



**Marzo 2015**

## **INTERNET Y SEGURIDAD: IMPLICACIONES SOCIALES Y SUS ALCANCES**

**Ing. Com. Bolívar Espinoza Santos**

Magíster en Educación Superior por la Universidad de Guayaquil.

Ingeniero Comercial Catedrático de la Universidad de Guayaquil.

bolivar.espinozas@ug.edu.ec

bol\_espinoza@hotmail.com

**Arq. Luis Fernando Terán Viteri**

Magíster en Educación Superior por la Universidad de Guayaquil.

Arquitecto-Urbanista por la Universidad de Guayaquil.

Catedrático de la Universidad de Guayaquil.

luis.teranv@ug.edu.ec

teranluis58@gmail.com

### **RESUMEN**

En este artículo pretendemos analizar cuáles son las implicaciones con respecto a la seguridad al acceder mediante el uso del internet, y qué se necesita para obtener una conexión confiable. Es de entender que todos los individuos estamos inmersos o relacionados de una u otra manera con un medio electrónico y que en la actualidad también inciden en las actividades diarias. Por lo consiguiente se intenta mencionar algunos de los campos de vulnerables, así como las implicaciones de este delito a nivel cibernético, tanto en el aspecto técnico como en el legal, ya que en los actuales momentos, todo está globalizado, y por último, se concluye en la necesidad de cambiar la óptica en el enfoque del tema, hallando la necesidad de un cambio que induzca en una mejor utilización.

Palabras clave:

Delito cibernético, Internet confiable, seguridad informática, medio electrónico.

### **ABSTRACT**

In this article we intend to analyze what are the implications with respect to security access through the use of the internet, and what is needed to get a reliable connection. It is understood that all individuals are immersed or related in one way or another with an electronic medium and that now also affect daily activities. Therefore trying to mention some of the vulnerable, as well as the implications of this crime to cyber level, both technical and legal side, because currently, everything

is globalized, and finally, we concluded the need to change the optics in the approach to the topic, finding the need for a change that induces in better utilization.

Key words:

Cybercrime, Reliable Internet, computing security, electronic media.

## 1. INTRODUCCION.

La aspiración de este artículo es el de incentivar al lector en un aspecto tan importante como es la seguridad en internet, es que, la mayoría de personas lo maneja pero desconoce muchos aspectos inherentes donde pueden afectarlo seriamente, con consecuencias de futuros agravantes, y van de la mano con los futuros avances tecnológicos y deja la interrogante ¿qué pasará si el control se escapa de la manos del individuo o de toda una comunidad?

Es por ello que al iniciar la investigación se han tomado ciertos tópicos para dar una mejor definición de los temas que competen a nuestro estudio:

### a. Delito cibernético.

*Figura 1: Delincuente cibernético*



Fuente: <http://info.uas.edu.mx/wp-content/uploads/2014/02/delitos.jpg>

Al igual que cualquier tipo de delito, éste, puede ocurrir de manera inesperada en cualquier sitio, momento y bajo cualquier forma; los métodos que se utilizan son variados, dependiendo del objetivo a conseguir. En realidad lo que lo diferencia del crimen común es el elemento informático inherente a este, es decir que para definirlo debe de existir la necesidad primaria de comprobar, que haya sido realizado mediante el uso de un ordenador, una red o cualquier hardware.<sup>1</sup>

Las Naciones Unidas elaboraron un Manual de Prevención y control de Crímenes Informáticos, en él se estipulan como tales a: la falsificación de documentos, accesos sin permiso y al fraude, pero en la actualidad, el delito implica una gama cada vez más amplia de modalidades y alcances. (ONU, 2000).

En consecuencia a los delitos, se han podido clasificar en varios tipos siendo el primero, el que se adquiere haciendo lo más común, es decir, una descarga para conectar el equipo a un sitio urdidor. Son todas las variedades de virus, los phishing, manipulación de datos, robo de identidad, fraudes bancarios y todo tipo de troyanos, en realidad la facilidad o no de acceso dependerá de que tan endeble sea el usuario.<sup>2</sup>

En el otro tipo se encuentran actividades como acoso, localización de infantes, chantaje, espionaje, actividades de terrorismo, manipulación en el mercado de valores, generalmente uno de los medios utilizados es el contacto asiduo con la víctima, como por ejemplo las redes sociales o grupos de discusión, la idea es sacar la mayor información de la víctima y atacar en el momento oportuno, tratando de poner la menor sospecha posible.

#### **b. Seguridad informática.**

La seguridad informática se puede definir como todos los medios posibles para prevenir su violación y privacidad, generalmente son tipos de normas como: métodos, técnicas, procedimientos, que prueben su eficacia y durabilidad.

La seguridad debe cumplir con varios propósitos, es decir, encontrar todos los medios posibles para que el usuario halle la confianza necesaria al usar su computadora o medio informático.

Por otro lado, el ser confiable es otro aspecto a tomar en cuenta, si no existiera ese factor no podrían hacerse las millones de transacciones que se realizan hoy en día.

