: Deben denunciarse en la Fiscalía o Policía Judicial, para que inicien una investigación. La denuncia no requiere de abogado y debe ser reconocida.

¿En qué situaciones la Fiscalía NO puede ayudarme?

A la Fiscalía no le corresponde:

Receptar denuncias por pérdida de documentos de ningún tipo (competente Intendencia y Comisarías).

Daños a la propiedad privada. (Competente Juez Penal).

El Cobro de deudas provenientes de letras de cambio, pagarés y cheques en garantía. (Competente Juez Civil).

El Cobro de arriendos atrasados ni terminaciones de contratos de arrendamiento. (Competente es el Juez de Inquilinato).

Recuperación de menores llevados por sus progenitores (padre o madre), o cobro de pensiones alimenticias. (Competente Juez de Niñez y Adolescencia).

Recuperación de Animales (Competente es el Intendente).

Emisión de boletas de auxilio; elaboración de actas de mutua respeto entre las partes. (Competente Intendente, comisarios nacionales y comisarías de la mujer y la familia).

No tramita seguros.

DELITO CONTRA LA PROPIEDAD: robo a personas (vía pública); estruches (robo, departamentos.); robos locales comerciales; robo a bancos; hurto; abigeato; robo en transporte. Urbano; robo carreteras (transa.) (interp); robo carga carretera; apropiación ind./ abuso confianza.; estafas; extorsión.

TABLA 3

Denuncias receptadas en las Oficinas de Ministerio Público en Guayaquil

DENUNCIAS RECEPTADAS DURANTE EL AÑO 2013

Principales Delitos contra la Propiedad

DELITO	FRECUENCIA ABSOLUTA	PORCENTAJE RESPECTO A ESTA CATEGORÍA DE DELITO	PORCENTAJE RESPECTO A LA SUMA DE PRINCIPALES DELITOS	PORCENTAJE RESPECTO AL "GRAN TOTAL"
Robo Simple	2974(2418)	41,50%	20,52%	10,15%
Hurto	1851(1398)	25,83%	12,77%	6,31%
Robo en Domicilio	1141(1479)	15,92%	7,87%	3,89%
Robo de Vehículos	816(1282)	11,39%	5,63%	2,78%
Robo en Local Comercial	383(539)	5,34%	2,64%	1,31%
Robo en Bancos	2(2)	0,03%	0,01%	0,01%
SUMA DE LOS PRINCIPALES DELITOS CONTRA LA PROPIEDAD	***7167(7118)***	***100,00%***	***49,46%***	***24,45%***

NOTA: Los "delitos contra la propiedad" representan el 49,46% de los "principales delitos" denunciados y el 24,45% del "gran total"

Fuente: Recuperado de http://www.icm.espol.edu.ec/delitos

2. DENUNCIA

Artículo 421.- Denuncia. - La persona que llegue a conocer que se ha cometido un delito de ejercicio público de la acción, podrá presentar su denuncia ante la Fiscalía, al personal del Sistema especializado integral de investigación, medicina legal o ciencias forenses o ante el organismo competente en materia de tránsito.

La denuncia será pública, sin perjuicio de que los datos de identificación personal del denunciante, procesado o de la víctima, se guarden en reserva para su protección.

Artículo 422.- Deber de denunciar. - Deberán denunciar quienes están obligados a hacerlo por expreso mandato de la Ley, en especial:

1. La o el servidor público que, en el ejercicio de sus funciones, conozca de la comisión de un presunto delito contra la eficiencia de la administración pública.
2. Las o los profesionales de la salud de establecimientos públicos o privados, que conozcan de la comisión de un presunto delito.
3. Las o los directores, educadores u otras personas responsables de instituciones educativas, por presuntos delitos cometidos en dichos centros.

Artículo 427.- Formas de denuncia. - La denuncia podrá formularse verbalmente o por escrito.
Los escritos anónimos que no suministren evidencias o datos concretos que orienten la investigación se archivarán por la o el fiscal correspondiente.

Artículo 428.- Denuncia escrita. - La denuncia escrita será firmada por la o el denunciante. Si este último no sabe o no puede firmar, debe estampar su huella digital y una o un testigo firmará por ella o él.

Artículo 429.- Denuncia verbal. - Si la denuncia es verbal se sentará el acta respectiva, al pie de la cual firmará la o el denunciante. Si este último no sabe o no puede firmar, se sujetará a lo dispuesto en el artículo anterior.

TABLA 4

Denuncias receptadas en las Oficinas de Ministerio Público en Guayaquil

Otras Denuncias: *Año* 2013

Resumen de Totales

TOTALES	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA RESPECTO AL TOTAL DE DENUNCIAS
SUBTOTAL PRINCIPALES DELITOS DEL AÑO (se reporta en el sitio web)	14491(15247)	49,44%
OTRAS DENUNCIAS (no se reporta en el sitio web)	14822(15434)	50,56%
GRAN TOTAL DE DENUNCIAS DEL AÑO	***29313(30681)***	***100,00%***

NOTA: El total de "principales delitos" representa el 49,44% de todos los delitos denunciados durante el Año 2013
( ) Los valores entre paréntesis corresponden al año anterior (2012)

Fuente: Recuperado de http://www.icm.espol.edu.ec/delitos

3. ACUSACIÓN PARTICULAR

Artículo 432.- Acusación particular. - Podrá presentar acusación particular:

1. La víctima, por sí misma o a través de su representante legal, sin perjuicio de la facultad de intervenir en todas las audiencias y de reclamar su derecho a la reparación integral, incluso cuando no presente acusación particular.
2. La víctima, como persona jurídica podrá acusar por medio de su representante legal, quien podrá actuar por sí mismo o mediante procuradora o procurador judicial.
3. La víctima como entidad u organismo público, podrá acusar por medio de sus representantes legales o de sus delegados especiales y la o el Procurador General del Estado, para las instituciones que carezcan de personería jurídica, sin perjuicio de la intervención de la Procuraduría General del Estado.

En la delegación especial deberá constar expresamente el nombre y apellido de la persona procesada y acusada y la relación completa de la infracción con la que se le quiere acusar.

Artículo 369.- Delincuencia Organizada.- La persona que mediante acuerdo o concertación forme un grupo estructurado de dos o más personas que, de forma permanente o reiterada, financien de cualquier forma, ejerzan el mando o dirección o planifiquen las actividades de una organización delictiva, con el propósito de cometer uno o más delitos sancionados con pena privativa de libertad de más de cinco años, que tenga como objetivo final la obtención de beneficios económicos u otros de orden material, será sancionada con pena privativa de libertad de siete a diez años.

Los demás colaboradores serán sancionados con pena privativa de libertad de cinco a siete años.

Artículo 370.- Asociación Ilícita. - Cuando dos o más personas se asocien con el fin de cometer delitos, sancionados con pena privativa de libertad de menos de cinco años, cada una de ellas será sancionada, por el solo hecho de la asociación, con pena privativa de libertad de tres a cinco años.

PARÁGRAFO ÚNICO

Contravenciones contra el derecho de propiedad (CÓDIGO ORGÁNICO INTEGRAL PENAL)

Artículo 209.- Contravención de hurto. - En caso de que lo hurtado no supere el cincuenta por ciento de un salario básico unificado del trabajador en general, la persona será sancionada con pena privativa de libertad de quince a treinta días.

Para la determinación de la infracción se considerará el valor de la cosa al momento del apoderamiento.

Artículo 210.- Contravención de abigeato. - En caso de que lo sustraído no supere un salario básico unificado del trabajador en general, la persona será sancionada con pena privativa de libertad de quince a treinta días. Para la determinación de la infracción se considerará el valor de la cosa al momento del apoderamiento.

Artículo 196.- Hurto. - La persona que, sin ejercer violencia, amenaza o intimidación en la persona o fuerza en las cosas, se apodere ilegítimamente de cosa mueble ajena, será sancionada con pena privativa de libertad de seis meses a dos años.

Si el delito se comete sobre bienes públicos se impondrá el máximo de la pena prevista aumentada en un tercio. Para la determinación de la pena se considerará el valor de la cosa al momento del apoderamiento.

Artículo 189.- Robo. - La persona que mediante amenazas o violencias sustraiga o se apodere de cosa mueble ajena, sea que la violencia tenga lugar antes del acto para facilitarlo, en el momento de cometerlo o después de cometido para procurar impunidad, será sancionada con pena privativa de libertad de cinco a siete años.

Cuando el robo se produce únicamente con fuerza en las cosas, será sancionada con pena privativa de libertad de tres a cinco años.

Si se ejecuta utilizando sustancias que afecten la capacidad volitiva, cognitiva y motriz, con el fin de someter a la víctima, de dejarla en estado de somnolencia, inconciencia o indefensión o para obligarla a ejecutar actos que con conciencia y voluntad no los habría ejecutado, será sancionada con pena privativa de libertad de cinco a siete años.

Si a consecuencia del robo se ocasionan lesiones de las previstas en el numeral 5 del artículo 152 se sancionará con pena privativa de libertad de siete a diez años.

Si el delito se comete sobre bienes públicos, se impondrá la pena máxima, dependiendo de las circunstancias de la infracción, aumentadas en un tercio.

Si a consecuencia del robo se ocasiona la muerte, la pena privativa de libertad será de veintidós a veintiséis años.

La o el servidor policial o militar que robe material bélico, como armas, municiones, explosivos o equipos de uso policial o militar, será sancionado con pena privativa de libertad de cinco a siete años.

SECCIÓN NOVENA
Delitos contra el derecho a la propiedad

Artículo 185.- Extorsión. - La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

La sanción será de cinco a siete años si se verifican alguna de las siguientes circunstancias:

1. Si la víctima es una persona menor a dieciocho años, mayor a sesenta y cinco años, mujer embarazada o persona con discapacidad, o una persona que padezca enfermedades que comprometan su vida.
2. Si se ejecuta con la intervención de una persona con quien la víctima mantenga relación laboral, comercio u otra similar o con una persona de confianza o pariente dentro del cuarto grado de consanguinidad y segundo de afinidad.
3. Si el constreñimiento se ejecuta con amenaza de muerte, lesión, secuestro o acto del cual pueda derivarse calamidad, infortunio o peligro común.
4. Si se comete total o parcialmente desde un lugar de privación de libertad.
5. Si se comete total o parcialmente desde el extranjero.

Artículo 161.- Secuestro. - La persona que prive de la libertad, retenga, oculte, arrebate o traslade a lugar distinto a una o más personas, en contra de su voluntad, será sancionada con pena privativa de libertad de cinco a siete años.

Artículo 162.- Secuestro extorsivo. - Si la persona que ejecuta la conducta sancionada en el artículo 161 de este Código tiene como propósito cometer otra infracción u obtener de la o las víctimas o de terceras personas dinero, bienes, títulos, documentos, beneficios, acciones u omisiones que produzcan efectos jurídicos o que alteren de cualquier manera sus derechos a cambio de su libertad, será sancionado con pena privativa de libertad de diez a trece años.

Se aplicará la pena máxima cuando concurra alguna de las siguientes circunstancias:

1. Si la privación de libertad de la víctima se prolonga por más de ocho días.
2. Si se ha cumplido alguna de las condiciones impuestas para recuperar la libertad.

3. Si la víctima es una persona menor de dieciocho años, mayor de sesenta y cinco años, mujer embarazada o persona con discapacidad o que padezca enfermedades que comprometan su vida.
4. Si se comete con apoderamiento de nave o aeronave, vehículos o cualquier otro transporte.
5. Si se comete total o parcialmente desde el extranjero.
6. Si la víctima es entregada a terceros a fin de obtener cualquier beneficio o asegurar el cumplimiento de la exigencia a cambio de su liberación.
7. Si se ejecuta la conducta con la intervención de una persona con quien la víctima mantenga relación laboral, comercial u otra similar; persona de confianza o pariente dentro del cuarto grado de consanguinidad y segundo de afinidad.
8. Si el secuestro se realiza con fines políticos, ideológicos, religiosos o publicitarios.
9. Si se somete a la víctima a tortura física o psicológica, teniendo como resultado lesiones no permanentes, durante el tiempo que permanezca secuestrada, siempre que no constituya otro delito que pueda ser juzgado independientemente.
10. Si la víctima ha sido sometida a violencia física, sexual o psicológica ocasionándole lesiones permanentes.

Cuando por causa o con ocasión del secuestro le sobrevenga a la víctima la muerte, se sancionará con pena privativa de libertad de veintidós a veintiséis años.

4. GEOESTADÍSTICA Y EL ANÁLISIS ESPACIAL

La Geoestadística implica el análisis y la estimación de fenómenos espaciales o temporales, tales como: calidades de metal, porosidades.

La palabra Geoestadística es anormalmente asociada con geología, desde que esta ciencia tiene origines en minería.

Hoy en día la Geoestadística es un nombre asociado con una clase de técnicas, para analizar y predecir los valores de una variable que está distribuida en espacio o tiempo.
Se asume tales valores implícitamente, para ser puestos en correlación entre sí, y el estudio de semejante correlación normalmente se llama un análisis estructural o un “Variograma”. Después del análisis estructural, se hacen estimaciones a las situaciones de los sectores no muestreados usando la técnica de Interpolación “Kriging”.
La Geoestadística, tiene como objetivo el caracterizar o interpretar el comportamiento de los datos que están distribuidos como “variables regionalizadas”.

1º) Análisis exploratorio de los datos:

En esta fase se estudian los datos muestrales sin tener en cuenta su distribución geográfica. Sería una etapa de aplicación de la estadística. Se comprueba la consistencia de los datos, eliminándose aquellos que sean erróneos, y se identifican las distribuciones de las cuales provienen.

2º) Análisis estructural:

Se estudia la continuidad espacial de la variable. En esta etapa se calcula el Variograma experimental, o cualquier otra función que nos explique la variabilidad espacial, se ajusta al mismo un Variograma teórico y se analiza e interpreta dicho ajuste al modelo paramétrico seleccionado.

3º) Predicciones:

Estimaciones de la variable en los puntos no muestrales, considerando la estructura de correlación espacial seleccionada e integrando la información obtenida de forma directa, en los puntos muestrales, así como la conseguida indirectamente en forma de tendencias conocidas u observadas. También se pueden realizar simulaciones, teniendo en cuenta los patrones de continuidad espacial elegidos.
Para la determinación del Variograma experimental deben cumplirse una serie de etapas.

Se calcula un Variograma onidireccional, se define como un Variograma válido para todas las direcciones, o como aquel en el cual la tolerancia direccional es de 360º. Evidentemente, este Variograma será función sólo de la distancia, h. Se puede considerar, no muy estrictamente, como un Variograma medio para todas las direcciones.

Sin embargo, el cálculo de un Variograma omnidireccional no significa que la continuidad espacial sea idéntica en todas las direcciones. Simplemente constituye el inicio del análisis estructural, sirviendo para determinar los parámetros relacionados con la distancia que generan los mejores resultados, ya que no depende de la dirección.

Son varios los paquetes de software, que proporciona ayuda para desarrollar análisis de datos espaciales, muchos de estos paquetes proporcionan los cálculos tradicionales Estadísticos, como son análisis Univariado, gráficos de histogramas, gráficos de correlación; además de las técnicas básicas, que conforman el análisis Geoestadístico.

Descripción de los Software a utilizar.

Para el desarrollo del análisis se utilizó el Software Variowin en la elaboración de modelos para Variogramas Versión 2.2 (2003), y además se recurrió al software SADA, como soporte para la elección del mejor modelo que describa el comportamiento de las variables de interés

Variowin 2.2

Análisis espacial Variowin 2.21, elaboración de modelos para Variogramas común.

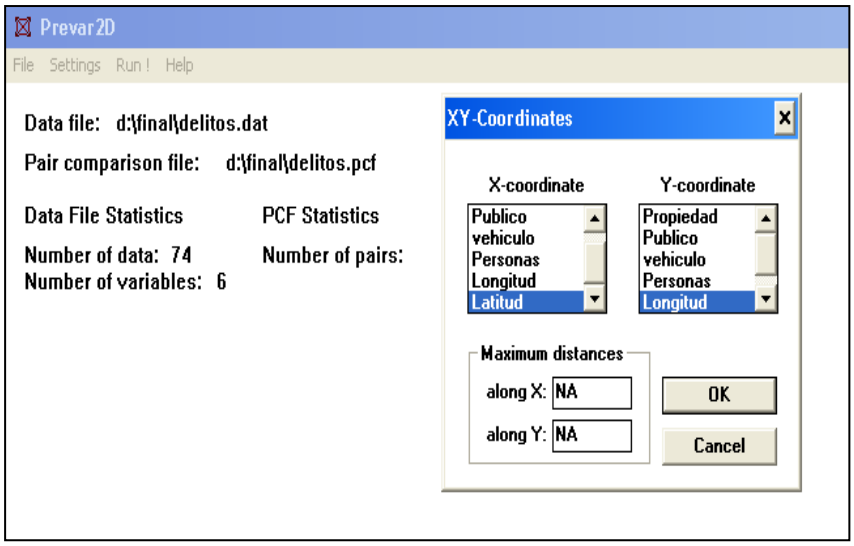
Opera como un banco de datos geográficos sin fronteras y soporta un gran volumen de datos (sin limitaciones de escala, proyección y huso), manteniendo la identidad de los objetos geográficos a lo largo de todo banco.

Proporciona un ambiente de trabajo amigable y poderoso, a través de la combinación de menús y ventanas con un lenguaje espacial fácilmente programable por el usuario.

Módulos del Variowin 2.21:

Prevar2D. Se crea un archivo.dat con todos los datos georreferenciados y se establece los parámetros de longitud y latitud para poder crear otro archivo pcf para el cálculo geoestadístico.

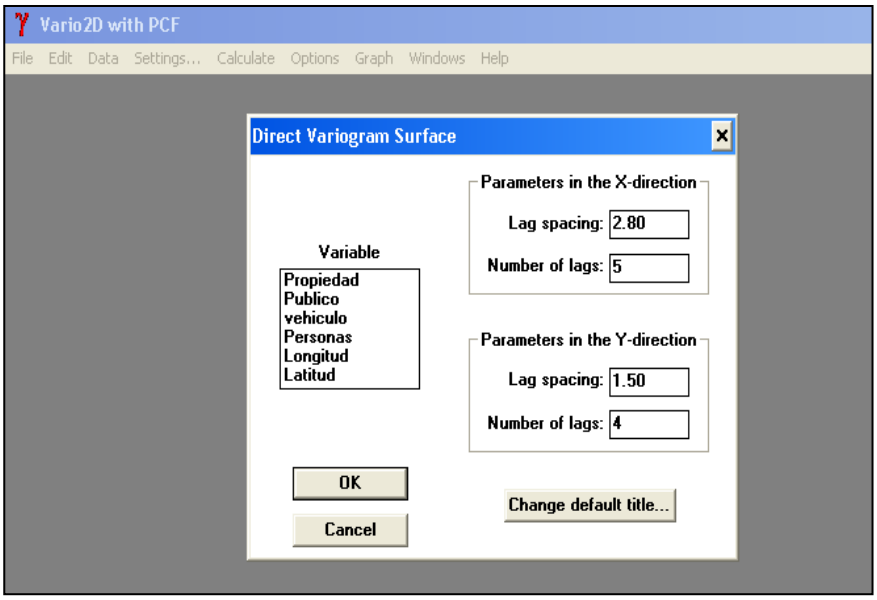
Gráfico 2.1. Corrida del módulo Prevar2D



Fuente: Variowin 2.2

Vario2D with PCF. Trabaja con un archivo.pcf que se crea en el módulo prevar2d al momento de ejecutarlo el cual permite efectuar los cálculos de las estimaciones geoestadísticas.