Adicionalmente, es importante y técnicamente valedero llevar a cabo la actualización de datos y mucho más delicado si se tienen varios usuarios compartidos.

Debido a que las computadoras actúan de forma mecánica, la seguridad se ve intervenida por el acceso a diferentes dispositivos y en líneas generales su función es actuar, antes que ocurran los

---

<sup>1</sup> Krone, T. (2005). *High Tech Crime Brief. Australian Institute of Criminology.* Canberra, Australia. ISSN 1832-3413.

<sup>2</sup> Zeviar-Geese, G. (1997-98). *The State of the Law on Cyberjurisdiction and Cybercrime on the Internet.* California Pacific School of Law. Gonzaga Journal of International Law. Volumen 1.

delitos, o hallar los medios de corrección y prevención antes que lleguen a ocurrir los mismos. Uno de los dispositivos que ayuda a la detección de usuarios no autorizados, son los mouse<sup>3</sup> que permiten identificar huellas dactilares.

*Figura 2: Mouse*



**Fuente:** <http://www6.pcmag.com/media/images/1654-biolink-u-match-mouse.jpg>

En fin, los mecanismos son muchos, van desde una simple contraseña de acceso, instalación de un buen antivirus, hasta el empleo de firewall que restringen el ingreso entre redes, así también, como los cifrados encriptados de datos para evitar lectura de terceros que pudieran extraer una información importante.

### **c. Internet confiable.**

Para hacer del internet un medio de comunicación más seguro, intentamos encontrar esa seguridad, esto va a depender de la acción que se realice, por ejemplo la comunicación en los niveles empresariales. Esto dependerá de la estructura organizacional de una empresa para que el usuario sienta confianza en una compañía de prestigio y fama frente a otra totalmente desconocida. En realidad la credibilidad solo la otorga la constancia en el tiempo, obviamente fortalecida con medios adicionales que mantengan en contacto permanente al usuario con la compañía, el usuario debe entonces comprobar toda la información proveniente de dicha compañía: dirección, teléfonos, correos electrónicos, calidad en la atención, en fin, solo así se lograría hacer una compra on-line, en las compañías más confiables.<sup>4</sup>

El internet no solo es inseguro para transacciones de pagos, también lo es por información, es decir, un dato o consejo falso puede ser tan perjudicial como el robo de información, existe un estudio estadístico que demuestra científicamente que las personas al relacionarse vía internet con información tipo “cadena” presentan una elevada aceptación y creencias a los mismos.

---

<sup>3</sup> *Mouse con lector de huella dactilar es un periférico para la seguridad del ordenador y seguridad informática en general.*

<sup>4</sup> *Mendoza, A. (s.f.). Cómo determinar si una empresa es o no confiable en internet. Recuperado el 27 de enero de 2015 de <http://mercadeoglobal.com/blog/confiabilidad-empresa/>*

Pero de dónde salió la creencia? Quién le dio validez al asunto? La internet no tiene los medios legales para validar de forma certera la validez de una hipótesis o creencia originada en una información o encuesta, sin duda este es otro campo donde algunas personas inescrupulosas pueden sacar ventaja del mismo, para tener más información de un caso específico el lector puede ir a: <http://www.razonypalabra.org.mx/anteriores/n46/opaez.html>

#### **d. Medio electrónico.**

Se define como tal a todo instrumento físico o intangible que tiene la capacidad de contener y transportar información digitalizada, bajo este concepto tanto el internet como todo tipo de computadora al igual que los smartphones cumplen esas características.

Los medios electrónicos tienen una participación activa en nuestras vidas, por ejemplo en el área de la educación se vuelve un recurso audiovisual indispensable, en el área de la comunicación es imposible dejar de lado un recurso como tal, convencionales, inalámbricos igual cumplen su función, la radio y la televisión se mantienen como elementos importantes pues han sabido adaptarse a los cambios tecnológicos.

## **2. CONTENIDO.**

### **a. Antecedentes.**

Con la creación de la computadora, la humanidad nunca imaginó que en la actualidad, se hubiese alcanzado un desarrollo tan impresionante con respecto a la tecnología de la comunicación. Luego de esto aparece el internet y el mundo cambia radicalmente. Internet es una red<sup>5</sup> que comunica a varias computadoras, estas son en un número de cientos de millones a nivel de todo el mundo, con ello se puede compartir información entre máquinas.

---

<sup>5</sup> Red de computadoras, es también conocida como red de ordenadores o red informática, son todos los equipos informáticos que están conectados entre sí usando diferentes software y hardware con el objetivo de compartir información.

Figura 3: Redes de Computadoras



Fuente: <http://redesdecomputadorasads.blogspot.com/>

Según el sitio oficial ilifebelt.com, en Latinoamérica hay más de 231,000,000 usuarios de Internet; Este dato representa el 39% de la población. En el mundo, la penetración de Internet es en porcentaje del 33%, esto representa que la tendencia en Latinoamérica indica que se está convirtiendo en una región con alto volumen de usuarios de la red puesto que su porcentaje de penetración ya es mayor al promedio global. (iLifebelt Times, 2012)

Los países latinoamericanos que en la actualidad tienen una mayor penetración en el Internet de más del 50% son: Colombia, Uruguay, Argentina, Puerto Rico y Chile. Seguidos por los países que tienen una participación entre el 40 y el 50% como son: República Dominicana, Costa Rica, Panamá, Brasil, y Venezuela.