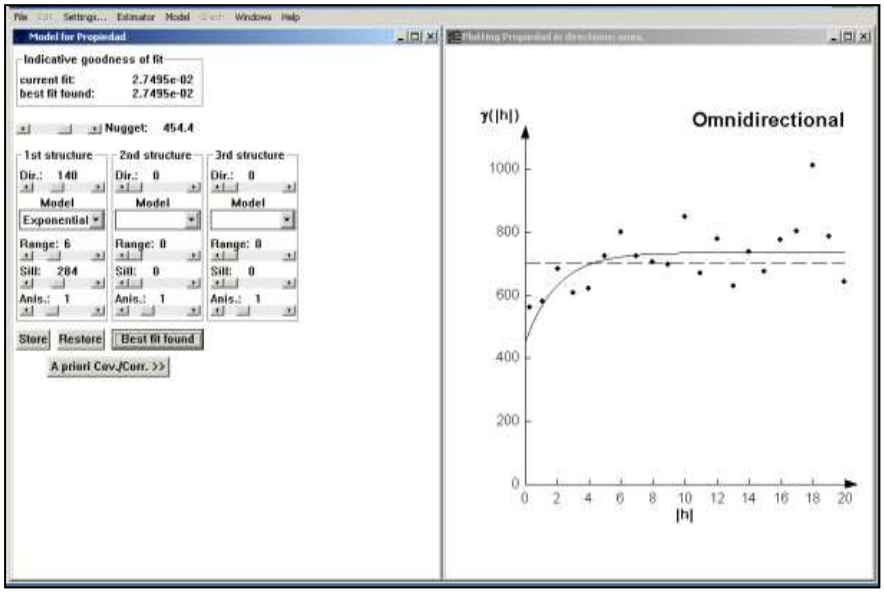
Gráfico 2.2. Corrida del módulo Vario2D With PCF



Fuente: Variowin 2.2

Model. Trabaja con un archivo. var que se crea en el módulo Vario2D with pcf y permite calcular los diferentes modelos geoestadíscos y obtener el mejor modelo.

Gráfico 2.3. Corrida del módulo Model

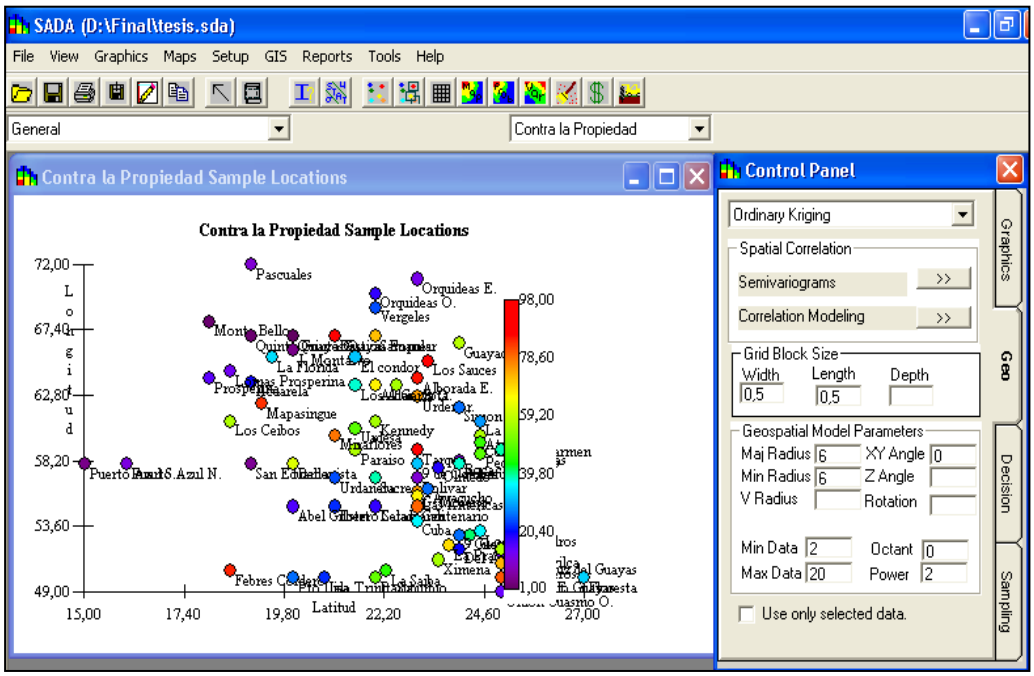


Fuente: Variowin 2.2

SADA

Análisis espacial y Ayuda de Decisión (SADA) direcciones que la valoración medioambiental. Para alcanzar estos objetivos, el SADA se basa en un modelo de datos orientado a objetos, del cual se derivada su interfaz de menús y el lenguaje espacial. Algoritmos innovadores, como los utilizados para indexación espacial, segmentación de imágenes y creación de retículas, garantizan el desempeño adecuado en las más diversas aplicaciones. Estos estudios incluyen: Datos Exploración y Visualización, Sistema de Información Geográfico, Análisis, Decisión,

Gráfico 2.4. Corrida del módulo Sada



Fuente: Sada

DATOS DEL ESTUDIO

Área de estudio. Comprende la jurisdicción del Cantón Guayaquil, con una superficie aproximada de 600.000 hectáreas, situada entre 1°55’ y 3°10’ de latitud Sur y 79°40’ y 80°30’ de longitud Oeste.

Área: Indica el nombre del proyecto en estudio, en este caso Proyecto Análisis Espacial de la Distribución de la Delincuencia en Guayaquil.

Delito: Este dato muestra el nombre de la persona responsable de realizar el acto delictivo en un espacio determinado.

Zona: Esta información se define el nombre de la zona de estudio, que adopta los nombres de los tipos de delitos.

CUADRO 2

Denuncias receptadas en las Oficinas de Ministerio Público en Guayaquil

TASAS DE DELITOS POR CADA CIEN MIL HABITANTES
CIUDAD GUAYAQUIL DEL AÑO 2005 AL 2013

Principales Delitos contra las Personas

DELITO	AÑO 2005	AÑO 2006	AÑO 2007	AÑO 2008	AÑO 2009	AÑO 2010	AÑO 2011	AÑO 2012	AÑO 2013
Homicidio	14,05	14,73	9,71	11,05	21,74	21,82	13,48	7,58	5,47
Plagio	38,06	30,85	26,17	28,41	32,92	18,54	13,57	11,72	7,41
Robo Agravado	137,3	249,35	226,99	199,92	336,12	424,13	359,15	300,61	268,78
Secuestro Express	9,77	13,66	9,98	8,66	12,42	14,03	10,33	9,42	7,45
Violación	29,98	21,52	21,7	22,65	29,28	30,82	24,03	17,00	19,24

Principales Delitos contra la Propiedad

DELITO	AÑO 2005	AÑO 2006	AÑO 2007	AÑO 2008	AÑO 2009	AÑO 2010	AÑO 2011	AÑO 2012	AÑO 2013
Robo Simple	720,33	485,80	355,65	318,74	200,58	164,77	87,00	103,02	125,21
Hurto	132,24	101,17	53,06	53,41	26,49	58,02	73,77	59,56	77,93
Robo en Domicilio	35,09	59,47	49,93	51,92	66,77	63,53	54,76	63,01	48,04
Robo de Vehículos	124,12	108,31	118,51	150,26	169,48	126,24	62,19	54,62	34,36
Robo en Local Comercial	24,6	42,95	39,99	39,72	50,27	34,63	21,26	22,96	16,13
Robo en Banco	0,09	0,22	0,13	0,30	0,09	0,17	0,04	0,09	0,08

Fuente: Recuperado de http://www.icm.espol.edu.ec/delitos

En la descripción de la clasificación de los departamentos judiciales donde se asienta la denuncia por tipo de delito, se cuentan con varios datos que fueron observadas y determinadas en el momento del levantamiento de la información.

Para la obtención de los datos del espacio físico en la ciudad de Guayaquil, se hace un reconocimiento de la zona de interés, se cuentan con tomas aéreas de los sectores que componen el área de estudio, para determinar la estructura geográfica de la que está compuesta, luego se prosigue a determinar la técnica de recolección de los datos y conjuntamente a determinar la localización exacta de cada unidad de observación, se obtiene la ubicación geográfica del delito en general.

CUADRO 3

Denuncias receptadas en las Oficinas de Ministerio Público en Guayaquil

PORCENTAJES DE VARIACIÓN RESPECTO AL AÑO ANTERIOR

AÑO 2013 RESPECTO AL AÑO 2012

Principales Delitos contra las PERSONAS

PRINCIPALES DELITOS CONTRA LAS PERSONAS	TASA DE DELITOS POR CADA CIEN MIL HAB. AÑO 2012	TASA DE DELITOS POR CADA CIEN MIL HAB. AÑO 2013	DIFERENCIA	PORCENTAJE DE VARIACIÓN
Homicidio	7,58	5,47	-2,11	-27,79%
Plagio	11,72	7,41	-4,31	-36,77%
Robo agravado	300,61	268,78	-31,83	-10,59%
Secuestro express	9,42	7,45	-1,97	-20,89%
Violación*	17,00	19,24	2,24	13,18%

Fuente: Población urbana estimada de Guayaquil a 2012: 2'375.168 hab.
Población urbana estimada de Guayaquil a 2011: 2'347.205 hab

Principales Delitos contra las PROPIEDAD

PRINCIPALES DELITOS CONTRA LA PROPIEDAD	TASA DE DELITOS POR CADA CIEN MIL HAB. AÑO 2012	TASA DE DELITOS POR CADA CIEN MIL HAB. AÑO 2013	DIFERENCIA	PORCENTAJE DE VARIACIÓN
Robo simple	103,02	125,21	22,19	21,54%
Hurto	59,56	77,93	18,37	30,85%
Robo en domicilio	63,01	48,04	-14,97	-23,76%
Robo de vehículos	54,62	34,36	-20,26	-37,10%
Robo en local comercial	22,96	16,13	-6,83	-29,77%
Robo en Banco	0,09	0,08	-0,01	-6,44%

Fuente: Recuperado de http://www.icm.espol.edu.ec/delitos

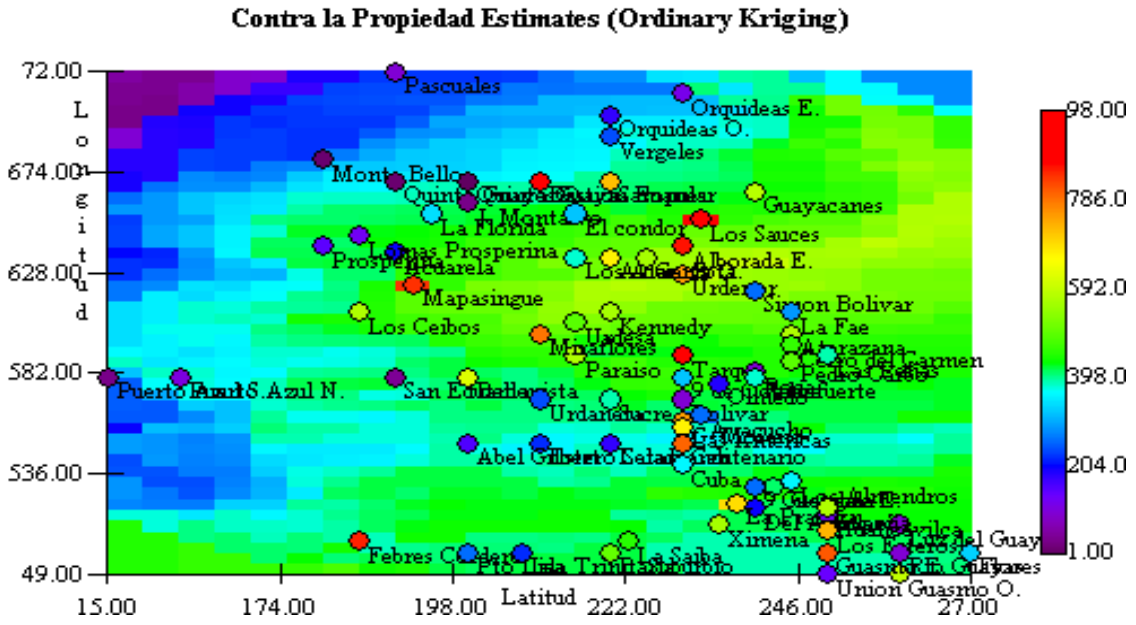
ANÁLISIS DE LA VARIABILIDAD ESPACIAL.

En este análisis, se determina el comportamiento espacial que presentan cada uno de los delitos, este comportamiento se lo representa por medio de un ajuste a los modelos teóricos antes detallados, una vez determinados los modelos se procede a realizar las estimaciones para el nivel de concentración en el mapa, y poder así tener un mejor conocimiento de las características que describen la zona de la ciudad de Guayaquil. Para determinar el modelo de Variograma que mejor.

DELITO CONTRA LA PROPIEDAD

Robo a personas, estruches (robo a casa, departamento), robo a locales comerciales, hurto, robo a transporte urbano colectivos.

Gráfico 2.5. Parroquias de la Ciudad de Guayaquil según su composición delitos contra la propiedad año 2013

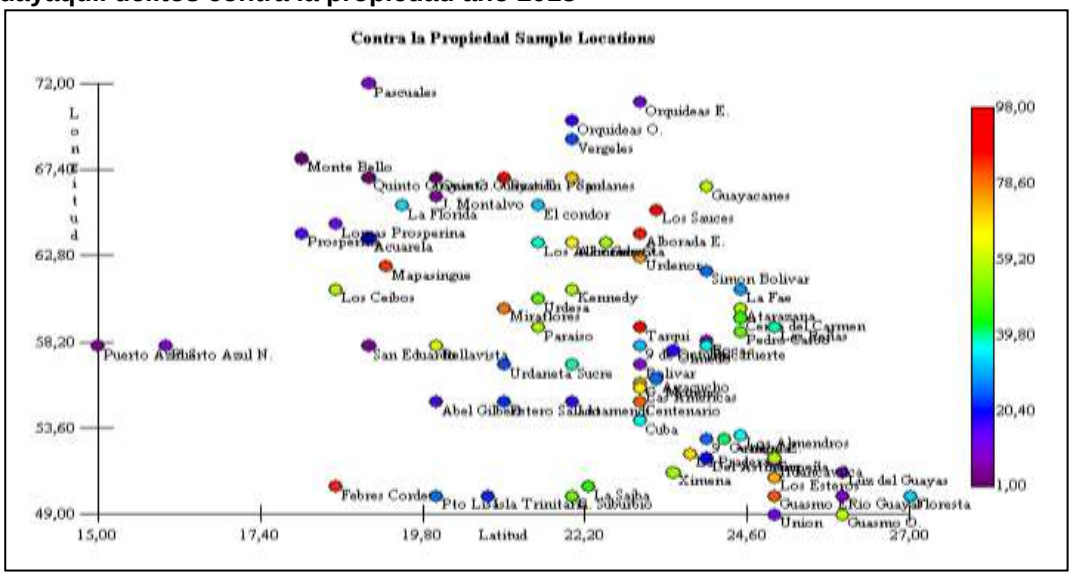


Fuente: Policía Judicial del Guayas
Elaborado: SADA

Esta división y polarización coincide a grandes rasgos con la distribución desigual de activos existente en el espacio urbano y con el mapa de factores de riesgos sociales de la ciudad. Aquellas zonas más vulnerables a los delitos contra las propiedades tenemos las parroquias Febrescordero, Tarqui, Mapasingue, Bastión Popular y las ciudadelas de la Alborada y Sauces, son las que precisamente presentan las mayores tasas de delincuencia.

Se define como un Variograma válido para todas las direcciones, o como aquel en el cual la tolerancia direccional es de 0º y 90º. Evidentemente, este Variograma será función sólo de la distancia, h. Se puede considerar, no muy estrictamente, como un Variograma medio para todas las direcciones.

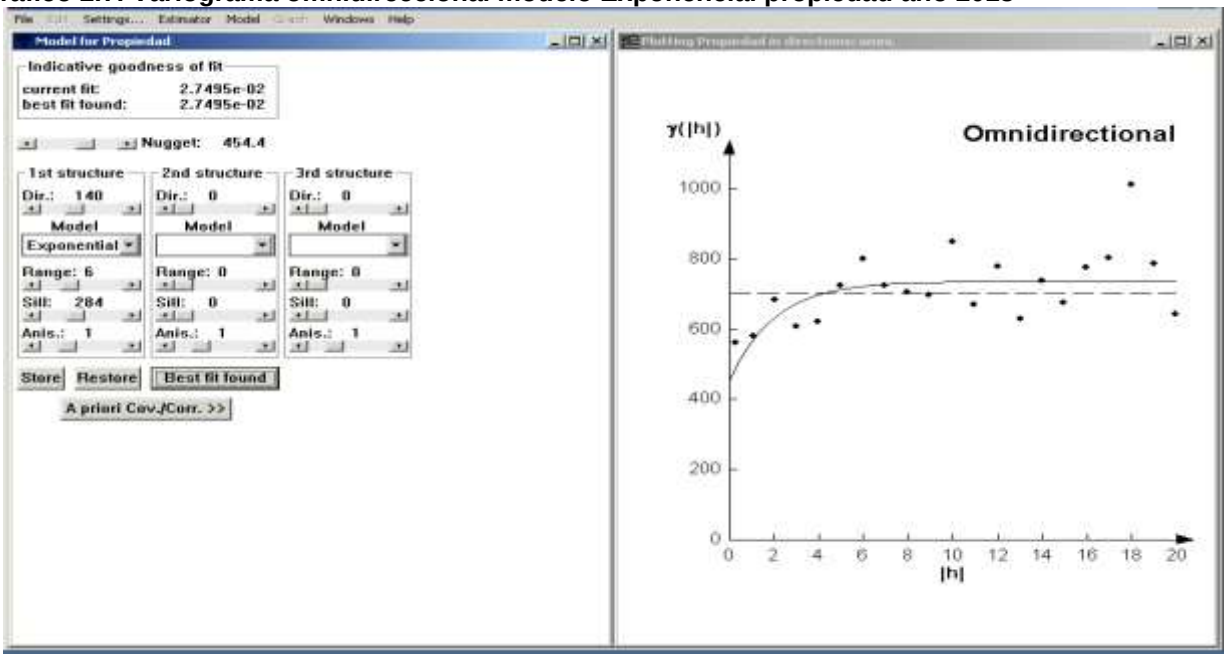
Gráfico 2.6. Mapa de posicionamiento de las observaciones georeferenciadas en la ciudad de Guayaquil delitos contra la propiedad año 2013



Fuente: Policía Judicial del Guayas
Elaborado: SADA

La correlación entre los delitos permite captar los distintos patrones de asociación espacial existentes entre las unidades bajo estudio. La gráfica muestra la relación existente entre los diferentes delitos dentro de la ciudad de Guayaquil correspondiente al área urbana.