En cuanto al nivel de intensidad en el uso del internet son: Argentina, Chile y Venezuela.

Existe un 60% que tienen como modalidad conectarse desde el hogar, un dato bastante alentador y positivo puesto que en años anteriores existía un alto porcentaje que solo se conectaba a través del trabajo o en lugares de acceso público. Otro dato mayormente relevante es que ya un 20% se conectan a través de su dispositivo celular o Smartphone.

#### **b. Orígenes del problema.**

Lejos de demostrar su importancia, la internet nunca se tomó como lo que es en la actualidad, y lo peor es que tampoco en estos tiempos se puede predecir su futuro, es que en realidad ha cambiado demasiado en esta dos últimas décadas desde que nació; al crecer su éxito comercial creció también la forma de vulnerar o trampear sus seguridades, llegando a ser cada vez más frágiles, pasando a ser de un elemento simplemente informativo de carácter social, a un ambiente

de comercio y finanzas, en forma que casi todo intento de protección es rápidamente vulnerado, desde ahí comenzó el asunto más álgido, que ha causado tantos problemas a grandes compañías e incluso a gobiernos enteros.

Figura 4: Vulnerabilidad de los Sistemas



Fuente:

<http://www.viruslist.com/sp/images/vlweblog/207764619.jpg>; <http://jonathanmelgoza.com/blog/wp-content/uploads/2013/06/seguridad-informatica-jonathanmelgoza.jpg>

### c. Áreas involucradas.

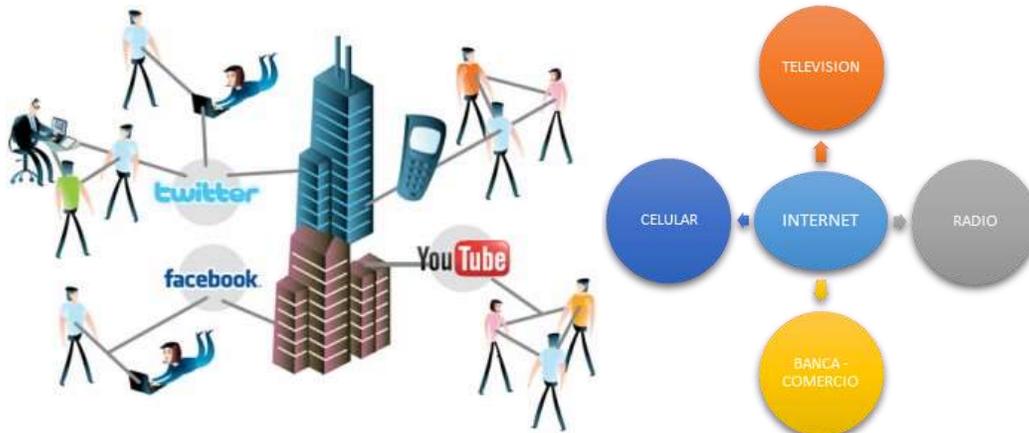
El asunto es que, en todas estas áreas, el internet está involucrado en menor o mayor porcentaje, imposible evadir o dejar de lado su existencia y peor aún será en el devenir, por ende su influencia es vital en el ser humano.



Figura 5: Áreas que se conectan

Fuente: Autores de este artículo

Figura 6: Medios Involucrados



Fuente: <http://negocios.maimonides.edu/wp-content/uploads/2013/12/redes-sociales-negocios-402x300.jpg>; y Autores de este artículo.

### **Implicaciones Sociales.**

Es de entender que debido a los avances tecnológicos, los individuos, empresas y naciones se han visto en la imperiosa necesidad de salvaguardar sus conexiones, pero, esto no reduce o elimina las implicaciones que los seres humanos nos enfrentamos día a día, es por ello que en este trabajo de investigación mencionaremos las principales implicaciones que puedan suscitarse con las diferentes variantes y que se mencionaran en cada caso:

#### **i. Dañar la imagen honorable de las personas**

Esto posibilita la intromisión indebida de datos personales, no autorizados, acoso informático, difamación, calumnias, incitación al odio racial o discriminación. Ponemos como ejemplo los siguientes casos:

En un Artículo de la Agencia Carabobeña de noticias, se describen algunos ataques de seguridad virtual más trascendentales que ocurrieron en el 2014. (Hernandez, 2014)<sup>6</sup>

Las Compañías Panda Security y The Cloud Security Company, presentaron un importante resumen de varios de los ataques más sonados y hace un recordatorio a los internautas: “Reforzar la seguridad de las claves de acceso y evitar el usar las mismas en todos los soportes, con la finalidad de ser menos vulnerables a los delincuentes informáticos”.