Gráfico 2.7. Variograma omnidireccional modelo Exponencial propiedad año 2013



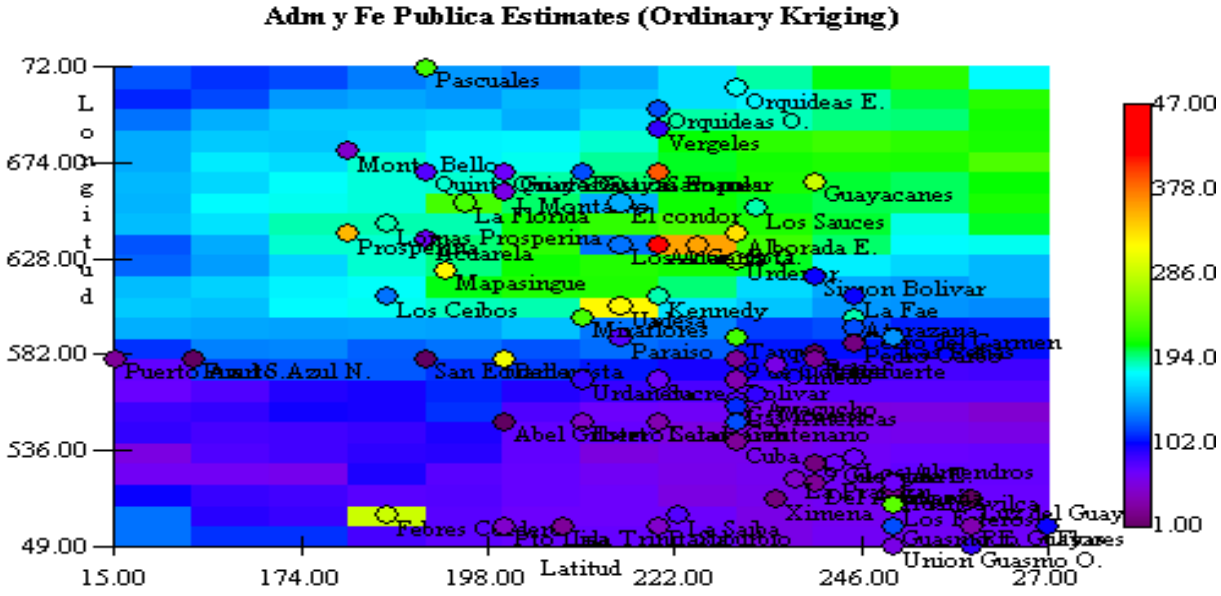
Fuente: Variowin 2.2

Para obtener el mejor modelo omnidireccional, se tiene los parámetros de Nugget de 454.4, su estructura se define con una dirección de 140, rango de 6 y un sill de 284, ya que influirá muy notablemente en los patrones de distribución que se obtengan, el mejor modelo de esta variable de investigación es el modelo Exponencial.

DELITO A LA ADMINISTRACION Y FE PÚBLICA

Estafas, falsificación de firma.

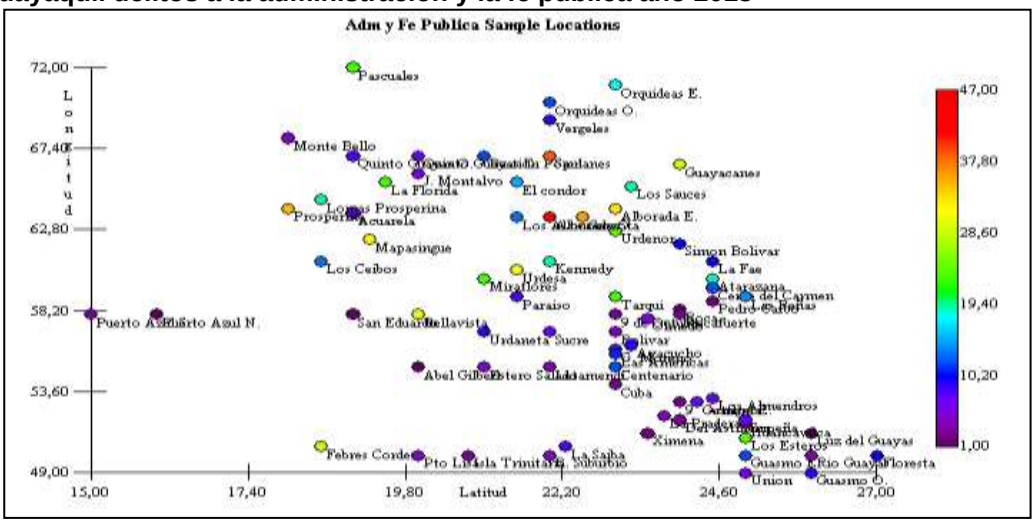
Gráfico 2.8. Parroquias de la Ciudad de Guayaquil según su composición delitos a la administración y la fe pública año 2013



Fuente: Policía Judicial del Guayas
Elaborado: SADA

Esta división y polarización coincide a grandes rasgos con la distribución desigual de activos existente en el espacio urbano y con el mapa de factores de riesgos sociales de la ciudad. Delitos a la administración y fe pública se presentan con más intensidad en los sauces aquellas zonas son más céntricas.

Gráfico 2.9. Mapa de posicionamiento de las observaciones georeferenciadas en la ciudad de Guayaquil delitos a la administración y la fe pública año 2013

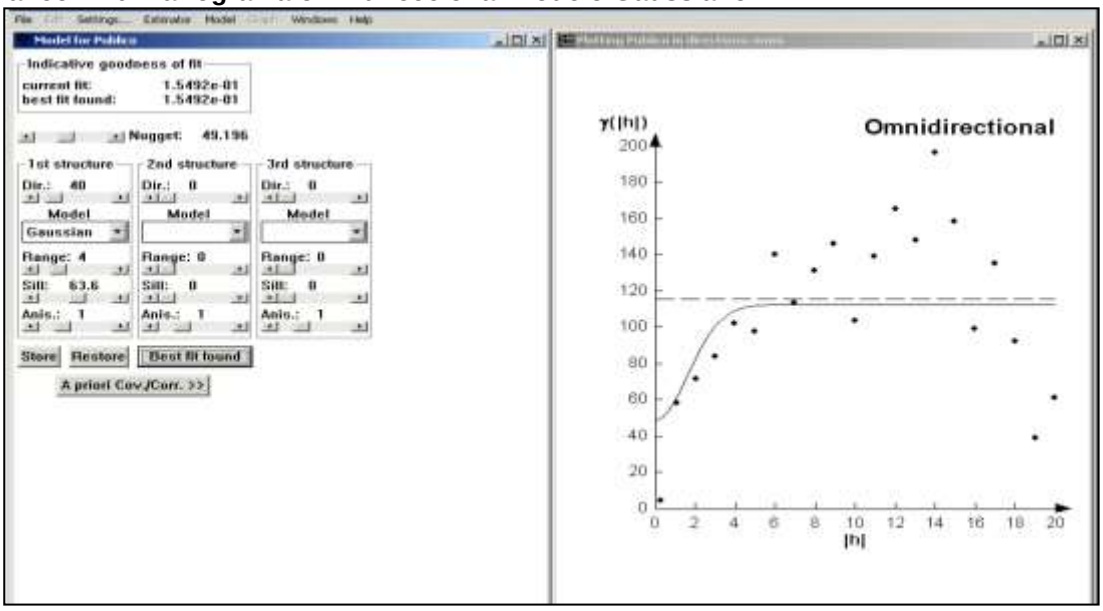


Fuente: Policía Judicial del Guayas
Elaborado: SADA

Es necesario que el Variograma que se elija refleje el patrón de continuidad espacial de la variable analizada.

La gráfica muestra la relación existente entre los diferentes delitos dentro de la ciudad de Guayaquil correspondiente al área urbana. Cada punto se ubica en el plano referencial por cada cuadricula del mapa. Así, el plano está formado por cuadrantes donde existen puntos en los cuales la tasa de delitos se muestra por puntos en cada parte de la ciudad.

Gráfico 2.10. Variograma omnidireccional modelo Gaussiano

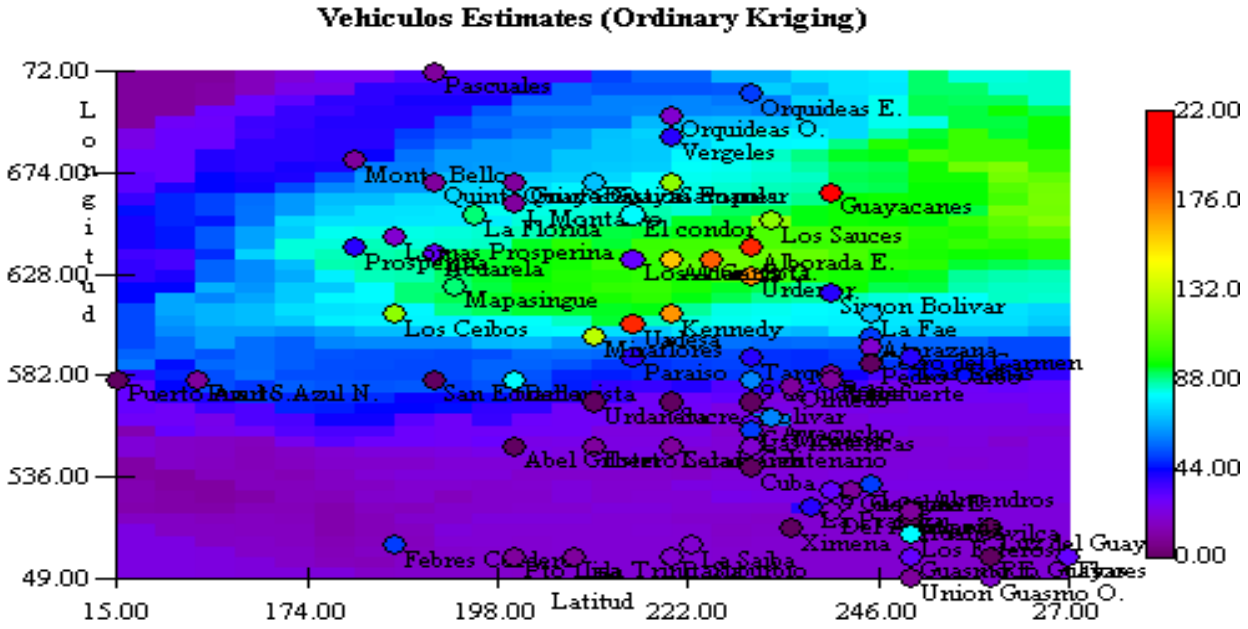


Fuente: Variowin 2.2

Para obtener el mejor modelo omnidireccional, se tiene los parámetros de Nugget de 49.196, su estructura se define con una dirección de 40, rango de 4 y un sill de 63.6, ya que influirá muy notablemente en los patrones de distribución que se obtengan, el mejor modelo de esta variable de investigación es el modelo Gaussiano.

VEHICULOS
Asalto y robo de carros

Gráfico 2.11. Parroquias de la Ciudad de Guayaquil según su composición delitos contra los vehículos año 2013

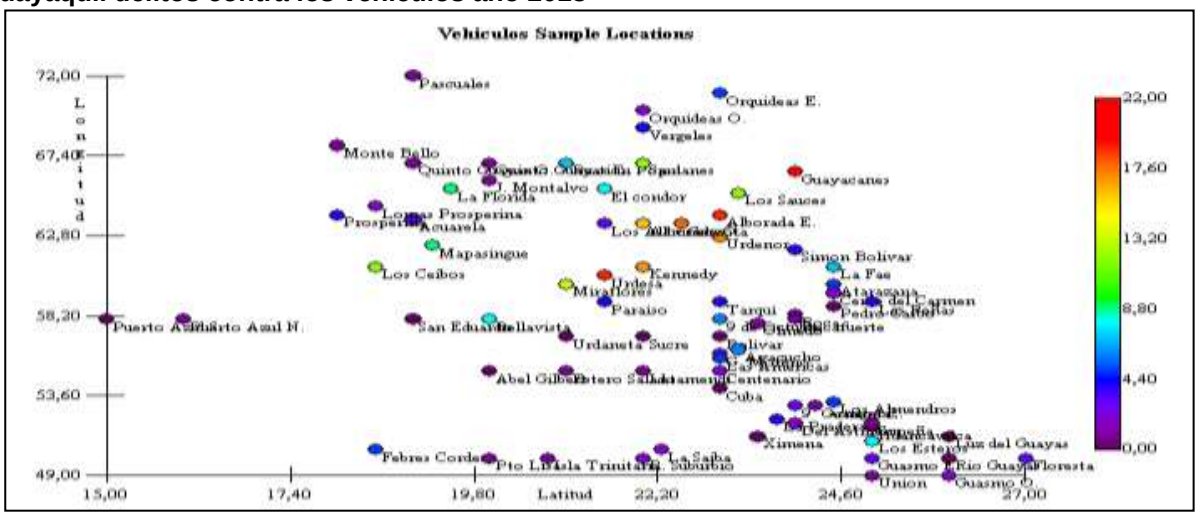


Fuente: Policía Judicial del Guayas
Elaborado: SADA

Aquellas zonas como los Sauces, Alborada Guayacanes y Urdesa que están en el sector norte de la ciudad son las que precisamente presentan las mayores tasas de delincuencia en lo que a robo de vehículos se refiere, siendo estas de nivel socio económico más alto.

El cálculo de un Variograma omnidireccional no significa que la continuidad espacial sea idéntica en todas las direcciones.

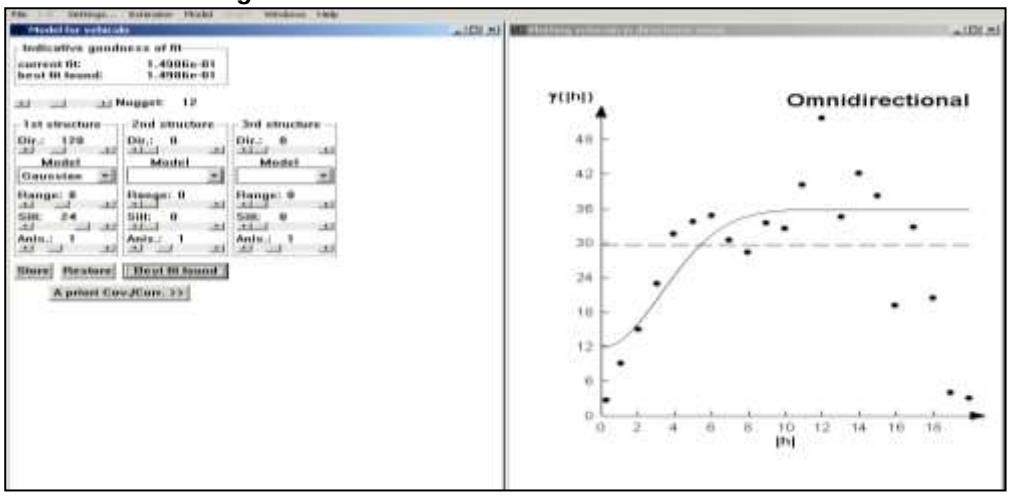
Gráfico 2.12. Mapa de posicionamiento de las observaciones georeferenciadas en la ciudad de Guayaquil delitos contra los vehículos año 2013



Fuente: Policía Judicial del Guayas
Elaborado: SADA

La gráfica muestra la relación existente entre los diferentes delitos dentro de la ciudad de Guayaquil correspondiente al área urbana. Cada punto se ubica en el plano referencial por cada cuadricula del mapa. Así, el plano está formado por cuadrantes donde existen puntos en los cuales la tasa de delitos se muestra por puntos en cada parte de la ciudad.

Gráfico 2.13. Variograma omnidireccional modelo Gaussiano



Fuente: Variowin 2.2

Para obtener el mejor modelo omnidireccional, se tiene los parámetros de Nugget de 12, su estructura se define con una dirección de 120, rango de 6 y un sill de 24, ya que influirá muy notablemente en los patrones de distribución que se obtengan, el mejor modelo de esta variable de investigación es el modelo Gaussiano

DELITOS CONTRA LAS PERSONAS

Homicidios, violación, tenencia ilegal arma de fuego, delitos varios contra la inviolabilidad de la vida

Artículo 140.- Asesinato. - La persona que mate a otra será sancionada con pena privativa de libertad de veintidós a veintiséis años, si concurre alguna de las siguientes circunstancias:

1. A sabiendas, la persona infractora ha dado muerte a su ascendiente, descendiente, cónyuge, conviviente, hermana o hermano.
2. Colocar a la víctima en situación de indefensión, inferioridad o aprovecharse de esta situación.
3. Por medio de inundación, envenenamiento, incendio o cualquier otro medio se pone en peligro la vida o la salud de otras personas
4. Buscar con dicho propósito, la noche o el despoblado.
5. Utilizar medio o medios capaces de causar grandes estragos.
6. Aumentar deliberada e inhumanamente el dolor a la víctima.
7. Preparar, facilitar, consumar u ocultar otra infracción.
8. Asegurar los resultados o impunidad de otra infracción.
9. Si la muerte se produce durante concentraciones masivas, tumulto, conmoción popular, evento deportivo o calamidad pública.
10. Perpetrar el acto en contra de una o un dignatario o candidato a elección popular, elementos de las Fuerzas Armadas o la Policía Nacional, fiscales, jueces o miembros de la Función Judicial por asuntos relacionados con sus funciones o testigo protegido.

Art.144.- Homicidio. - La persona que mate a otra será sancionado con pena privativa de libertad de diez a trece años.

Artículo 143.- Sicariato. - La persona que mate a otra por precio, pago, recompensa, promesa remuneratoria u otra forma de beneficio, para sí o un tercero, será sancionada con pena privativa de libertad de veintidós a veintiséis años.
La misma pena será aplicable a la persona, que en forma directa o por intermediación, encargue u ordene el cometimiento de este ilícito.

Artículo 171.- Violación. - Es violación el acceso carnal, con introducción total o parcial del miembro viril, por vía oral, anal o vaginal; o la introducción, por vía vaginal o anal, de objetos, dedos u órganos distintos al miembro viril, a una persona de cualquier sexo.