#### **1. eBay y PayPal, fueron los primeros afectados**

<sup>6</sup>Hernandez, V. (23 de Diciembre de 2014). *Los 6 ataques de seguridad virtual más famosos de 2014*. Recuperado el 27 de Enero de 2015, de <http://acn.com.ve/especial-los-6-ataques-de-seguridad-virtual-mas-famosos-de-2014/>

En mayo, eBay nos sorprendía pidiendo a los usuarios de PayPal, la página web de pagos online de su propiedad, que cambiaran sus contraseñas de acceso.

Parece que la compañía había confirmado que los ciberdelincuentes habían ya accedido, un par de meses antes, a las cuentas de algunos empleados.

Esto les habría dado acceso a la red interna de la empresa y, desde allí, a la base de datos con nombres de usuarios, teléfonos, direcciones de correo electrónico y contraseñas.

## 2. Imágenes de Hollywood en la red

El ataque que más se había hablado fue en septiembre del año 2014: el CelebGate.

Se filtraron y divulgaron imágenes íntimas de la ganadora del Óscar en 2013, Jennifer Lawrence, así como de otras modelos y actrices, esto dio mucho de qué hablar.

*Figura 7: Personajes de Hollywood*



Fuente:[http://cdn.larepublica.pe/sites/default/files/imagecache/img\\_noticia\\_640x384/imagen/2014/10/10/imagen-fotos-intimas.jpg](http://cdn.larepublica.pe/sites/default/files/imagecache/img_noticia_640x384/imagen/2014/10/10/imagen-fotos-intimas.jpg)

Apple, aseguró que las cuentas de estas celebridades “fueron comprometidas por un ataque muy específico sobre los nombres de usuario, contraseñas y preguntas de seguridad”. Una práctica “que se ha vuelto muy común en Internet”.

De esta manera, Apple negó que el hackeo a estas cuentas se produjeran por una vulnerabilidad en servicios como iCloud o ‘Find my iPhone’.

## 3. 200.000 fotografías de Snapchat robadas

Tras las modelos y actrices de Hollywood, en octubre fueron las personas registradas en Snapchat los que vieron comprometida la seguridad de sus archivos.

Snapchat es una aplicación móvil con la que se pueden enviar fotos y mensajes que se eliminan entre uno y diez segundos después de haberlos leído.

Figura 8: snapchat hackeado imágenes.



Fuente: <http://gdatavenezuela.com/wp-content/uploads/2014/12/snapchat.jpg>

Aunque Snapchat no guarda las imágenes de sus usuarios, otra aplicación, Snapsave, disponible para Android e iOS, sí lo hace, lo que permitió el robo de 200.000 fotografías.

## ii. Fomentar el libertinaje sexual.

Pues permite propagar imágenes e informaciones exhibicionistas, provocativas e incitan la pornografía infantil.

### 1. Sitios oscuros

Actualmente, todos los elementos que observamos en la web no son los únicos que existen también hay muchos sitios no visibles, bastante protegidos incluso protegidos con cierta ilegalidad, este sitio se denomina Deep Web (Red Profunda) y su acceso es bastante sencillo, tan solo se descarga un programa y ahí se otorga una clave de internet que es difícil de hacer seguimiento y generalmente está llena de pornografía.

Es tal la gravedad del asunto que se permite intercambiar todo tipo de material generalmente sexual y registrada por todos los delincuentes cibernéticos en realidad es un sitio donde no hay normas que incluye venta de drogas y todo tipo de acciones ilegales.

*“La pornografía infantil a través de medios electrónicos es un mal que parece difícil de erradicarse, pues lamentablemente su consumo en internet se sigue dando”.* Tovar,C. (2014).

### 2. La comprensión de la psicología en los mundos virtuales. <sup>7</sup>

Por otro lado existen cinco dimensiones fundamentales a la hora de entender el vínculo de unión entre una herramienta como Internet y la conducta social: la sincronía generada a partir de la rapidez de establecer una conversación con otras personas que están al otro lado de la red.

---

<sup>7</sup> Joinson, A. N. (2003). Understanding the psychology of internet behaviour. Virtual worlds, real lives. *Revista iberoamericana de educación a distancia*,6(2), 190.

Se habla también de un determinismo tecnológico, acuñado por Markus en 1994, que asume cómo ciertas características de la tecnología, como por ejemplo el anonimato visual, conducen a determinados resultados psicológicos y conductuales, no siempre positivos para el individuo.

Hay dos tipos de aproximaciones que defienden ese determinismo tecnológico: el primero, predice que la ausencia de pistas sociales en la comunicación a través de los medios implica una comunicación regulada, despersonalizada y desindividualizada.

El segundo, parte de la base de que el diseño de la tecnología supone cambios en la identidad personal o social, lo que a su vez tiene una serie de efectos psicológicos y comportamentales.

Todos estos argumentos se basan en experimentos y estudios que toman como base muchos presupuestos fundamentales de la psicología social, los resultados del uso de la tecnología sobre la conducta proceden no de la tecnología en sí misma, sino también de las elecciones que los individuos hacen sobre cuándo y cómo utilizarla. Asimismo, se menciona también otro modelo alternativo al determinismo tecnológico, la perspectiva del proceso emergente, el cual defiende cómo la interacción entre las intenciones del usuario y el medio elegido para comunicarse puede conllevar consecuencias no previsibles y no intencionadas.