Quien la comete, será sancionado con pena privativa de libertad de diecinueve a veintidós años en cualquiera de los siguientes casos:

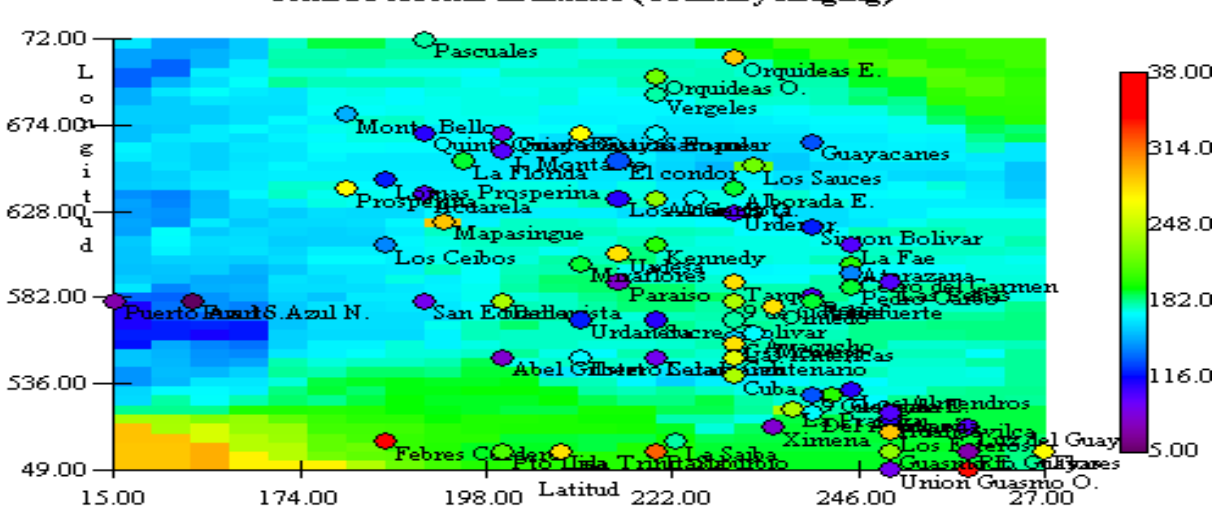
1. Cuando la víctima se halle privada de la razón o del sentido, o cuando por enfermedad o por discapacidad no pudiera resistirse.
2. Cuando se use violencia, amenaza o intimidación.
3. Cuando la víctima sea menor de catorce años.

Se sancionará con el máximo de la pena prevista en el primer inciso, cuando:

1. La víctima, como consecuencia de la infracción, sufre una lesión física o daño psicológico permanente.
2. La víctima, como consecuencia de la infracción, contrae una enfermedad grave o mortal.
3. La víctima es menor de diez años.
4. La o el agresor es tutora o tutor, representante legal, curadora o curador o cualquier persona del entorno íntimo de la familia o del entorno de la víctima, ministro de culto o profesional de la educación o de la salud o cualquier persona que tenga el deber de custodia sobre la víctima.
5. La o el agresor es ascendiente o descendente o colateral hasta el cuarto grado de consanguinidad o segundo de afinidad.
6. La víctima se encuentre bajo el cuidado de la o el agresor por cualquier motivo.

En todos los casos, si se produce la muerte de la víctima se sancionará con pena privativa de libertad de veintidós a veintiséis años.

Gráfico 2.14. Parroquias de la Ciudad de Guayaquil según su composición delitos contra las personas año 2013

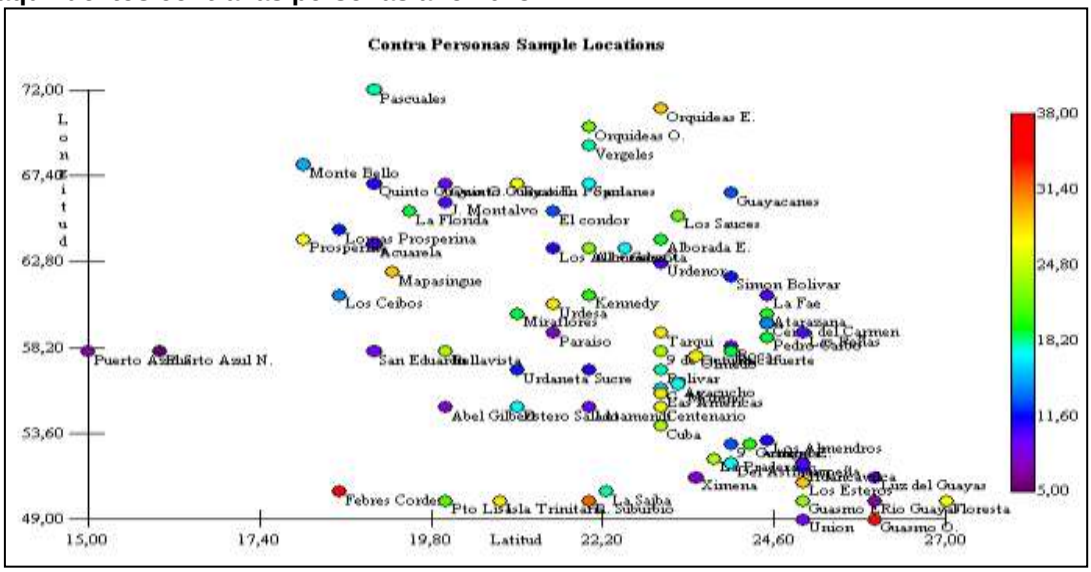


Fuente: Policía Judicial del Guayas
Elaborado: SADA

Aquellas zonas más vulnerables y pobres, como los Guasmos y Febrescordero son las que precisamente presentan las mayores tasas de delincuencia y un mayor índice en tenencias de armas de fuego, para seguridad o sea estas por las pandillas.

El inicio del análisis estructural, válido para todas las direcciones, o como aquel en el cual la tolerancia direccional es de 0º y 90. Esos parámetros serán el incremento de la distancia y la tolerancia dimensional, el cálculo de un Variograma omnidireccional no significa que la continuidad espacial sea idéntica en todas las direcciones.

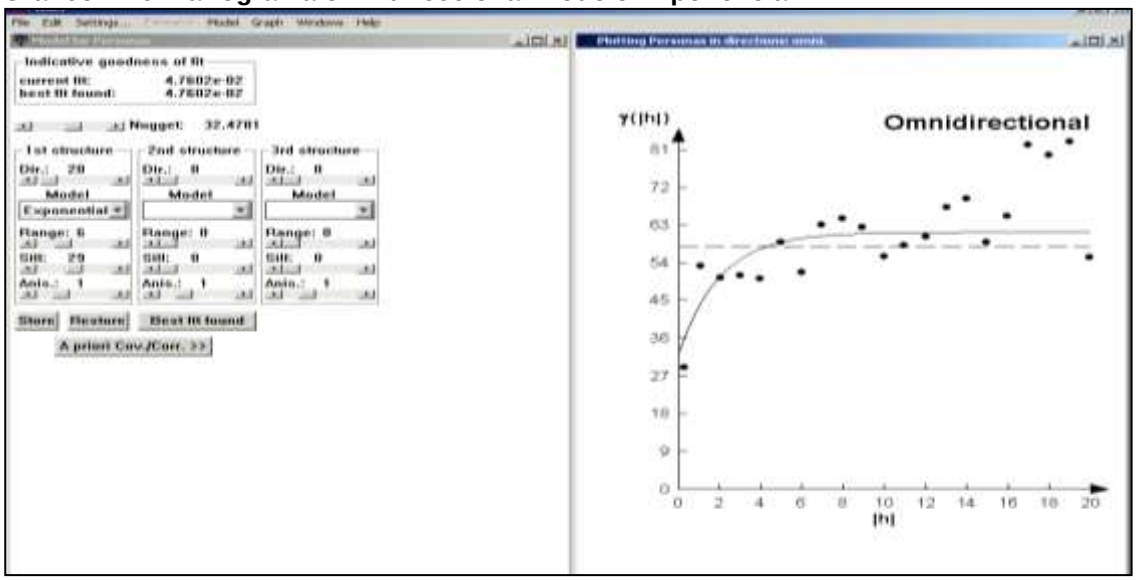
Gráfico 2.15. Mapa de posicionamiento de las observaciones georeferenciadas en la ciudad de Guayaquil delitos contra las personas año 2013



Fuente: Policía Judicial del Guayas
Elaborado: SADA

La gráfica muestra la relación existente entre los diferentes delitos dentro de la ciudad de Guayaquil correspondiente al área urbana. Cada punto se ubica en el plano referencial por cada cuadrícula del mapa.

Gráfico 2.16. Variograma omnidireccional modelo Exponencial



Fuente: Variowin 2.2

Para obtener el mejor modelo omnidireccional, se tiene los parámetros de Nugget de 32.4781, su estructura se define con una dirección de 20, rango de 6 y un sill de 29, ya que influirá muy notablemente en los patrones de distribución que se obtengan, el mejor modelo de esta variable de investigación es el modelo Exponencial.

CAPÍTULO III.- EL PHISHING COMO NUEVA MODALIDAD DE FRAUDE EN LA ERA DIGITAL

Autores: Carlos Alcívar Trejo, Mgs.
Coordinador Académico y Docente de la Facultad de Derecho de la Universidad Tecnológica ECOTEC

Juan Tarquino Calderón Cisneros, Mgs.
Docente Titular de la Facultad de Ciencias de la Salud de la Universidad Estatal de Milagro (UNEMI).

INTRODUCCIÓN

El proceso de revisar tu estado de cuenta bancaria, cambio de contraseñas, transacciones de dinero y mucho más ha sido un beneficio de las entidades bancarias hacia sus clientes pero una de las desventajas para estos procesos es el tiempo ya que para realizar cada uno de ellas se debería de disponer un tiempo específico para acercarse al banco, como nuestra sociedad ha ido creciendo a pasas agigantados en cuanto al mundo tecnológico los propietarios de las cuentas bancarias ya sean estas cuentas corrientes o cuentas de ahorros, cada vez tienen menos tiempo para poderse acercar a las entidades a realizar sus transacciones debido a sus múltiples ocupaciones.

Por tal motivo aproximadamente desde hace 5 años se ha venido realizando este tipo de transacciones de manera online la cual permite al usuario que desde cualquier parte del mundo pueda tener acceso a la información de su cuenta bancaria y también realizar consultas online con servicio al cliente y realizar transacciones bancarias en menor tiempo y sin interrumpir sus labores cotidianas. En el siguiente texto se describirá el delito informático que se comete contra la información bancaria y la manera de hacer phishing en contra de una entidad bancaria.

EL término phishing fue creado a mediados de los años 90 y proviene de la palabra inglesa “fishing” que significa pesca, esto hacía alusión a que la persona que lo realizaba lo que pretendía es que el dueño de la cuenta pueda morder el anzuelo, y la persona que realiza esta actividad se lo llama phisher(etapa,2016).

El término phishing fue creado por crackers que intentaban obtener las contraseñas de los miembros de AOL para utilizarlas con propósitos específicos como eran: usar los servicios de la compañía AOL a través de números de tarjetas de crédito.

El phishing en AOL estaba relacionado con la comunidad warez que se dedicaba a intercambiar softwares falsificados (etapa, 2016). El phisher una vez que ya había obtenido el código de acceso al sistema como trabajador de la compañía AOL lo que hacía era enviar correo a las víctimas que ya se habían establecido con el fin de que la víctima diera información relevante para ellos. Una vez que el usuario enviaba su contraseña el phisher podía tener acceso a la cuenta de la víctima y utilizarla para diferentes delitos y beneficio propio.

En 1997 la compañía AOL reforzó su política de seguridad con respecto al phishing y los warez por la cual fueron expulsados de los servidores de la compañía además de eso ellos como seguridad en el sistema de mensajería incluyeron un mensaje que decía (<<Nadie que trabaje en AOL le pedirá su contraseña o información de facturación >>) y desactivaban las cuentas que habían sido inmersas en phishing de manera automática antes de que las víctimas respondieras los mensajes fraudulentos.

De acuerdo con el informe anual "Fraudes en Línea al Consumidor en Instituciones Financieras", elaborado por RSA, la división de Seguridad de la empresa EMC, el 82 por ciento de los titulares de cuentas son menos propensos a responder un correo electrónico de su banco debido a las estafas de phishing.

Para evitar ser víctimas de un fraude electrónico, el 91 por ciento de los titulares de cuentas bancarias encuestados están dispuestos a utilizar un nuevo método de autenticación más allá del usuario y contraseña.

Sin embargo, la confianza de los usuarios en la banca electrónica sigue disminuyendo, ya que ahora están más conscientes de las amenazas.

Al menos el 70 por ciento de los encuestados está familiarizado con el término phishing, en tanto que el 44 por ciento mostró una preocupación ante el incremento de otro tipo de ataques con virus o troyanos.

Buscan otra protección

Aunque el 90 por ciento de los usuarios encuestados están dispuestos a utilizar un método de seguridad distinto a las contraseñas, las preferencias varían pues van desde dispositivos tokens, imágenes personalizadas y autenticación basada en el riesgo.

El 73 por ciento se inclinó por el uso de autenticación basada en el riesgo, que implica una evaluación de la identidad del usuario incluyendo la ubicación de conexión al sistema, dirección de internet y comportamiento de la transacción.

“Para el 2007 la firma prevé que la seguridad de la banca en línea evolucione, pero al mismo tiempo esperan un incremento en las amenazas informáticas”. (Valencia, 2007, p.7)

El delito informático produce un impacto económico negativo: no solo el daño directo para el que sufre o asume la estafa, sino también las pérdidas derivadas de la erosión de la imagen del suplantado; ambas provocan un impacto social, que se traduce en un freno al desarrollo de la Sociedad de la Información.

• El spam o mensajes de correo electrónico no solicitados que son enviados en cantidades masivas a un número muy amplio de usuarios suponen, en muchos casos, la cabeza de puente para la comisión de un fraude electrónico (phishing, scam, “cartas nigerianas”, bulos, etc.).

Observatorio de la Seguridad de la Información

• Una primera clasificación distinguiría entre los delitos que tienen su origen en técnicas de ingeniería social y los que tratan de aprovecharse de vulnerabilidades de los sistemas. No obstante, en algunos ciberdelitos se combinan ambos orígenes.

Siguiendo el Código Penal español de 1995, se distingue entre los supuestos basados en técnicas de ingeniería social, que son tipificados en el mismo apartado que las estafas tradicionales (Art. 248.1 Código Penal), y los supuestos de utilización de código malicioso (malware) o de intrusión en sistemas de información recogidos en el artículo 248.2 del CP.

Dentro del primer grupo se encuentran algunas de las estafas tradicionales “puestas al día” para el mundo Internet. Forman parte del segundo grupo aquellos fraudes que utilizan códigos maliciosos o métodos de intromisión ilegal en los sistemas de información, por lo que es normalmente necesaria, una mayor habilidad técnica por parte del ciberdelincuente. (INTECO, 2007)

Definición de Delito Informático

Aunque no hay una definición específica acerca de “Delito Informático”, varios tratadistas y doctrinarios en el tema han hecho el esfuerzo por dilucidar un concepto claro y conciso respecto a este ilícito de la nueva era. Es así que entre los más conocidos tenemos las siguientes definiciones:

Nidia Callegari define al “delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas”. El Departamento de Investigación de la Universidad de México, señala como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático”. El italiano Carlos Sarzana, define el Delito Informático como "cualquier

comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".

María de la Luz Lima dice que el "delito electrónico" "en un sentido amplio es 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. (Conde et al., 2009)

Definición de Phishing

Es una técnica que se utiliza para duplicar una página web o manipular el diseño de correo electrónico logrando que cualquier enlace que generen los phishers parezca legítimo y así hacen creer al usuario que se encuentran en una página oficial y que el correo que reciben proviene de una identidad segura y lo utilizan generalmente en páginas de instituciones bancarias para poder tener el login y la contraseña del cliente de la institución y así poder realizar diversos delitos.

Carlos Lang, presidente de Hauri Latinoamérica comenta que aun cuando este ilícito en el país es menor respecto a lo que sucede en Estados Unidos y Brasil, las pérdidas asumidas por las instituciones financieras mexicanas están en franco aumento.

Durante el 2004, precisa a El Economista, los fraudes cometidos en contra de los clientes o usuarios, tuvieron un costo para las instituciones financieras de más de 11 millones de dólares, cifra que para el primer trimestre de este año ascendió a 50 millones de dólares.

Esto es, que, en tan solo tres meses, los costos por este ilícito no solo superaron la cifra total que se reportó en un año, sino que aumentó cinco más, de ahí la importancia de contar con soluciones tecnológicas que permitan proteger a los usuarios y clientes de la banca, destaca.

Además, de que ya no se habla de hackers sino de la participación de bandas organizadas, agrega.

"Ya no es un muchacho que está con su computadora en la noche tratando de ingresar al sistema de una compañía para inyectar un virus o simplemente tener acceso a su información, sino que ya hablamos de bandas organizadas que se dedican al fraude por el internet", refiere.

Con base en las estadísticas de la Policía Federal Preventiva al 2004, cinco de los grupos financieros más importantes del sistema financiero han resultado ser los más afectados:

HSBC con 28%, Bancomer con 22%, Banamex con 21%, Banorte con 19%, Santander Serfin con 8.0% y Banco Azteca con 2.0 por ciento.

Debe quedar claro que el objeto de fraude no es el banco, sino el cliente o usuario, ya que las instituciones mexicanas cuentan con todos los mecanismos de seguridad en sus servidores y áreas de comunicación.

Situación que no se observa en el sistema bancario de Estados Unidos, en donde de acuerdo con sus leyes, el culpable del fraude es el cliente o usuario, los cuales durante el 2004 asumieron una perdida por 2.4 billones de dólares. (Reynold, 2005)

Métodos de phishing

URLs manipuladas, o el uso de subdominios los cuales son trucos comúnmente utilizados por los phishers ejemplo: http://www.nombredelbanco.com/ejemplo, el cual no es la dirección original si no que se agrega algo al final que direccione a otro enlace para capturar la información.

Para disfrazar enlaces utilizando en las direcciones de las páginas el símbolo @ para así poder solicitar usuario y contraseña y captar esa información ejemplo: http://www.nombredelbanco.com@members.tripod.com/ en la que el usuario cree que ingresa a un sitio oficial pero en realidad está ingresando a members.tripod.com/ solo para capturar los datos. (UAL, 2016)

El método Cross siete Scripting en este ataque utilizan el propio código del banco para que todo el ambiente parezca oficial de la institución bancaria y el cliente recibe un mensaje diciendo que debe verificar sus cuentas, la cual es un enlace modificado para obtener datos del cliente.

El phishing se ha sofisticado y mutando, lo que ha hecho que cada vez sea más difícil prevenirlo o encontrar a sus autores. Los phishers ya no sólo utilizan los correos electrónicos para enganchar a sus víctimas, sino que se valen de nuevas tácticas. Han alcanzado tales niveles, que ahora con la variante del spear phishing pueden localizar de manera focalizada a una víctima para defraudarla. También estos delicuentes lo que están haciendo es diseñar las páginas de phishing en Flash, en vez de lenguaje HTML, para evitar así las herramientas que existen en contra de este ataque. Entrevistado por TECNOLOGÍA, Alfredo Reyes Krafft, Vicepresidente Ejecutivo de la Asociación Mexicana de Internet (AMPICI), explicó las diversas formas de ataque que utilizan los phishers?: El phishing se puede hacer a través de correo tradicional, a través del teléfono por medio de un centro de contacto, por un mensajero instantáneo o incluso a través de aplicaciones como Google Talk?. Puntualizó que esta nueva

forma de realizar ataques para robo de identidad se debe a que son más intrusivos; como el correo electrónico ya puede detectar si un mensaje es spam o no lo es, los usuarios se toman más tiempo en revisar sus bandejas de entrada. En cambio, si reciben una liga por medio de un mensaje instantáneo en su PDA o teléfono inteligente, por la premura es más probable que los usuarios accedan a los sitios de phishing. Incluso, a través de un mensaje de texto, SMS, en teléfonos celulares que tienen acceso a Internet, se puede realizar un fraude. Ataque nuevo, métodos tradicionales (Nájera, 2017).

Juan Carlos Guel, jefe de Seguridad en Cómputo de la UNAM, reveló que, según datos de la Secretaría de Seguridad Pública federal, entre el 1 de enero y la primera quincena de abril, las autoridades tomaron conocimiento de 884 casos, cuando en el primer cuatrimestre de 2008 fueron 461.

El especialista en delitos cibernéticos detalló que en todo 2008 se reportaron mil 396 incidentes de ese tipo, es decir, que el promedio semanal fue de 29 eventos, mientras que en este año es de 59.

A este ritmo, el récord de 2008 será superado en junio, e incluso podría llegar a los 2 mil 50 casos que se reportaron en 2006, que es el máximo que la Policía Cibernética registra desde hace tres años, cuando el "phishing" comenzó a representar una amenaza para las instituciones mexicanas y sus usuarios.

Guel advirtió, durante una ponencia en la UNAM, que esa tendencia es preocupante porque las dependencias y los bancos ya han mejorado sus "candados" electrónicos y sistemas de seguridad virtual.

Incluso, en 2007 se creó "E-Crime", un grupo interdisciplinario en el que participan gobierno, academia, iniciativa privada y asociaciones civiles, para analizar la problemática e implementar acciones conjuntas para reducir los delitos en internet.

Según el especialista, el tipo de "phishing" más recurrente en México es que sufren las instituciones bancarias y que consiste en el envío masivo de correos electrónicos provenientes de supuestos entes oficiales y benéficos, pero cuyo objetivo es el de obtener información financiera confidencial -como nips o números de cuenta- para realizar fraudes (Baranda, 2009).

El phishing funciona de tres maneras

- Haciendo que respondas un correo electrónico en el cual podrá hacerse pasar por cualquier institución y solicitar datos personales, o usuario y contraseña de dicha institución.

- Haciendo que la víctima haga clic en un enlace que los phisher envía por correo electrónico suplantando una página web y solicitando loogin y contraseña.
- Simplemente haciéndote enviar un mensaje de texto con usuario y contraseña para validación de información tomando el puesto de una institución. (UAL, 2016)

Las identidades que pueden verse suplantadas son:

- Bancos
- Instituciones Públicas (Policía, SRI, etc.…)
- Centros Educativos (Universidades)
- Entre otras.

Las medidas que han tomado las entidades bancarias

Actualmente, como medida de seguridad, los bancos han creado unos teclados virtuales con orden alfabético aleatorio para que de esa manera la información que se ingresa ahí como login y contraseña no sea interceptada por un keylogger ni por cualquier información ilícita.

Además de ellos han agregado en sus páginas oficiales comunicados en la cual indica que el banco no solicita información personal ni cambio de clave por medio de correo electrónico ni sincronizaciones de tarjetas de crédito.

También se han agregados números telefónicos para que se comuniquen con servicio al cliente si reciben información sospechosa.

La única información enviada por entidades bancarias

- Acceso éxito
- Acceso denegado
- Notificación cuando ocurre cambio de contraseña
- Mensajes de bienvenida
- Solicitudes de código de autorización
- Modificación de clave de débito
- Activación de tarjeta de débito
- Transacciones realizadas (pagos,retiros,transferencias). (BP, 2016)

¿Cuál es la finalidad del Phishing?

- Fraude y robo en instituciones bancarias.
- La suplantación de Identidad
- Envíos de Virus y span para ocasionar caos.
- Robo de datos personales

El Phishing Una Nueva Modalidad De Fraude En Ecuador:

Bogotá, 23 feb (EFE). - Brasil y Ecuador fueron los países latinoamericanos con mayor cantidad de víctimas en 2015 de ataques "phishing", en los que los usuarios son engañados mediante correos electrónicos o páginas falsas, según un estudio mundial sobre seguridad en internet.

"Latinoamérica siempre ha sido un territorio bastante atractivo para los criminales cibernéticos y, por ello, podemos ver, además, la presencia de los países de la región en el 'top' de los emisores de 'spam'", dijo hoy a Efe Dmitry Bestuzhev, director para América Latina del equipo de Análisis e Investigación Global de la compañía de seguridad informática Kaspersky Lab, firma autora del estudio.

El estudio indica que Japón es el país con mayor número de usuarios afectados por "phishing", con un 21,68 %, seguido de Brasil (21,63 %), India (21,02 %), Ecuador (20,03 %) y Mozambique (18,30 %).

Según el informe, los temas más usados el año pasado para este tipo de fraudes fueron los Juegos Olímpicos en Brasil, la situación política de Ucrania, la guerra en Siria, las elecciones en Nigeria y el terremoto en Nepal.

El documento muestra también que Estados Unidos sigue siendo la mayor fuente de "spam" o correo no deseado del mundo (15,2 %), seguido por Rusia (6,15 %), Vietnam (6,13 %) y China (6,12 %).

Dentro de las naciones latinoamericanas, Argentina (2,90 %) ocupa el lugar nueve, Brasil (2,85 %), el puesto diez, y México (1,93 %), el quince.

En cuanto a víctimas de "spam", Alemania figura en el primer puesto con 19,06 % de los ataques, seguido por Brasil (7,64 %) y Rusia (6,03 %).

El informe detalla que el volumen de correos electrónicos no deseados el año pasado se redujo hasta el 55,28 % del total, lo que representa un descenso del 11,4 % respecto al año anterior, y advierte que los dispositivos móviles son el nuevo objetivo para los ataques o fraudes informáticos.

"Aún se vive en la ingenuidad de pensar que los dispositivos móviles no son vulnerables a los ataques informáticos. Dichas circunstancias le hacen el escenario perfecto para los atacantes", indicó Bestuzhev.

En 2015, los ciberdelincuentes continuaron enviando correos electrónicos falsos desde dispositivos móviles y notificaciones de aplicaciones móviles que contenían malware o mensajes publicitarios, sostiene el informe.

"El aumento del uso de dispositivos móviles en nuestra vida diaria para intercambiar mensajes y datos, así como para tener acceso y controlar cuentas bancarias, también ha tenido como resultado el aumento de oportunidades de explotación para los ciberdelincuentes", afirmó Daria Loseva, experta en Análisis de Spam de Kaspersky Lab.

"Por tal razón, los usuarios de dispositivos móviles tienen que estar atentos y no bajar la guardia, ya que las actividades de los ciberdelincuentes en esta área es muy probable que aumente, junto con nuestra dependencia de los dispositivos", agregó. (EFE, 2016)

En Latinoamérica, el 21% de los internautas hacen transacciones en línea todos los días, pero un 42% hace menos de una al mes o no usa este mecanismo de pago.

¿Por qué? El temor al robo o fraude electrónico y la percepción de que no es seguro es la principal razón citada por casi de cuatro de cada 10 de ellos.

Esta es una de las conclusiones del informe Visión de los Consumidores Latinoamericanos sobre el Fraude Electrónico 2013", realizado por Easy Solutions en Costa Rica, República Dominicana, Panamá, Colombia, Venezuela, Ecuador, Chile, Argentina, México y Brasil.

Aun así, la banca móvil y en línea continua su crecimiento en términos de uso y preferencia, mientras que las oficinas físicas y los cajeros electrónicos pierden favoritismo.

Internet se mantiene como el canal más frecuentemente usado para las transacciones bancarias (el 77% de los encuestados manifestó su predilección por este canal). Los usuarios optaron por este canal en promedio 3,9 veces por mes, y el 65% de ellos realiza algún tipo de transacción al menos una vez a la semana (Jiménez, 2015).

Kaspersky Lab anunció el descubrimiento de una nueva campaña de ciberespionaje con el nombre clave de 'Machete', la cual se ha dirigido a víctimas de alto perfil, incluyendo gobiernos, fuerzas militares, embajadas y las fuerzas del orden desde hace por lo menos 4 años.

El campo principal de su operación ha sido América Latina: la mayoría de las víctimas parecen estar ubicada en Venezuela, Ecuador y Colombia. Entre otros países afectados se encuentran Rusia, Perú, Cuba y España.

El objetivo de los atacantes es recopilar información sensible de las organizaciones comprometidas. Hasta ahora es posible que los atacantes hayan podido robar gigabytes de datos confidenciales exitosamente.

Parece ser que los cibercriminales de América Latina están adoptando las prácticas de sus colegas en otras regiones. Anticipamos que el nivel tecnológico de los cibercriminales locales aumente considerablemente, por lo que, probablemente, nuevas campañas de ataques

dirigidos pueden llegar a ser muy similares, desde el punto de vista técnico, a aquellas consideradas como las más sofisticadas del mundo" dijo Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky Lab.

Con base en la evidencia descubierta durante la investigación de Kaspersky Lab, los expertos concluyeron que los atacantes de la campaña parecen hablar español, y tener raíces en algún lugar de América Latina

La mejor protección contra campaña de ciberespionaje tales como Machete es aprender como el spear-phishing funciona y no caer en sus trampas, así como contar con una solución de seguridad funcional y actualizada. Los productos de Kaspersky Lab identifican y protegen contra este ataque dirigido.

ANÁLISIS LEGAL

Con el rápido avance de la tecnología en los últimos 30 años cada vez a pasos más acelerados y la democratización del acceso al Internet en casi todo el planeta, podemos decir sin lugar a dudas que el mundo se ha digitalizado. Desde los aspectos más humanos y sensibles como la música o el cine, hasta los más especializados procesos y actividades desarrolladas por el hombre, como son las complejas transacciones financieras que hoy en día atraviesan el mundo en fracciones de segundo se manejan hoy a través de computadores y redes globales.

Constitución Del Ecuador

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.

Sección novena

Personas usuarias y consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

Sección cuarta

Acción de acceso a la información pública

Art. 91.- La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley.

Sección quinta

Acción de hábeas data

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

SECCIÓN TERCERA

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de

tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

CAPÍTULO IV.- EL DERECHO DE LA PROPIEDAD INTELECTUAL EN EL DESARROLLO DE LA PROTECCIÓN AL CAPITAL INTELECTUAL

Autor: Carlos Alcívar Trejo, Mgs.
Coordinador Académico y Docente de la Facultad de Derecho de la Universidad Tecnológica ECOTEC

INTRODUCCIÓN

Hoy en día Ecuador se encuentra adherido a la Organización Mundial de Comercio y ha ratificado el Acuerdo sobre los Derechos de La Propiedad Intelectual.

Ecuador se unió a esta con el fin de ponerle un alto a este delito, el cual perjudica económicamente y causa conflictos tanto nacionales como internacionales, enfocándonos también en que esto no permite el correcto desarrollo del país, ya que, al tomar el nombre e imagen de otra Propiedad Intelectual no se logra avanzar tecnológica, cultural ni socialmente, por el simple hecho de que nos acostumbramos a tomar ideas de otros autores y usarlas como si fueran propiedad de esa persona, algo que no favorece al desarrollo de nuestro país , porque Ecuador busca convertirse en un país en vías de desarrollo y con lo simple que pueda parecer este caso, lo único que obtendremos es un atraso como sociedad al mal acostumbrarnos a necesitar de otras ideas y no poder aplicar una que sea razonada por nosotros.

La propiedad intelectual tiene que ver con las creaciones de la mente: invenciones, obras literarias y artísticas, símbolos, nombres, imágenes, dibujos y modelos utilizados en el comercio, en base a esto, la declaración Universal de los Derechos Humanos, aprobada por la ONU.

En el mundo existe un organismo especializado del sistema de organizaciones de las Naciones Unidas, desde 1967, OMPI o WIPO – por sus siglas en inglés-, su objetivo es desarrollar un sistema de propiedad intelectual internacional, que sea equilibrado y accesible y recompense la creatividad, estimule la innovación y contribuya al desarrollo económico, salvaguardando a la vez el interés público. Nuestro país como miembro de este organismo internacional goza de todos los derechos que se concede a los integrantes y debe cumplir con todo lo convenido. (IEPI, 1999)

Uno de los mayores problemas en la actualidad es el Robo de La Identidad Intelectual.

La propiedad intelectual referente a los derechos de autor comprende todo lo relacionado a obras literarias y artísticas, como por ejemplo novelas, poemas, obras de teatro, obras musicales, películas, obras de arte, diseños arquitectónicos, entre otros. Asimismo, los

derechos relacionados o conexos a los derechos de autor incluyen los derechos de los artistas intérpretes sobre sus interpretaciones realizadas, los derechos de los productores musicales sobre sus grabaciones, así como también los derechos de las empresas u organismos de radiodifusión sobre las transmisiones de sus programas de radio y televisión. (Arce, 2009, p. 61).

Ecuador es uno de los países con mayor índice de Robo de La identidad Intelectual o Piratería. (Colaboradores de Wikipedia, 2015) En el año 2007, el entonces Presidente del Instituto Ecuatoriano de Propiedad Intelectual (IEPI), Alfredo Corral, manifestó que Ecuador es uno de los países en Latinoamérica con los más altos índices de piratería, cuyos porcentajes respondían a las siguientes cifras: discos de música 95%; software 60%; y obras audiovisuales 99%.

Con estos porcentajes por delante se puede notar la facilidad de la adquisición de estos elementos, que tienen el fin de ser vendidos al público. Una de las principales causas de piratería como comercio es la facilidad con la que se pueden conseguir, en Ecuador se ha demostrado que la piratería es uno de los medios principales por el cual se puede lucrar de las ideas de otros individuos, usando sus ideas y vendiéndolas a un precio extremadamente bajo, todo esto es aceptado por los ciudadanos ecuatorianos los cuales en vez de denunciar este tipo de actos lo que hacen es ser los principales influyentes de que se sigan dando casos de este índole.

En Ecuador El Órgano Principal que se encarga de regular y aplicar las Leyes de La Propiedad intelectual es el IEPI.

(Instituto Ecuatoriano de La Propiedad Intelectual, 1999) El IEPI es una Institución revolucionaria que promueve a la propiedad intelectual en el Ecuador, como una herramienta para alcanzar el “sumak kawsay o buen vivir”, a través de la democratización del conocimiento y de la puesta al servicio de la sociedad de los avances tecnológicos y científicos de la humanidad, precautelando la soberanía nacional y los derechos de los ciudadanos y ciudadanas.

El IEPI es el Organismo Administrativo Competente para propiciar, promover, fomentar, prevenir, proteger y defender a nombre del Estado Ecuatoriano, los derechos de propiedad intelectual reconocidos en la Ley y en los tratados y convenios internacionales, sin perjuicio de las acciones civiles y penales que sobre esta materia deberán conocerse por la Función Judicial.

El IEPI es una institución comprometida con la promoción de la creación intelectual y su protección. Promueve una gestión de calidad, talento humano competitivo y servicios técnicos que satisfagan las necesidades de los usuarios de acuerdo a la Ley nacional, los tratados y convenios internacionales vigentes.

(UNESCO, 2007) A los creadores, comprendidos los autores y los titulares de derechos conexos, ya que las ventas ilícitas afectan a su principal fuente de ingreso, que se deriva de las regalías provenientes de las ventas lícitas.
A los trabajadores de todas las industrias culturales, debido a que la piratería remplaza a la producción de productos originales y los empleos.
Al Estado, ya que las actividades relacionadas con la piratería se llevan siempre a cabo, al menos parcialmente, al margen del sistema establecido y, en consecuencia, no se cobran impuestos que se reinvertirían en el desarrollo cultural.

Estos comportamientos causan en la sociedad una reacción de conformismo, ya que , se acostumbran a vivir de las ideas de otras personas para poder desarrollar sus vidas, esto causa en la sociedad ecuatoriana un atraso de ideas y cultural, esto se da porque al no tener la capacidad de usar sus propias ideas depende de otros individuos o industrias para poder crear o revolucionar de manera en la que sean reconocidos como Autores de esas ideas, pero según El Gobierno busca crear una conciencia en los ciudadanos de manera en la que su formación sea totalmente independiente, refiriéndose a los pensamientos e ideologías, pero al aceptar este tipo de actos como la piratería se transforma en una sociedad mediocre y conformista.
Ya se encuentra tipificado en la Ley los medios por los cuales se puede aplicar una sanción por este caso, en el ámbito civil, administrativo y sin perjuicios penales las sanciones pueden ser multas económicas, la cesación de los actos violatorios, indemnización por daños y perjuicios, el valor total de los costos procesales.
Podrán exigirse también los derechos establecidos en los convenios internacionales vigentes en el Ecuador, especialmente los determinados en el Acuerdo sobre los Aspectos de Propiedad Intelectual relacionados con el Comercio (ADPIC) de la Organización Mundial del Comercio. (SICE Art.288 y Art.289).

En Ecuador se promulgaron leyes para poder salvaguardar la propiedad intelectual de cada persona (Registro Oficial No 320 Ley de Propiedad Intelectual) siempre y cuando esta se encuentre registrada por su autor.
Actualmente en Ecuador, estas Leyes no son respetadas y tampoco son sancionadas, esto en la sociedad no influye negativamente, todo lo contrario, esto genera comercio y este genera

empleo para las personas, también son bien vistas en el campo del mercado, porque brindan a facilidad a las personas con menor poder adquisitivo a obtener objetos de imagen similar a la de otras marcas (propiedades intelectuales).
Según la Legislatura Ecuatoriana estos casos son penados civiles, administrativamente y sin perjuicios penales pueden ser sancionados con una multa económica, la cesación de los actos violatorios, Indemnización por daños y perjuicios, el valor total de los costos procesales.
Podrán exigirse también los derechos establecidos en los convenios internacionales vigentes en el Ecuador, especialmente los determinados en el Acuerdo sobre los Aspectos de Propiedad Intelectual relacionados con el Comercio (ADPIC) de la Organización Mundial del Comercio. (SICE Art.288 y Art.289).

Antecedentes
Los primeros indicios de Derechos de la Propiedad Intelectual se remontan a los tiempos de la Antigua Grecia.
(Instituto de Derecho de Autor, 2010) *Podemos remontarnos a la antigua Grecia para encontrar los primeros ejemplos de reconocimiento de la creatividad y el trabajo intelectual. En el año 330 a.c, una ley ateniense ordenó que se depositaran en los archivos de la ciudad copias exactas de las obras de los grandes clásicos. Entonces, los libros eran copiados en forma manuscrita, por consiguiente, el costo de las copias era muy alto y su número total muy limitado. Este hecho, sumado a la escasez de personas capacitadas para leer y en condiciones de poder adquirirlas, determinó el nacimiento de un interés jurídico específico que proteger.*

En la época romana, no existía el reconocimiento de derechos que provinieran de las creaciones del intelecto, y mucho menos, que estos derechos fueran afines a la categoría de derechos que los romanos habían establecido, es decir, los derechos personales, de obligaciones y reales.
Por consiguiente, los propios autores no se planteaban la necesidad de que sus obras fueran objeto de alguna recompensa derivada del prestigio y reputación que les proporcionaban. Sin embargo, existía como forma de adquirir la propiedad, la especificación, que era la creación de un bien, desde luego material; no obstante, podría considerarse un antecedente remoto ya que la propiedad intelectual es respecto de creaciones del intelecto.