Aspectos negativos de la conducta intra e interpersonal se ponen de manifiesto en Internet. El autor insiste en el hecho de que no debería sorprendernos que Internet, como otras tecnologías anteriores, se haya asociado con la conducta desviada, el crimen y otros efectos negativos para la gente y la sociedad.

Se consideró adictiva la conducta de aquellos participantes que pasaban una media de 8,48 horas a la semana conectados en Internet. Se comprobaron también cómo los usuarios a los que se les atribuía una conducta patológica en Internet, mostraban más tendencia a utilizar con mayor frecuencia unos servicios de Internet que otros como por ejemplo, la realidad virtual, apuestas, juegos, la búsqueda de apoyo social, conocimiento de nueva gente, etc.

Hablando de la paradoja Internet. Katz, J. E., & Rice, R. E. (2006).<sup>8</sup>, ésta se propone aislar cada vez mas al ser humano por el abuso de la tecnología entre ellos.

### **iii. Perjudicar la propiedad intelectual en general.**

Pues contribuye a la distribución ilícita de obras con propiedad intelectual legalizada, fomenta la piratería de programas, incluso difunde contenido publicitario de manera ilícita.

---

<sup>8</sup> Katz, J. E., & Rice, R. E. (2006). *Consecuencias sociales del uso de Internet*. Editorial UOC.  
<https://books.google.es/books?hl=es&lr=&id=4tTtCNrkhKkC&oi=fnd&pg=PA9&dq=implicaciones+sociales+por+el+uso+del+internet&ots=SxK4oEldPQ&sig=J21U0EfVmmGVKsoh5K3iVf67nSY>

## 1. Robo de 5 millones de contraseñas de Gmail.

Un foro de ciberseguridad ruso publicó el mes de septiembre de 2014 un archivo con más de 5 millones de cuentas de Gmail.

*Figura 9: Vulnerabilidad de contraseñas Gmail*



**Fuente:**<http://www.24horas.cl/incoming/article1137405.ece/ALTERNATES/w620h350/Hacking%20Gmail%20account%20with%20password%20reset%20system%20vulnerability.jpg>

Según varios expertos, más del 60% de las combinaciones de usuarios y contraseñas eran válidas. Sin embargo, Google afirmó que esta información estaba “desactualizada”, es decir, que estas cuentas o no existían o sus usuarios no accedían a ellas. Al igual que Apple, aseguró no tener evidencia de que sus sistemas fueran comprometidos.

## 2. Viator y los datos bancarios de sus usuarios.

También en septiembre, Viator sufrió un ataque de seguridad mediante el que los ciberdelincuentes consiguieron acceder a datos bancarios de sus usuarios. Según aseguró la compañía, el ataque se produjo entre el 2 y 3 de septiembre de 2014.

Parece ser que Viator fue consciente del hackeo debido a las quejas de sus clientes sobre cargos no autorizados en las tarjetas utilizadas en su servicio.

Como siempre y, para evitar en lo posible el robo de más datos, Viator les pidió que cambiaran su contraseña de acceso a la cuenta y que prestasen atención a los movimientos de las tarjetas de crédito.

## 3. Ataque a Dropbox.

Un usuario de la web Pastebin, punto de encuentro para hackers y especialistas en seguridad informática, aseguró disponer de las contraseñas de 7 millones de usuarios de Dropbox y, para demostrarlo, compartió una parte de ellos.

Figura 10: Dropbox



Fuente:<http://elblogdeangelucho.com/elblogdeangelucho/wp-content/uploads/2014/10/drohack.jpg>

A través de su Blog oficial, Dropbox no tardó en anunciar que sus servicios no fueron hackeados, sino que esos datos fueron robados de otros servicios y serían los mismos que se utilizan para acceder a su plataforma.

Al igual que a todos los que acceden a un sistema informático, Dropbox también recomienda: No utilizar las mismas contraseñas para todos los servicios y activar la verificación en dos pasos.

#### **4. Hackers' atacan la tienda online de playstation de sony.** (Reuters, Thomson, 2014)<sup>9</sup>

La compañía afirmó que el servicio se interrumpió durante ese día por 2 horas y no estuvo comprometida ninguna información.

Figura 11: PlayStation



**Fuente:**<http://s1.reutersmedia.net/resources/r/?m=02&d=20141208&t=2&i=997776196&w=&fh=&fw=&ll=192&pl=155&r=LYNXMPEAB70Z0>

---

<sup>9</sup> Reuters, Thomson. (8 de Diciembre de 2014). *Hackers atacan tienda online de PlayStation de Sony: Reuters*. Obtenido de <http://lta.reuters.com/article/entertainmentNews/idLTAKBN0JM1TW20141208>

En una fuente noticiosa se indicó que la compañía Sony verificó que este corte existió y que estaba encontrando los motivos sin que se haya pasado información valiosa. Así mismo afirmó esta transnacional que el problema había sido superado y que los internautas, pese a tener dificultades de acceso ese lunes, luego habían tenido normalidad en el servicio.

El diario Financial Times afirmó que usuarios de PlayStation online se percataron del anuncio que anunciaba el problema en sus máquinas; también hace poco la Sony Pictures Entertainment sufrió un percance serio que hizo paralizar el servicio web durante siete días, luego del atentado los culpables hicieron público información confidencial de la compañía e información secreta de filmes que no se habían producido aún..

#### **iv. Cuarto: Poner en riesgo la seguridad nacional y el orden público.**

Pues contribuye a facilitar atentados y desórdenes públicos así como actividades terroristas

En la actualidad uno de los mayores problemas que están enfrentando muchas de las naciones, donde se han llegado a formar bandas de criminales organizadas, delitos cometidos por la Red mediante el uso de computadoras.

En principio el internet se creó con la finalidad de facilitar las comunicaciones entre los usuarios y se difundió para este fin, pero es muy cierto que en el mundo están operando bandas de criminales haciendo un mal uso de esta herramienta por medio del internet.

En las diferentes naciones existen las amenazas terroristas, haciendo un mal uso de las nuevas tecnología, esto preocupa mucho a los gobernantes, ya que el efecto destructivo, puede llegar a causar mucho daño así como lo señala Ortega, J.(2002)<sup>10</sup>

Que la preocupación por las muchas amenazas que realizan los terroristas, usando medios tecnológicos mediante la Red, sean las excusas perfectas para llegar a la sustitución de los derechos por la lógica de la seguridad, y desemboque en el uso de Red Echelon”, organización dirigida por la Agencia Nacional de Seguridad de los Estados Unidos (NASA) y formada, por países anglosajones, esta Red a estado funcionando por décadas de forma clandestina. Además se trata de un programa que tiene como finalidad el rastreo de las comunicaciones en el espacio digital, ósea, una “macro vigilancia”, esto ha significado que cualquier tipo de comunicación como son telefónicas o fax, han sido interceptadas de forma rutinaria por los servicios de inteligencia. En inicio fue creada para evitar ataques terroristas, pero se han usado para averiguar asuntos de índole económico y político.

Asimismo, y como ejemplo más reciente, se recuerda los atentados terroristas ocurridos en el territorio de los Estados Unidos, fecha fatídica 11 de septiembre de 2001, lo que ha generado preocupación y ha dado lugar a una legislación emergente, la “USA Patriot Act” (24 de octubre de

---

<sup>10</sup> Ortega, J. J. L. (2002). *La admisibilidad de los medios de investigación basados en registros informáticos. Cuadernos de derecho judicial*, (9), 77-112.

2001), que en el ámbito de las comunicaciones permite con una única autorización judicial, válida para solo el territorio de los Estados Unidos, intervenir teléfonos o direcciones de correo electrónico que podrían usarse en actividades terroristas. También, se imponen reglas rigurosas a los que proveen servicios de internet.

En Sevilla<sup>11</sup> España, en uno de los congresos donde se imparten conferencias sobre la responsabilidad penal en Internet, se menciona como ejemplo la ejecución de un ciudadano que lo habían secuestrado por una organización terrorista en el país de Irak y que la misma se estaba difundiendo por medio del Internet en todo el mundo.

Esto quiere decir, que las grabaciones de hechos delictivos se difunden por el mundo, de manera fácil y simple con solo el libre acceso a una página Web. Por esta razón, apunta Gonzalo Quintero Olivares<sup>12</sup> que el mencionado Grupo de los Ocho habló en una reunión en París en el año 2000 la intranquilidad por el uso de Internet, donde organizaciones terroristas o simplemente criminales pueden echar abajo aparatos, bloquear servicios públicos y sistemas financieros, o que pueden reproducir el número de víctimas de definitivos delitos hasta niveles incalculables.<sup>13</sup> Gómez, M. A. (2010).

#### **d. Los delitos cibernéticos.**

Cada vez es más común que haya crímenes relacionados con las TIC, sin dejar atrás que algunos comportamientos continúan siendo más relevantes por su frecuencia o a veces por su nivel de gravedad. Anexo a esto también es cierto que todas estas van cambiando de acuerdo al tiempo, ya que se adaptan a este.<sup>14</sup> (Carlos, 1988) Con todo esto hay que recalcar que el uso de Internet es un 'boom' de este siglo, lo cual nos ha llevado a ocasionar desencuentros o enfrentamientos entre culturas, sistemas políticos, jurídicos, etc., al mismo tiempo nos ha llevado a un mundo de facilismo para causar daños.<sup>15</sup> (Thomas, 2000), (Moron, 2002).

Cuando se manifiesten estos delitos cibernéticos en los ámbitos políticos-criminales, se pondrá a prueba cada una de las instituciones y su efectividad, ya que están a cargo de que no se cometan estos y así poder lograr un eficiente trabajo con la persecución y captura de los responsables de cualquier delito involucrando el Internet. (Pérez, 2007, págs. 649-669)

---

<sup>11</sup> Congreso "Protección de la Propiedad Intelectual". Sevilla, 24 y 25 de junio de 2004. Sociedad General de Autores de España.