Tal situación se prolongó hasta el siglo XV, en el cual, surge la imprenta y la posibilidad de una divulgación más amplia de todas las obras que en esa época ya existían; y a partir de tal suceso, el monarca utilizaba un sistema de privilegio para animar y mejorar el trabajo de los autores, a través de este sistema, como un acto del soberano se concedía una licencia para

la explotación en forma exclusiva de un invento o una obra por un tiempo determinado y sobre ciertas condiciones, llevando implícita la censura previa o el examen de las obras o inventos sujetos al privilegio.

(Instituto de Derecho de Autor, 2010) La imprenta inventada por Gutenberg a mediados del siglo XV, y el descubrimiento del grabado producen transformaciones radicales en el mundo. Con la imprenta aumenta la producción y reproducción de libros en grandes cantidades y a bajo coste.

La posibilidad de utilizar la obra se independiza de la persona de su autor. Nace entonces la necesidad de regular el derecho de reproducción de las obras, aunque llevaría varios siglos más delimitar los caracteres actuales. Primero apareció bajo la forma de "privilegios". Estos privilegios eran monopolios de explotación que el poder gubernativo otorgaba a los impresores y libreros, por un tiempo determinado, a condición de haber obtenido la aprobación de la censura y de registrar la obra publicada. Surgen las primeras normativas que vienen a regular los privilegios de impresión y reproducción de obras concedidos en aquel tiempo por la Corona; destacándose las normas españolas conocidas como "Pragmáticas" de 1502 y 1558, y la Ley de Licencias (Licensing Act) de 1662 en Inglaterra. Dichos textos conceden la protección a través de un privilegio a la persona que difunde la obra escrita (editores y dueños de imprentas), y no al autor de la obra. En definitiva, se constituía un "monopolio concedido" que regía por un tiempo y para un territorio determinado. Evidentemente los límites espaciales no podían exceder el territorio nacional, y así cada país en el ejercicio de la voluntad soberana otorgaba los privilegios territoriales según sus criterios propios.

La primera ley moderna de derechos de autor cobra vida de la mano del llamado "Estatuto de la Reina Ana", cuyo título original es "An act for the encouragement of learning, by vesting the copies for printed books in the authors or purchasers of Duch copies, during times there in mentioned". Dicha ley, promulgada en 1710 en Inglaterra, designa al autor como dueño de los derechos intelectuales sobre su obra, y limita la protección de sus trabajos publicados a un plazo fijo. Este principio que prioriza el rol del creador en vez del editor es recogido más tarde por la Constitución de los Estados Unidos de América de 1787, que incorpora expresamente la protección de los derechos del autor y también del inventor[1]

Con la Revolución Francesa, se suprimieron los privilegios y con el fin de mejorar la protección de los creadores intelectuales, las relaciones que vinculaban a éstos con sus obras, fueron

[1] En efecto, la sección 8 del artículo 1 de la Constitución permite al Congreso legislar "a fin de promover el progreso de las ciencias y artes, asegurando por tiempo limitado, a los autores e inventores los derechos exclusivos sobre sus escritos e invenciones".

asimiladas al derecho real de dominio, considerando a este tipo de propiedad como más importante que la que existía sobre los bienes inmateriales.

(Instituto de Derecho de Autor) (2010) En 1710, a pesar de las fuertes resistencias que opusieron impresores y libreros, llegó a la Cámara de los Comunes un proyecto de ley conocido como el "Estatuto de la Reina Ana", que acabó con el privilegio Real de 1557 establecido a favor de la Stationers Company, quien ostentaba el monopolio de la publicación de libros en Inglaterra.

En 1763 en España, el Rey Carlos III dispuso, por real ordenanza, que el privilegio exclusivo de imprimir una obra sólo podía otorgarse a su autor y debía negarse a toda comunidad secular o regular.

En Francia, el proceso de reconocimiento de derechos a los autores tuvo su origen en los litigios que, desde principios del siglo XVIII, mantuvieron los impresores y libreros "privilegiados" de París (que defendían la utilidad de renovación de los privilegios a su vencimiento) con los no "privilegiados". El gobierno de Luis XVI intervino en la cuestión dictando, en agosto de 1777, seis decretos en los que reconoció al autor el derecho a editar y vender sus obras, creándose así dos categorías diferentes de privilegios, los de los editores y los reservados a los autores.

Este sistema continuó hasta la segunda mitad del siglo XIX.

El sistema de privilegio y el sistema de la asimilación al dominio mostraron una buena reacción contra las posiciones que negaban el derecho de goce que asiste a los autores en relación con el producto de su creación intelectual.

Esto era viéndolo desde el punto de vista en Las Civilizaciones Antiguas pero los antecedentes en la actualidad fueron los siguientes.

- **Inicios del derecho de patentes**

En lo concerniente al derecho de patentes comúnmente se nombra como primer intento normativo la ley veneciana de 1474 adoptada en Italia. Sin embargo, las primeras leyes modernas de patentes se dictan:

- En Inglaterra, en 1624, con el llamado Statue of Monopolies que regula y objetiviza el otorgamiento de las patentes, prerrogativa real que se otorgan al primer inventor por un término de 14 años.

- En Estados Unidos, con la Ley de Patentes de 1790[2].
- En Francia, con la Ley de Patentes de 1791[3].

Esos tres países económicamente significativos en el siglo XVlll ejercen un rol de vanguardia[4] Poco a poco se aprueban también en otros países las primeras leyes que protegen las invenciones: Holanda lo hace en 1809, Austria en 1810, España en 1811[5], Bavaria[6] y Rusia en 1812, Prusia en 1815, Suecia en 1819 y Portugal en 1837

En esa época surgen asimismo las primeras oficinas de patentes, tales como la "Dirección de Patentes" en Francia, creada por el Reglamento de la Ley de 1791[7];el "Conservatorio de Artes y Oficios" establecido en 1810 en Madrid[8] ; en 1836, la primera oficina de patentes de Estados Unidos, que dependía del Departamento de Estado[9] y en Inglaterra *"The Patent Office" creada en 1852 por la nueva Ley de Patentes[10]. Ello no hace sino subrayar el carácter territorial que imperaba en la regulación y administración de los derechos de propiedad industrial. Dada esa limitación, no se concebía la obtención de una patente en varios países, ni la protección de las invenciones a nivel internacional.*

[2] La primera ley estadounidense de patentes se titulaba: "An Act to promote the progress of useful Arts" y fue promulgada por el presidente George Washington el 10 de abril de 1790. Después de solo tres años de vigencia ya fue objeto de una reforma, promulgándose el 21 de febrero de 1793 la "Patent Act of 1793". En los años siguientes iban a continuar dictándose leyes reformatorias del sistema de patentes de Estados Unidos, lo cual demuestra el énfasis e importancia que esta joven nación ponía en el tema de la promoción de la creatividad e innovación.

[3] Dicha ley –loi sur le brevet– fue votada por la Asamblea constituyente el 30 de diciembre de 1790 y promulgada por el Rey el 7 de enero de 1791. Mayor información sobre la historia de esa ley se encuentra en Block, M.M., Dictionnaire de l'Administration Française, Librairie Administrative de Veuve Berger-Levrault et fils, París, 1856, p. 230

[4] Mayores antecedentes sobre estos tres casos en Sáiz González, J. Patricio, Invención, Patentes e Innovación en la España Contemporánea, Oficina Española de Patentes y Marcas, Madrid, 1999, pp. 61 y ss.

[5] "Durante el gobierno afrancesado de José Bonaparte se promulgó el Real Decreto de 16 de septiembre de 1811, estableciendo las reglas por las que han de regirse en España los que inventen, perfeccionen o introduzcan nuevos artilugios en cualquier ramo de la industria": [http:// www.exposicionesvirtuales.oepm.es/].

[6] En 1871 nace el Imperio Alemán, como consecuencia de la unificación alemana, y la primera ley de patentes de la Alemania unificada se promulga el 25 de mayo de 1877, normativa que entra en vigencia el 1º de julio del mismo año. Mayores antecedentes

[7] Dicho reglamento fue promulgado pocos meses después de la ley, el 25 de mayo de 1791. Algunos años después se cambió la denominación de la Dirección, pasando a llamarse "Conservatoire des Arts et Métiers de Paris".

[8] "En 1810 se estableció en Madrid un Conservatorio de Artes y Oficios –firmado por el secretario de Estado, Mariano Luis de Urquijo (1768-1817)–, que funcionó como una primera Oficina de Patentes. Tenía previsto ser un depósito general de todo tipo de máquinas, modelos, instrumentos, dibujos, descripciones y libros en relación a cualquier arte y oficio, pero, además, por vez primera se especificaba la obligatoriedad de depositar los originales de toda máquina e instrumento inventado o perfeccionado en España. También estaba encargado de difundir la información tecnológica, a través de la publicación de un periódico especializado ('Anales de las Artes') o remitiendo duplicados de los inventos a otros establecimientos": Oficina Española de Patentes y Marcas, "200 años de Patentes", en Revista Electrónica de la oepm, n.º 23, febrero de 2011, publicada en: [http://www. oepm.es/cs/oepmSite/contenidos/Revista_Infopym/2011/Febrero/Febrero/noticia-04.html]. También existe amplia información sobre el punto en: [http://historico.oepm.es/historia_oepm/default.html].

[9] Al respecto cfr. la Ley de Patentes de 1836 de Estados Unidos: Patent Act of 1836, Ch. 357, 5 Stat. 117 (July 4, 1836), en: [http://ipmall.info/hosted_resources/lipa/patents/ Patent_Act_of_1836.pdf]. A partir del año 1926 la Oficina de Patentes de Estados Unidos dependía del Departamento de Comercio

[10] En 1852 se promulga la segunda ley de patentes en el Reino Unido, llamada "British Patent Law Amendment Act". Más antecedentes se pueden encontrar en Dutton, H.I., The patent system and inventive activity during the Industrial Revolution, 1750-1852, Manchester University Press, Manchester, 1984, pp. 57 y ss. Solo muy recientemente, el 2 de abril de 2007, "The Patent Office" pasó a cambiar su nombre al actualmente vigente: "Intellectual Property Office".

La independencia de cada país en el proceso legislativo que conduce a las primeras normas de protección de patentes queda de manifiesto en el siguiente párrafo: "Pendant tout le xixè siècle, les pays industrialisés […] développent en fait
leur loi sur les brevets de façon indépendante selon leur propre mentalité et leur degré spécifique de développement". (Rolnik, 2002, p. 8.)

- **El Convenio de Berna para la Protección de las Obras Literarias y Artísticas**

De la misma forma como respecto de las patentes, también en el ámbito de los derechos de autor los autores comenzaron, pocas décadas después de haberse reconocido sus derechos por leyes nacionales, a presionar por un sistema más equitativo y universal. La autora argentina Delia Lipsyc expresa esta evolución de forma muy precisa: "la protección del derecho dentro de los límites del propio".
Estado no alcanzaba para asegurar su vigencia. El don de ubicuidad que caracteriza a las obras del espíritu y la internacionalización de los mercados del libro y de la música hicieron imprescindible que el derecho de autor fuera reconocido en todos los lugares donde la obra pudiera ser utilizada". (Lipsyc, 2006, p.37)

(Instituto Ecuatoriano de la Propiedad Intelectual) (1999) La propiedad intelectual tiene que ver con las creaciones de la mente: invenciones, obras literarias y artísticas, símbolos, nombres, imágenes, dibujos y modelos utilizados en el comercio, en base a esto, la Declaración Universal de los Derechos Humanos, aprobada por la ONU, reconoce como un derecho fundamental la protección de las creaciones intelectuales y designa al Estado como su defensor.

En el mundo existe un organismo especializado del sistema de organizaciones de las Naciones Unidas, desde 1967, OMPI o WIPO – por sus siglas en inglés-, su objetivo es desarrollar un sistema de propiedad intelectual (P.I.) internacional, que sea equilibrado y accesible y recompense la creatividad, estimule la innovación y contribuya al desarrollo económico, salvaguardando a la vez el interés público. Nuestro país como miembro de este organismo internacional goza de todos los Derechos que se concede a los integrantes y debe cumplir con todo lo convenido.

- **El Convenio de París para la Protección de la Propiedad Industrial**

Para la Exposición Universal de Viena de 1873, los inventores amenazaban con boicotear el evento, de no contar con una protección suficiente contra copias e imitaciones. Es así como los Gobiernos europeos comenzaron a preocuparse del tema. El mismo año 1873 se iniciaron

trabajos preparatorios de cooperación, avanzándose hacia la elaboración de un borrador de convenio en una Conferencia

Diplomática celebrada en París en 1880. Finalmente, en la Conferencia Diplomática de París de 20 de marzo 1883, once Estados[11] suscribieron el Convenio de París para la Protección de la Propiedad Industrial. Después de los procesos de ratificación posteriores, el Convenio entró en vigencia el 7 de julio de 1884.

Pese a su antigüedad, el Convenio de París sigue en vigor, sin que haya perdido relevancia; así, aún hoy constituye uno de los tratados más importantes en la materia que nos ocupa.

Este tema como principio moral se lo puede aplicar como principal ideología en nuestra sociedad, porque al solo lucrarse de la idea de alguien más, esto causa que la sociedad se acostumbre a obtener las cosas de la manera fácil sin sacrificio formando ciudadanos que no serán productivos para la sociedad.

Principalmente creo que se debería empezar aplicando las leyes **(Registro Oficial No 320 Ley de Propiedad Intelectual)** para de esta manera lograr concientizar a los ciudadanos para poder llegar a formar ciudadanos que pienses en el futuro de su país. Al lograr esto por muy simple que sea, se desarrollara una mentalidad más amplia y junto con valores morales, al contrario de lo que se tiene hoy en día.

Uno de los casos más patéticos que se encuentra en el día a día, se da en el ámbito escolar, a la hora de presentar tareas los estudiantes que no cumplen con sus deberes buscan la solución más fácil, la cual es copiar el deber a otro compañero, este se lucra del sacrificio y conocimiento de su compañero, con tal de presentar el deber; pero lo que causa este acto es que el estudiante quien copia el deber no adquiere conocimientos y probablemente se llegará a acostumbrar a copiar el deber a su compañero, es lo mismo en la sociedad que se acostumbra a realizar una acción, sirviéndose de los conocimientos ajenos para su bien estar, formándolos como ciudadanos Conformistas.

[11] Los 11 países originales son: Bélgica, Brasil, El Salvador, España, Francia, Guatemala, Italia, Países Bajos, Portugal, Serbia y Suiza. Al momento de la entrada de vigencia del Convenio en 1884, adhieren otros 3 países: Ecuador, Gran Bretaña y Túnez. Con posterioridad adhieren Noruega (1885), Suecia (1885), los Estados Unidos de América (1887), República Dominicana (1890), Dinamarca (1894) y Japón (1899). De esta forma, hacia fines del siglo xix, los países miembros de la Unión de París eran 20. Actualmente, el Convenio ha sido ratificado por 173 países. La lista completa de las naciones miembros se encuentra en el sitio web de la Organización Mundial de Propiedad Intelectual: [http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=2].

Pero también se debe tener en cuenta un pequeño detalle en esta ley, no se defiende el robo de la imagen o el mal uso de esta solamente.
Existen circunstancias en las que se defiende un punto en específico o como es conocido un SECRETO COMERCIAL, este es un punto conocido solo por X empresa que no se desea que la competencia conozca.

(OMPI, 2013) El secreto forma parte de las actividades económicas desde hace miles de años. Por ejemplo, el secreto permitió a una región de China beneficiarse hábilmente de siglos de explotación de hilo de gusano de seda, y a una familia de Armenia le brindó una ventaja de 400 años en la producción de los mejores platillos de orquesta.

El secreto comercial es un régimen jurídico que protege las relaciones de confianza. Antes de la era industrial, los artesanos innovadores guardaban celosamente sus "trucos del oficio" en los pequeños talleres familiares. Sin embargo, a medida que la industria se trasladó del taller artesanal a la fábrica, surgió la necesidad de un sistema jurídico que obligase a los empleados a guardar la promesa de confidencialidad respecto de un determinado proceso o pieza de maquinaria secretos.

Es importante tener en cuenta que el secreto es una herramienta legítima de toda empresa, cualquiera que sea su tamaño. Hacer valer el derecho al secreto comercial no tiene nada que ver con la falta de transparencia pública. Aunque parezca paradójico, la legislación sobre secretos comerciales puede permitir y fomentar la transferencia de tecnología, dado que ofrece una forma comercialmente razonable de difundir información. Si bien algunos aspectos de las leyes sobre el secreto pueden ser controvertidos, como el período de exclusividad de datos en el caso de las empresas farmacéuticas **(Artículo 39.3 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC))**, en general se considera que en las economías modernas la confidencialidad resulta beneficiosa frente a la divulgación. En efecto, guardar secretos —a menudo información sobre los clientes, sus necesidades y preferencias— es la forma principal en que las pequeñas y medianas empresas (Pymes) protegen sus ventajas comerciales.

Para evitar que alguien se aproveche de esta manera se debe aplicar la Protección Jurídica de la Propiedad Intelectual que cita lo siguiente. **(OMPI, 2013)** La regulación de los secretos comerciales, como la de otras formas de propiedad intelectual, se rige por los ordenamientos jurídicos nacionales. No obstante, en 1995 se crearon normas internacionales para la protección de secretos ("información no divulgada") en el marco del Acuerdo sobre los ADPIC. El artículo 39 del acuerdo establece que los Estados miembros protegerán la "información no divulgada" contra el uso no autorizado "de manera contraria a los usos comerciales honestos"

(esto incluye el incumplimiento de contratos, el abuso de confianza y la competencia desleal). La información no debe ser generalmente conocida ni fácilmente accesible, debe tener un valor por ser secreta, y debe ser objeto de "medidas razonables" para mantenerla en secreto. Esta fórmula general de las leyes sobre secretos comerciales ha sido adoptada por más de 100 de los 159 miembros de la Organización Mundial del Comercio.

Los artículos 42 a 49 del Acuerdo sobre los ADPIC tratan sobre la observancia, y en ellos se contemplan procedimientos judiciales para lograr la observancia de todos los derechos de propiedad intelectual, así como que la "información confidencial" esté protegida frente a la divulgación. Sin embargo, debido a que los sistemas judiciales nacionales, y en especial los métodos de concesión de acceso a las pruebas, son muy diferentes unos de otros, en general se considera que la observancia de los derechos en materia de secretos comerciales también varía mucho de un caso a otro.

Enfocándonos en la sociedad, al permitir este tipo de actos se forman ciudadanos conformistas con ideales pobres, esto lleva toda la contraria a la ideología del actual gobierno que busca ampliar los conocimientos a los jóvenes; no obstante, siempre habrá un choque por los diferentes ideales y pensamientos de los ciudadanos, por culpa de la subjetividad moral, pero eso no quiere decir que sea legal.