<sup>12</sup> Gonzalo Quintero Olivares. "Internet y Propiedad Intelectual". En Cuadernos de Derecho Judicial. 2001. X. Internet y Derecho Penal.

<sup>13</sup> Gómez, M. A. (2010). *Delitos y Delinquentes*. Editorial Club Universitario.

Disponible: <https://books.google.es/books?id=vnFelnQCH2sC&pg=PA119&dq=delitos+informaticos&hl=es&sa=X&ei=9k6TVPO0Hle5OLb4gagC&sqi=2&ved=0CE8Q6AEwBw#v=onepage&q=delitos%20informaticos&f=true>

<sup>14</sup> Para comprobar esta evolución y la problemática jurídico-penal específica en épocas anteriores v. Carlos María Romero Casabona, Poder informático y seguridad jurídica, Madrid, Fundesco, 1988, pp. 13 y ss.

<sup>15</sup> Esta doble perspectiva es compartida por Douglas THOMAS y Brian D. LOADER, *Cybercrime. Law enforcement, security and surveillance in the information age*, London, Routledge, 2000, p. 2.

V. sobre ello Esther MORÓN LERMA, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, 2ª ed., Pamplona, Aranzadi, 2002, pp. 25 y ss.

### **i. Clasificación de los delitos informáticos**

De acuerdo al apdo. XIV del Preámbulo de la LO 5/2010, de 22 de junio, se dice que existen dos apartados para clasificar los delitos cibernéticos. El primero, tiende a involucrar cualquier daño o perjuicio, alterar o suprimir o hace inaccesibles datos o programas informáticos ajenos, u obstaculizar el correcto funcionamiento de este. El segundo, tiende a involucrar la revelación o el descubrimiento de algún secreto, donde estaría siendo desautorizado al acceso a esta información, vulnerando cualquier medida de seguridad que el programa informático requiere.

Sin embargo, la realidad es otra, ya que no se ha podido llegar a un acuerdo para definir el tipo de delito informático, y cuando se usa este aspecto es para generalizar, agrupando varias conductas de nivel informática alcanzando la relevancia penal.

Como consecuencia tenemos que las nuevas tecnologías que últimamente conocemos, incrementan cuantitativa y cualitativamente infringiendo los derechos a la libertad, indemnidad sexual e intimidad: afectaría a delitos clásicos, a los que se aplica la informática, lo cual implicaría que esas nuevas tecnologías permiten que se realicen nuevas formas de cometer delitos informáticos tradicionales. Por otro lado también surgen crímenes nuevos involucrando la informática como suelen ser el espionaje o el 'hacking', sabotaje o piratería informática.

Todo esto se puede incluir en una lista de varios delitos informáticos, que también se los puede llamar delitos telemáticos, en los cuales se encuentra el cibercrimen. (Juanes Peces, 2012, págs. 123-124)

Este hecho de que exista Internet, significa que tenemos una nueva de red de comunicación, la cual nos permite compartir información desde un lugar a otro del planeta. Cualquier persona en cualquier parte del mundo se puede informar a partir de una determinada página Web. Esto nos deja fascinados, como el nuevo invento de gran potencial que, por muy raro que veas, no tiene dueño. Porque es así, el Internet no es un sistema en el que alguien pueda tener el control de entrar y salir con información, dejar y recogerla cuando quieran, o saber la información de todo el mundo; por esto es que Moles Plaza<sup>16</sup> (Moles, 2003) Señala que la Red es la que nos regula y maneja el Internet a medida que lo modifican.

De acuerdo a cada una de estas actividades del Internet es donde se centra el estado, para regir con firmeza el control de que es lo que fluye por este medio, y así tomar medidas si es necesario; en cuanto no atenten a los derechos, o que puedan ser constitutivos de ilícitos penales.

---

<sup>16</sup> Ramón J. Moles Plaza. *Derecho y control en Internet. La regulabilidad de Internet*. Ariel Derecho. 2003.

Esto significa que el Internet tiene una capacidad informativa, como nos señalan Juana López Moreno y Emilio Manuel Fernández<sup>17</sup> (Lopez, 2001), que la Red es el centro permanente en donde pasan noticias, actividades informáticas, comerciales, económicas, etc., lo que significa que Internet está tomado como un punto de referencia para todo.

Por otro lado, esta maravilla de Internet y los medios informáticos nos han llevado a otro efecto, que más bien nos constituye a un 'defecto' y es que nos está causando una enorme dependencia de este, y de todas sus tecnologías que se derivan, por lo que autores como Hugo Daniel Carrión<sup>18</sup> (Carrion, 2002) nos dice que sin el Internet o Informática, las sociedades colapsarían por completo, haciéndose ver el 'computer dependency', también nos recalca que existe una relación intrínseca entre la Informática y el Poder.