El Robo de la Propiedad Intelectual como comercio es uno de los casos más tratados, en la Legislatura actual las sanciones que se pueden dar son heterónomas **(SICE Art.288)** y para mala suerte nuestra en Ecuador las marcas Internacionales tienes mayor influencia que las Nacionales, y esto causa que se busque la manera de producir empleo, al que todos los ecuatorianos mayores de edad tenemos **(Art. 325 Constitución de la República del Ecuador).**

LEY DE PROPIEDAD INTELECTUAL, CODIFICACIÓN:
TÍTULO PRELIMINAR

Art. 1.- El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador.

La propiedad intelectual comprende:

1. Los derechos de autor y derechos conexos;
2. La propiedad industrial, que abarca, entre otros elementos, los siguientes:
   a) Las invenciones;

b) Los dibujos y modelos industriales;
c) Los esquemas de trazado (topografías) de circuitos integrados;
d) La información no divulgada y los secretos comerciales e industriales;
e) Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;
f) Las apariencias distintivas de los negocios y establecimientos de comercio;
g) Los nombres comerciales;
h) Las indicaciones geográficas; y,
i) Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

Art. 3.- El Instituto Ecuatoriano de la Propiedad Intelectual (IEPI), es el organismo administrativo competente para propiciar, promover, fomentar, prevenir, proteger y defender a nombre del Estado ecuatoriano, los derechos de propiedad intelectual reconocidos en la presente Ley y en los tratados y convenios internacionales, sin perjuicio de las acciones civiles y penales que sobre esta materia deberán conocerse por la Función Judicial.

Art. 11.- Únicamente la persona natural puede ser autor. Las personas jurídicas pueden ser titulares de derechos de autor, de conformidad con el presente libro.
Para la determinación de la titularidad se estará a lo que disponga la ley del país de origen de la obra, conforme con los criterios contenidos en el Convenio de Berna, Acta de París de 1971.

DECISIÓN 351 DE LA CAN
RÉGIMEN COMÚN SOBRE DERECHO DE AUTOR Y DERECHOS CONEXOS

Artículo 4.- La protección reconocida por la presente Decisión recae sobre todas las obras literarias, artísticas y científicas que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocer, y que incluye, entre otras, las siguientes:

a. Las obras expresadas por escrito, es decir, los libros, folletos y cualquier tipo de obra expresada mediante letras, signos o marcas convencionales;
b. Las conferencias, alocuciones, sermones y otras obras de la misma naturaleza;
c. Las composiciones musicales con letra o sin ella;
d. Las obras dramáticas y dramático-musicales;
e. Las obras coreográficas y las pantomimas;
f. Las obras cinematográficas y demás obras audiovisuales expresadas por cualquier procedimiento;
g. Las obras de bellas artes, incluidos los dibujos, pinturas, esculturas, grabados y litografías;

h. Las obras de arquitectura;
i. Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía;
j. Las obras de arte aplicado;
k. Las ilustraciones, mapas, croquis, planos, bosquejos y las obras plásticas relativas a la geografía, la topografía, la arquitectura o las ciencias;
l. Los programas de ordenador;
m. Las antologías o compilaciones de obras diversas y las bases de datos, que por la selección o disposición de las materias constituyan creaciones personales.

CAPÍTULO V.- LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS

Autores: Carlos Alcívar Trejo, Mgs.
Coordinador Académico y Docente de la Facultad de Derecho de la Universidad Tecnológica ECOTEC

Juan Tarquino Calderón Cisneros, Mgs.
Docente Titular de la Facultad de Ciencias de la Salud de la Universidad Estatal de Milagro (UNEMI).

INTRODUCCIÓN

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas y parte de la criminalidad informática (Acevedo, 2010). La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático. (Cuervo, 2008)

Los delitos informáticos que pueden ser considerados como crímenes electrónicos, tan graves que pueden llegar a ser un genérico problema para el avance de la informática. Sin embargo, este puede tener consigo delitos tan graves como el robo, falsificación de documentos, fraudes, chantajes y malversación de caudales públicos. Un ejemplo muy común es cuando una persona llega a robar información y a causar daños de computadoras o servidores que pueden llegar a ser absolutamente virtuales porque la información se encuentra en forma digital y el daño cada vez se vuelve más grande. Muchas de las personas que cometen este tipo de delitos informáticos tienen diferentes características, tales como la habilidad del manejo de los diferentes sistemas informáticos o la realización de tareas laborales que le facilitan el acceso de carácter simple. También se le puede definir como toda acción culpable por el ser humano quede alguna u otra manera nos lleva a causar un perjuicio a personas que sin necesariamente se beneficien de los distintos tipos de manejo informático ya que los delincuentes que hacen este tipo de delitos nos están quitando la posibilidad de ver todo de

una manera muy distinta y con distinta me refiera a verla de manera original sin quitarle nada o sin quitarlo de aquel lugar donde siempre se mantuvo.
Los delitos informáticos son aquellas actividades ilícitas que: (a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o (b) Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos).

Los también conocidos como Ciberdelitos como lo señala Téllez que son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas atípicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico) Julio Téllez, Derecho Informático, 3ª ed., McGraw-Hill,2004, México, p.7u7

Mucha información es almacenada en un reducido espacio, con una posibilidad de recuperación inmediata, pero por complejas que sean las medidas de seguridad que se puedan implantar, aún no existe un método infalible de protección (Pecoy, 2012a).

La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de data crédito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de Bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

1. ANTECEDENTES HISTÓRICOS

El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica. Después de una reunión en Lyon, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado “G8” con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por lo que migraron a Internet.

El “Grupo de Lyon” utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.
Al mismo tiempo, y guiado por los participantes en el grupo de Lyon, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático.

Este tratado, que fuera presentado a la opinión pública por primera vez en el año 2000, incorporó una nueva gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el “delito informático”. ¿Cómo se definió el delito informático? La versión final de ese tratado, aprobada en noviembre de 2001 después de los acontecimientos del 11 de septiembre, no definió el término. Es un término muy amplio referido a los problemas que aumentaron el poder informático, abarataron las comunicaciones y provocaron que haya surgido el fenómeno de Internet para las agencias policiales y de inteligencia. El tratado describe de la siguiente manera las diferentes disposiciones y áreas temáticas en las que se requiere una nueva legislación:

- ✓ Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- ✓ Delitos relacionados con las computadoras [falsificación y fraude].
- ✓ Delitos relacionados con el contenido [pornografía].
- ✓ Delitos relacionados con la violación del derecho de autor y los derechos asociados.
- ✓ Responsabilidades secundarias y sanciones [cooperación delictiva, responsabilidad empresarial].

I. ANÁLISIS

No hay definición de carácter universal propia de delito informático, no obstante, muchos han sido los esfuerzos de expertos que se han ocupado del tema y, aun cuando no existe una definición con carácter universal, se ha formulado conceptos funcionales atendiendo a realidades nacionales concretas.
En el ámbito internacional se considera que no existe una definición propia del delito informático, pero, al consultar bibliografía, específicamente del español Carlos Sarzana, en su obra Criminalitá e tecnología, los crímenes por computadora comprenden “cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo”.

Criterios doctrinales de algunos tratadistas:

- Nidia Callegari define al “delito Informático” como “aquel que se da con la ayuda de la informática o de técnicas anexas” (Pérez, 1986).
- Rafael Fernández Calvo define al “delito informático” como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española”
- María de la Luz Lima dice que el “delito electrónico”, “en un sentido amplio, es 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”
- Julio Téllez Valdés conceptualiza al “delito Informático” en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tiene a las computadoras como instrumento o fin”. Por otra parte, debe mencionarse que se ha formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa computadoras tales como “delitos informáticos”, “delitos electrónicos”, “delitos relacionados con la computadora”, “crímenes por computadora”, delincuencia relacionada con el ordenador”. Analizando estas determinaciones conceptuales estamos en condiciones de brindar una definición de delito informático:

Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático implicando actividades criminales.

- **Generalidades**

La criminalidad informática incluye una amplia variedad de delitos informáticos. (Pecoy, 2012b)
El fenómeno se puede analizar en dos grupos:

Informática como objeto del delito. Esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo y el DDNS (Denegación de servicio de nombres de dominio).

Informática como medio del delito. Dentro de este grupo se encuentra la falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil.

Crímenes específicos
Sabotaje informático

Implica que el "delincuente" recupere o busca destruir el centro de cómputos en sí (las máquinas) o los programas o informaciones almacenados en los ordenadores. Se presenta como uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito político.
Piratería informática.

La piratería informática consiste en la violación ilegal del derecho de autor. Según la definición que en su artículo 51 brinda el ADPIC (Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual) son aquellas "mercaderías que lesionan el derecho de autor". La piratería es una de las modalidades de reproducción técnica (la otra es la reprografía-reproducción burda del original cuya apariencia dista mucho de la auténtica), que implica la elaboración de una copia semejante al original, con la intención de hacerla pasar por tal.

Existen dos modalidades que se incluyen como piratería informática a saber:

El hurto de tiempo de máquina: consiste en el empleo del computador sin autorización, y se pretende aludir a situaciones en que un tercero utiliza indebidamente recursos de la empresa en que trabaja o un sujeto autorizados se vale de tales prestaciones informáticas en un horario no permitido, utilizándolas para su provecho sin contar con permiso para ese uso fuera de hora.
La apropiación o hurto de software y datos: en este caso el sujeto accede a un computador ajeno o a la sesión de otro usuario, retirando archivos informáticos, mediante la ejecución de los comandos copiar o cortar, para luego guardar ese contenido en un soporte propio.

Cajeros automáticos y tarjetas de crédito
Conductas mediante las cuales se logra retirar dinero del cajero automático, utilizando una tarjeta magnética robada, o los números de la clave para el acceso a la cuenta con fondos.

Robo de identidad
Luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de operaciones para provecho del victimario, fingiendo ser la persona a la que se extrajo su

información sensible. Encuadra como delito de estafa. Si el actuar del sujeto activo comporta dar a conocer datos personales ajenos contenidos en base de datos a las que por su empleo tiene acceso, entonces por expreso mandato legal la figura aplicable es la de revelación de secreto profesional.

Phreaking

Es la metodología más antigua dentro de los denominados ciberdelitos, consiste en ingresar en las redes de telecomunicaciones para realizar llamadas telefónicas a larga distancia utilizando la cuenta ajena. Resulta ser una modalidad primitiva de hacking.

Sujetos agente y paciente

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas, tales como, la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica, sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional. Son individuos con una gran especialización en informática, que conocen muy bien las particularidades de la programación de sistemas computarizados, de forma tal que logran un manejo muy solvente de las herramientas necesarias para violar la seguridad de un sistema automatizado (Pecoy, 2012 a).

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. Víctima puede ser cualquier persona física o jurídica que haya establecido una conexión a Internet (ya que es la principal ventana de entrada para estas conductas), una conexión entre computadoras, o que en definitiva cuenta con un sistema informático para el tratamiento de sus datos (Pecoy, 2012 b).

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

II. LOS DELITOS INFORMÁTICOS EN EL ECUADOR:

Quito, 13 de junio del 2015.- Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, pornografía infantil, acoso sexual, entre otros, se denuncian en las diferentes Unidades de la Fiscalía.
Internet abrió el paso a esas nuevas formas de delincuencia común y organizada que pone en riesgo la información privada, la seguridad en la navegación y de las instituciones públicas y privadas.

La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal (COIP)- hasta el 31 de mayo del 2015. A partir del COIP se tipifica este tipo de delitos.

En el COIP se sancionan los delitos informáticos, cuyos actos se comenten con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales. Estos actos que se registran a través de la Internet son: fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros.

Según el fiscal provincial de Pichincha, Wilson Toainga, las investigaciones referentes a los delitos informáticos se realizan de forma técnica y demanda tiempo para establecer la responsabilidad de aquellos que quebrantan la ley sentados frente a un monitor.

El fiscal Edwin Pérez, especialista en delitos informáticos, indicó que en Ecuador existen dificultades durante la investigación de delitos propiciados por el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país.

“Los grandes proveedores de las redes sociales y generadores de los sistemas informáticos como Google, Facebook, Yahoo, entre otros, tienen los bancos de datos de sus usuarios en Estados Unidos, y solicitar esa información puede demorar meses”, dijo el fiscal Pérez.

Un inconveniente para la investigación radica en que Ecuador no cuenta con convenios internacionales que faciliten el cruce de datos informáticos -como los que existe entre Estados Unidos y Europa-. Por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la sustracción de información personal ante las formalidades y la virtualidad de los procesos puede tardarse meses.

Uno de los casos de delito informático se registró en mayo del 2014, Diana (nombre protegido) se preguntaba: "¿Cómo consiguieron mis datos?". Solo recuerda que ingresó sus datos para realizar una compra por Internet, porque se ofrecían descuentos en productos de belleza. Lo único cierto es que la persona que usó su información le endeudó en 2.500 dólares, a través de débitos de su tarjeta. Su caso es investigado por la Fiscalía.

En el caso de Diana, si hubiese estado vigente el COIP y se descubriera a la persona que robó sus datos, este podría recibir una pena de uno a tres años de cárcel.

La persona que sustrajo la información de Diana compró por Internet dos celulares, una memoria externa y una tablet. La joven tiene una deuda que paga en cuotas mínimas porque su sueldo no le alcanza para cubrir más montos.

Ahora, con la aplicación del COIP, también se sancionan delitos por apropiación ilegal de datos almacenados en teléfonos inteligentes y tablets. En este, en su artículo 191 sanciona con una pena privativa de libertad de uno a tres años.

Imagen 4.1. Delitos Informáticos

Fuente: Consultado el 13 junio 2015. Recuperado de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

III. ANÁLISIS LEGAL: Regulación por países

- ***Argentina***

La ley vigente de Modificación al Código Penal sobre la incorporación de los Delitos Informáticos.

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

Definiciones vinculadas a la informática

En el nuevo ordenamiento se establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (Art. 77 Código Penal).

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (Art. 77 Código Penal).

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (Art. 77 Código Penal).

Delitos contra menores

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produzca, financie, ofrezca, comercialice, publique, facilite, divulgue o distribuya, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Protección de la privacidad

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena.

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no

destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

Delitos contra la propiedad:

Artículo 173 inciso 16: (Incurre en el delito de defraudación) ...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Artículo 183 del Código Penal: (Incurre en el delito de daño) ...En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Artículo 184 del Código Penal: (Eleva la pena a tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes):

Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

- **Delitos contra las comunicaciones**

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.
Delitos contra la administración de justicia

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

Delito sobre los Sistemas Informáticos' El 15 de noviembre de 2012, la Fiscalía General de la CABA dictó la Resolución 501/12, a través de la cual, creó como prueba piloto por el término de un año, el Equipo Fiscal Especializado en Delitos y Contravenciones Informáticas, que actúa con competencia única en toda la Ciudad Autónoma de Buenos Aires, con el fin de investigar los delitos informáticos propiamente dichos, y aquellos que se cometen a través de internet que por su complejidad en la investigación o su dificultad en individualizar a los autores, merecen un tratamiento especializado. Existen diferentes delitos informáticos en eucl es objeto el sistema informático, tales como Delito de Daño: La ley 26388 incorpora como segundo párrafo del art. 183 CP “En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos, o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño”.

Delito Agravado: La ley 26388 agrega dos nuevas agravantes al art. 184 CP: 5) “ejecutarlo en archivos, registros, bibliotecas, …o en datos, documentos, programas o sistemas informáticos públicos”; 6) “ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio. público”.[12]

- **Uruguay**

El Estado uruguayo aprobó en el año 2007 la ley Nª 18.237 denominada EXPEDIENTE ELECTRÓNICO cuyo único artículo autoriza el uso de expediente electrónico, de documento electrónico, clave informática simple, firma electrónica, firma digital y domicilio electrónico constituido en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. Se hace referencia a esta ley porque es evidente que será de amplio tratamiento para el caso de los delitos informáticos, puesto que las conductas que autoriza pueden ser objeto de un ciberdelito.

Los delitos informáticos no son de tratamiento específico por la legislación uruguaya, puesto que no existe una ley de ilícitos informáticos (no puede haber delito sin ley previa, estricta y escrita que lo determine - principio de legalidad-), ni tampoco un título específico relativo a los mismos en el Código Penal uruguayo. Se tratará de otorgar una vez más, la participación que al Derecho Penal corresponde dentro del ordenamiento jurídico, como último remedio a las conductas socialmente insoportables, que no pueden ser solucionadas por la aplicación de otro proveimiento jurídico que no se la aplicación de la sanción más gravosa de todo el sistema.

- **Colombia**

En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” (Ley de protección de la información y de los datos, 2009)

[12] http://delitosinformaticos.fiscalias.gob.ar/wp-content/uploads/2014/02/CyberCrime-Informe-Final-2013-flip.pdf

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadísticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas.

- **España**

En *España*, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de noviembre en el BOE número 281, de 24 de noviembre de 1995. Éstos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nª 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

A la hora de proceder a su investigación, debido a que una misma acción puede tener consecuencias en diferentes fueros, comenzará la investigación aquel partido judicial que primero tenga conocimiento de los hechos delictivos cometidos a través de un medio informático, si durante el transcurso de la investagación, se encuentra al autor del delito y pertenece a otro partido judicial, se podrá realizar una acción de inhibición a favor de este último para que continue con la investigación del delito.

- **México**

En *México* los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el título noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

- **Venezuela**

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001. (Ley Especial de Delitos Informáticos, 2001)

La Ley tipifica cinco clases de Delitos:

Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposo del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).

Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19);

Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22);

Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24);

Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

- **Estados Unidos**

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

- **Chile**

En Chile el 28 de mayo de 1993, se promulgó la ley 19.223 pero no fue hasta la fecha 7 de junio de 1993 que ésta se publicó. Esta ley, tipifica y sanciona los denominados Delitos Informáticos. (Delitos informáticos, 1993)

Los delitos tipificados en la Ley 19.223 consideran como un bien jurídico la calidad, la pureza e idoneidad de la información que está contenida en cualquier sistema automatizado de tratamiento de la información. Además, no solo se protege el bien mencionado anteriormente, sino que también los siguientes:

El patrimonio, en el caso de los fraudes informáticos.

La privacidad, intimidad y confidencialidad de los datos, en el caso de espionaje informático.

La seguridad y fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos probatorios mediante algún sistema o medio informático.

El derecho de propiedad sobre la información y sobre los elementos físicos y materiales de un sistema de información, en el caso de los delitos de daños.

ANÁLISIS LEGAL EN EL ECUADOR:

Políticas Públicas Para Proteger Los Sistemas Informáticos Desde El Estado (Código Orgánico Integral Penal – Coip)

Nuestra legislación regula penalmente las conductas ilícitas relacionadas con la informática, y es así como en el nuevo Código Orgánico Integral Penal COIP, manifiesta ciertas políticas para la protección de los sistemas informáticos

Los delitos informáticos tipificados en la normativa penal son los siguientes:

A. Art. 202 inciso 1.- Violación de claves o sistemas de seguridad, para acceder u obtener información protegida contenida en sistemas de información
   Prisión: Pena específica 6 meses a 1 año; multa de 500 a 1000 dólares.
B. Art. 202.2 Cesión, publicación, utilización o transferencia de datos personales sin autorización
   Prisión: Pena específica 2 meses a 2 años; multa de 1000 a 2000 dólares.
C. Art. 262 Destrucción o supresión de documentos o información por empleado público depositario de la misma. Reclusión menor ordinaria: Pena específica 3 a 6 años.
D. Art. 353. 1 Falsificación electrónica Varias
   Pena específica: Depende del tipo de falsificación de acuerdo con los artículos 337 al 353
E. Art. 415.1 Destrucción, alteración o supresión de contenidos de sistema informático o red electrónica Prisión: Pena específica 6 meses a 3 años; multa de 60 a 150 dólares
F. Art. 415.2 Destrucción de infraestructuras físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos Prisión: Pena específica, 8 meses a 4 años; multa de 200 a 600 dólares
G. Art. 553.2 Los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos

Prisión: Pena específica, 6 meses a 5 años; multa de 500 a 1000 dólares; los autores podrán ser colocados bajo la vigilancia especial de la autoridad por 2 años a lo menos y 5 a lo más.

CONCLUSIONES

- Con respecto a los delitos contra la propiedad se señalan las zonas más vulnerables a los delitos contra las propiedades como las parroquias Febres Cordero, Tarqui, Mapasingue, Bastión Popular y las ciudadelas de la Alborada y Sauces, las cuales son las que precisamente presentan las mayores tasas de delincuencia.
- El tema phishing se lo considera como falsificación electrónica, ya que es una actividad ilícita porque implica suplantación de páginas web o correos electrónicos para causar un perjuicio a otra persona valiéndose de herramientas informáticas que modifiquen información o ya sea simulando un mensaje de correo electrónico hacia una persona; suplantando un sitio oficial para así captar información relevante como login y contraseña en el caso de los bancos y así poder realizar un sin número de transacciones, por lo cual los phisher serán considerados reos de falsificación electrónica que con ánimo de lucro o por causar daño realizan esta actividad.
- Para obtener el mejor modelo omnidireccional, para los delitos contra la propiedad es el modelo Exponencial.
- Rasgos con la distribución desigual de activos existentes en el espacio urbano y con el mapa de factores de riesgos sociales de la ciudad, delitos a la administración y fe pública se presentan con más intensidad en los Sauces, Alborada, Guayacanas y Urdes, puesto que son las zonas son más céntricas.
- El Variograma que se elija refleje el patrón de continuidad espacial de la variable analizada. En los mapas se muestra la relación existente entre los diferentes delitos dentro de la ciudad de Guayaquil correspondiente al área urbana. Cada punto se ubica en el plano referencial por cada cuadrícula del mapa. Así, el plano está formado por cuadrantes donde existen puntos en los cuales la tasa de delitos se muestra por puntos en cada parte de la ciudad. Para obtener el mejor modelo omnidireccional, para los delitos a la administración y fe pública es el mejor modelo es el Gaussiano.
- Las zonas como los Sauces, Alborada Guayacanes y Urdesa que están en el sector norte de la ciudad son las que precisamente presentan las mayores tasas de delincuencia en lo que a robo de vehículos se refiere, siendo estas de nivel socio económico más alto. Para obtener el mejor modelo omnidireccional, para los delitos de vehículos el mejor modelo es el Gaussiano.

- Las zonas más vulnerables y pobres, como los Guasmos y Febres Cordero son las que precisamente presentan las mayores tasas de delincuencia y un mayor índice en tenencias de armas de fuego: por parte de las pandillas. Para obtener el mejor modelo omnidireccional, para los delitos contra las personas el modelo Exponencial.

BIBLIOGRAFÍA

Acevedo, P.J. (2010). Colegio Técnico Industrial Jose Elías Puyanaarea. Recuperado de Tecnología e informaticafloridablanca2010.

Acosta, A. (2010). Análisis de coyuntura: una lectura de los principales componentes económicos, políticos y sociales de Ecuador durante el año 2009. Flacso-Sede Ecuador. Acosta.

Alcívar, C., Domenech, G. A. y Ortiz, K.M. (2015). La Seguridad Jurídica Frente a los Delitos Informáticos: AVANCES, Revista de Investigación Jurídica. 10 (12). Cajamarca ISSN 2220-2129

Álava, M. C., Cortés Maya, G. M., & Faggioni Cubillos, R. (2013). Guayaquil de mis temores: Los miedos urbanos de los jóvenes guayaquileños (Doctoral dissertation).

Arce, C. (2009). Plagio y derecho de autor. Recuperado de https://www.plagios.org/plagio-y-derechos-de-autor-celin-arce-g/

Baranda, A. (2009). Se disparan ciberfraudes 91% Baranda, Antonio. El Norte [Monterrey, Mexico] 10 May 2009, p.13.

Bentley, L., Suthersanen, U. & Torremans, P. (2010). Global Copyright, Edward Elgar London: Publishing.

Block, M. M. (1856). Dictionnaire de l'Administration Francaise, Librairie Administrative de Veuve Berger-Levrault et fils, París.

Bolaños, F. y Gómez C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. Recuperado de http://recibe.cucei.udg.mx/revista/es/vol4-no3/computacion01.html

Burrough, P.A., & McDonnell, R.A. (1998). Principles of Geographical Information Systems. Oxford Univ. Press, New York.

Calderón, J. (2004). Análisis Espacial de la distribución de la delincuencia en Guayaquil. Tesis de Grado ESPOL, Guayaquil, Ecuador.

Castells, M. (1999). La Era de la información: economía, sociedad y cultura, vol. 1, México: Siglo XXI Editores.

Camones, C., & María, C. (2013). Disertación doctoral. Estudio exploratorio acerca de los desafíos sociales actuales y futuros para la función de Dirección de Recursos Humanos en la provincia del Guayas.

CLIRSEN. (1998). Mapa de Uso Actual del Suelo y Memoria Técnica del Cantón, Guayaquil.

Codificación 13. Registro Oficial Suplemento 426 de 28-dic-2006. Última modificación: 13-oct-2011. Estado: Vigente. Recuperado de http://institutoautor.org/story.php?id=316

Correa, C., Batto, H., Czar de Zalduendo, S. y Nazar, F. (1987). Cap. El derecho ante el desafío de la informática. En "Derecho informático", p. 295. Buenos Aires: Depalma. ISBN 950 14 0400 5

Correa, C. (1998). Acuerdo trips. Régimen Internacional de la Propiedad Intelectual, Ciudad Argentina, Buenos Aires.

Correa, C. (2005). Propiedad Intelectual y Políticas de Desarrollo, Ciudad Argentina, Buenos Aires.

Colorado, P.E. (2008). Recuperado de http://pcolorador.blogspot.com/2008/04/delitos-informaticos_14.html [Historia de Delitos Informáticos

Conde O'Donnell, H., González, C. y Heredia, A. (2009). Delito Informáticos. Argentina. Recuperado de http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf

Convention for the Protection of Industrial Property, United International Bureaux for the Protection of Intellectual Property, Ginebra, 1969.

Cuervo, J. (2008). Delitos informáticos: Protección penal de la intimidad. Publicado en http://www.INFORMÁTICA-jurídica.com/trabajos/delitos.asp.

Curtis, G. (2006). The Cave Painters: Probing the Mysteries of the World's First Artists. NY, USA: Knopf. ISBN 1-4000-4348-4.

Cuenca, A. (2012). El delito informático en el Ecuador. Una nueva tendencia criminal del siglo XXI. Su evolución, punibilidad y proceso penal. Quito, Ecuador.

DIARIO HOY. (2001). Archivo Histórico, Página web del Municipio de Quito destruida por "crackers"; 6-XII.

Delitos Informáticos (Chile). (1993). Recuperado de http://www2.udec.cl/contraloria/docs/materias/delitosinformaticos.pdf

Dutfield, G. & Suthersanen, U. Global Intellectual Property Law, Edward Elgar, (2008). London.

Dutton, H.I. (1984). The patent system and inventive activity during the Industrial Revolution, 1750-1852, Manchester University Press, Manchester.

Ecuador, F. (14 de 05 de 2013). *FOROS ECUADOR*. Recuperado el 01 de 02 de 2014, de FOROS ECUADOR: www.forosecuador.ec.

Espinosa, P. y Clemente, M. (2001). Teorías explicativas del delito desde la psicología jurídica., Madrid: Dykinson.

ESPOL. (2 de 10 de 2000). *ESPOL*. Recuperado el 01 de 02 de 2014, de ESPOL: www.espol.edu.ec

Fiscalía Gobierno Index. (2015). Recuperado de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html.

Garfinkel, S. y Spafford, G. (1999). Seguridad y comercio en el web. Madrid: McGraw-Hill.

González, G. (1990). El libro de los virus y la seguridad informática. RA-MA.

González, M., González, C. y Suárez, C.P. (2003). Seguridad en la información: el problema de la distribución de claves II Congreso Internacional Sociedad de la Información y del Conocimiento. CISIC. Universidad Pontificia de Salamanca, Campus de Madrid. McGraw-Hill. Madrid.

Gutiérrez, J.D. (2005). Seguridad digital y hackers. Anaya Multimedia.

Haz, A. R. (2011). Universidad Técnica Particular de Loja. Trabajo a distancia Investigación Jurídica. Recuperado de http://www.slideshare.net/hazandres/indice-tesis-sobre-migracion-andres-haz1

Instituto de derecho de autor. (2010). Recuperado de http://institutoautor.org/story.php?id=3156 http://www.propiedadintelectual.gob.ec/propiedad-intelectual/

IEPI. (1999). OMPI: Organización Mundial de la Propiedad Intelectual.

INDECO. (octubre de 2007). Estudio sobre la práctica fraudulenta conocida como phishing. Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing, pp. 5-169.

Jiménez, R. (2015). 21% de los internautas de Latinoamerica hacen transacciones en Internet todos los días: [Source: NoticiasFinancieras] NoticiasFinancieras [Miami] 13 Sep. 2013.

Lascaux, C. Ministerio de Cultura francés. Archivado del original 29 de noviembre de 2015. Consultado el 13-02-2008.

Laaz, S., María, L., & Falcón Méndez, A. R. (2013). Estructura del sector microempresarial formal e informal en la ciudad de Guayaquil sector sur.

LATINOAMÉRICA TECNOLOGÍA EFE. (23 de febrero de 2016). Brasil y Ecuador, entre países con mayor número de correos fraudulentos: News Service [Madrid]. Recuperado de http://search.proquest.com/docview/1767341742/6A5A0A64127149F2PQ/1?accountid=130858

Leiva, R. (1992). La protección penal de la intimidad y el delito informático. Chile: Editorial Andrés Bello.

Ley de la propiedad Intelectual. Registro oficial No. 320. Recuperado de http://www.correosdelecuador.gob.ec/wp-content/uploads/downloads/2015/05/LEY_DE_PROPIEDAD_INTELECTUAL.pdf

Ley de protección de la información y de los datos (Colombia). (2009). Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Ley Especial de Delitos Informáticos (Venezuela), http://web.archive.org/web/20140902120028/http://www.tsj.gov.ve/legislacion/ledi.htm

Ley Especial de Delitos Informáticos (Venezuela). (2001). Recuperado de http://web.archive.org/web/20140902120028/http://www.tsj.gov.ve/legislacion/ledi.htm

Lipsyc, D. (2006). Derecho de autor y derechos conexos. Buenos Aires: Ediciones unesco/cerlalc/ Zavalía.

Modificación al Código Penal sobre la incorporación de los Delitos Informáticos (Argentina). Recueprado de http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Morquecho, E. M. (01 de 01 de 2009). Analisis del impacto de la educación gratuita en las Universidades Estatales de la ciudad de Guayaquil. Guayaquil, Guayaquil, Ecuador.

Nájera, É. (2007). Phishing: un problema con nuevas aristas Elisa Nájera. Economista [Mexico City] 07 May 2007. http://search.proquest.com/docview/336496721/fulltext/A1893C35BC764A9BPQ/3?accountid=130858

Organiacion mundial de la propiedad intelectual. (2013). Recuperado de http://www.wipo.int/wipo_magazine/es/2013/03/article_0001.html

OMPI. (2013). 173 países. La lista completa de las naciones miembros se encuentra en el sitio web de la Organización Mundial de Propiedad Intelectual: [http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=2].

Orellana, W. O. (1998). Manual de Criminología. México: Editorial Porrúa.

Páez, J. J. y Acuario del Pino, S. (2010). Derecho y Nuevas Tecnología. Editora Corporación de Estudios y Publicaciones.

Pecoy, M. (2012a). Criminalidad informática. En "Delitos informáticos", pp.23-26. Montevideo: Universidad de Montevideo. ISBN 978 9974 8342 4 8

Pecoy, M. (2012b). Concepto de delito informático. En "Delitos informáticos", Montevideo: Universidad de Montevideo, pp.29-32.

Pecoy, M. (2012c). Aspecto subjetivo. En "Delitos informáticos". Montevideo: Universidad de Montevideo, p. 36.

Perez, Á. (1986). Curso de Criminología. Bogotá Colombia: Editorial Temis., p. 54.

Publicado por Gonzo. (2010). Delitos Informáticos. Recuperado de http://gonzo-stelgon.blogspot.com/2008/11/historia-de-delitos-informticos.html

Publicado por la Fiscalía General del Estado Ecuador. Recuperado de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Regimen Común sobre Derechos de Autor y Derechos conexos Decisión 351 de la Comunidad Andina de Naciones, 17 de diciembre de 1993.

Reyes, A. (2005). NoticiasFinancieras: Advierten aumento de fraudes en internet para sector bancario; [Source: El Economista], [Miami]. Consultado el 14 June 2005, p. 1. Recuperado de http://search.proquest.com/docview/468014267/fulltext/A1893C35BC764A9BPQ/4?accountid=130858

RICYT. (21 de 04 de 1995). RICYT. Recuperado el 01 de 02 de 2014, de RICYT: www.ricyt.org

Rolnik, H. (2002). La guerre des brevets: Quelle stratégies? Mémoire de dess en Ingénierie de l'Intelligence économique. Université de Marne-la-Vallée. Recuperado de: [http://memsic. ccsd.cnrs.fr/docs/00/33/49/01/PDF/mem_00000361.pdf], p. 8.

Schmitz, Ch. (2011). Legislación chilena de Propiedad Intelectual, Jurídica de Chile, Santiago.

Schmitz, Ch. (2006). Propiedad Industrial y Derecho de Autor: ¿Una división vigente?, en Morales Andrade, Marcos (ed.). Temas actuales de Propiedad Intelectual, Lexis Nexis, Santiago, pp. 21-53.

Silva, A. (s.f.). Sección 1823. Aldea Universitaria Juan de Villegas, Venezuela. Recuperado de http://es.slideshare.net/amarilissilva1823/aanali-de-delitos-informaticos-44107643

Stack, A. (2011). International Patent Law, Edward Elgar, London.

Secretos Industriales II (La Propiedad Intelectual). Recuperado de http://www.ugr.es/~plagio_hum/Documentacion/06Publicaciones/ART003.pdf

Sistema de información sobre Comercio Exterior. (2015). Recuperado de http://www.sice.oas.org/int_prop/nat_leg/ecuador/L320ind.asp

UNESCO. (1995-2007). Recuperado de http://portal.unesco.org/culture/es/ev.php-URL_ID=39442&URL_DO=DO_TOPIC&URL_SECTION=201.html

Valencia, A. M. (18 de 09 de 2013). Los avances de la tecnología en Ecuador. *El Comercio* - Tecnología, p. 1.

Valencia, V. (2007). Aprenden usuarios de banca electrónica lección del phishing. El Norte [Monterrey, Mexico]. Consultado el 5 de marzo de 2017, p. 7. Recuperado de http://search.proquest.com/docview/312004693/fulltext/A1893C35BC764A9BPQ/1?accountid=130858

Whitehouse, D. (s.f.). Ice Age star map discovered. BBC. Consultado el 09-06-2007. Recuperado de caribeña.eumed.net/delincuencia-guayaquil/

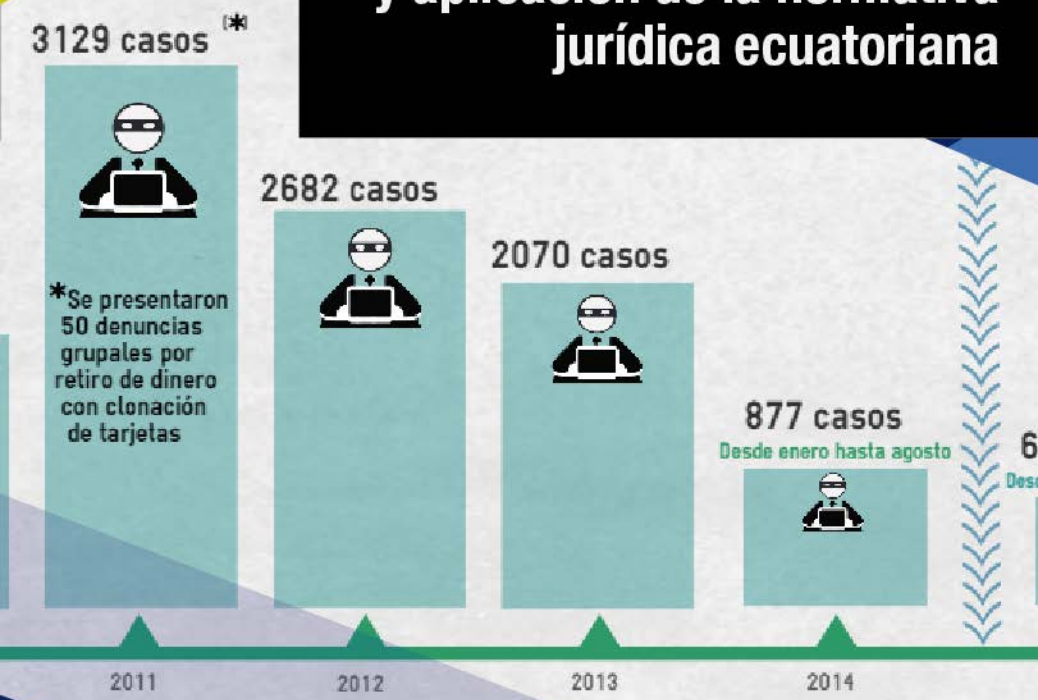
Zapata, F. (s.f.). Sociedad del Conocimiento y Nuevas Tecnologías. En: [http://www.oei.es/salactsi/zapata.htm].

Bibliografía Jurídica:

- Constitución Del Ecuador, 2008-2016
- Código Orgánico Integral Penal. Actual, (Ecuador), 2014
- Código Civil Ecuatoriano. Editora Corporación De Estudios Y Publicaciones, 2010

Universidad Ecotec

Análisis espacial de los delitos y aplicación de la normativa jurídica ecuatoriana



Compiladores

Carlos Esteban Alcívar Trejo, Mgs.
Juan Tarquino Calderón Cisneros, Mgs.

ISBN: 978-9942-960-10-8