Conocemos también a una persona llamada hacker, la cual es experta en sistemas informáticos, y por lo general es dentro de las edades entre 15 y 25 años. Se podría decir que la intención de estos hackers no es de dañar, ni nada por el estilo (hacking directo), sino más bien de una satisfacción que la podemos llamar personal, la cual se basa en burlar los sistemas de seguridad dispuestos. Aunque esto no nos represente un importante nivel de riesgo, cada vez que el hacker se manifieste como hacker o cracker, no son dos conductas tan distintas, pero si con la misma ilicitud penal.

Ahora lo que se le conoce como hacking indirecto es la conducta que opera como medio para cometer otros delitos como fraude, piratería, sabotaje, etc... la cual también se relaciona como cracking; entonces el autor concluye que en el hacking indirecto la intención del delincuente si es dañar, de fraudar, etc... aun así no desapareciendo del delito de acceso indebido.

En la actividad del hacker, señala Mir Puig<sup>19</sup> que la conducta de mero acceso o intrusismo informático encierra un evidente peligro, puesto que puede destruir datos por negligencia, puede causar bloqueos se sistemas, y la localización de las deficiencias en la seguridad del sistema informático por dicha conducta.

Existen otras conductas más graves aún, como son los fraudes informáticos, sabotaje informático, etc. En estos casos podría ocurrir que lo que primeramente era una simple actividad de "fisgón en la Red" se acaba convirtiendo en un cometimiento delictivo de cracker.

---

<sup>17</sup> Juana López Moreno (Secretario Judicial) y Emilio Manuel Fernández García Fiscal. "La World Wide Web como Vehículo de delincuencia: Supuestos frecuentes". En Cuadernos de Derecho Judicial. 2001. X. Internet y Derecho Penal.

<sup>18</sup> Daniel Carrión, Hugo. "presupuestos para la incriminación del Hacking". *Derecho informático y las nuevas tecnologías*. No. 4 Septiembre de 2002. Tesis presentada por Hugo Daniel Carrión

<sup>19</sup> Carlos Mir Puig. "Sobre algunas cuestiones relevantes del derecho penal en Internet". En Cuadernos de Derecho Judicial, 2001. X. Internet y Derecho Penal.

Figura 12: Fisgón Informático



Fuente: <http://static.betazeta.com/www.fayerwayer.com/up/2013/03/fbi1111111111-960x623.jpg>

Además, Hugo Daniel Carrión concluye que: El hacking es el presupuesto necesario del craking (todo crak supone un hack previo), pero cuando se consuma este ilícito, el anterior queda subsumido en él por reunir las exigencias del tipo, dándose un concurso aparente de delitos por razones de especialidad.

Lo contrario importa una doble persecución penal (non bis in ídem), situación que se encuentra proscripta por el principio constitucional de legalidad.

Al Analizar ambos sistemas se puede llegar a pensar en una postura intermedia, en la que ambos sistemas no trabajan por separado, sino que por el contrario, son complemento uno del otro. La unión de ambos podría presumir el amparo, en todas sus dimensiones, de un mundo virtual; es decir, todas aquellas vinculaciones de carácter delictivo que se pueden generar a través de la Red, lo que no deja de ser lo más cercano a la verdad.

Pues las Naciones Unidas realiza el siguiente esquema de delitos informáticos:(Naciones Unidas, 2010)<sup>20</sup>

- ✓ Fraudes cometidos mediante manipulación de computadoras
  - Manipulación de los datos de entrada.
  - La manipulación de programas.
  - Manipulación de los datos de salida.
  - Fraude efectuado por manipulación informática.
- ✓ Falsificaciones informáticas
  - Como objeto cuando se alteran datos de los documentos almacenados en forma computarizada
  - Como instrumentos, ya que las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

---

<sup>20</sup> Naciones Unidas. (2010). 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Recuperado el 22 de enero de 2010 de [https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A\\_CONF.213\\_9/V1050385s.pdf](https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf)

- ✓ Daños o modificaciones de programas o datos computarizados
  - Sabotaje informático.
  - Virus.
  - Gusanos.
  - Bomba lógica o cronológica.
  - Acceso no autorizado a Sistemas o Servicios.
  - Piratas informáticos o hackers
  - Reproducción no autorizada de programas informáticos de protección legal.

En uno de los Manuales de las Naciones Unidas se indica que a nivel internacional se eleva la dimensión de la prevención y control de los delitos, ya que los delitos informáticos constituyen nuevas formas de crimen transnacional y su combate requiere de mayores prevenciones y de una eficaz cooperación a nivel internacional concertada con todos los usuarios que utilizan la Red.

*Figura 13: Seguridad en Internet*



Fuente: <http://alinstantenoticias.com/portal/wp-content/uploads/2014/08/seguridad.jpg>

En definitiva las Naciones Unidas simplifican en 4 ítems los principales inconvenientes que la rodean en el área de crímenes informáticos: (Naciones Unidas, 2010).

- ✓ Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- ✓ Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- ✓ Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- ✓ No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

**e. Convenios internacionales de seguridad informática.<sup>21</sup>**

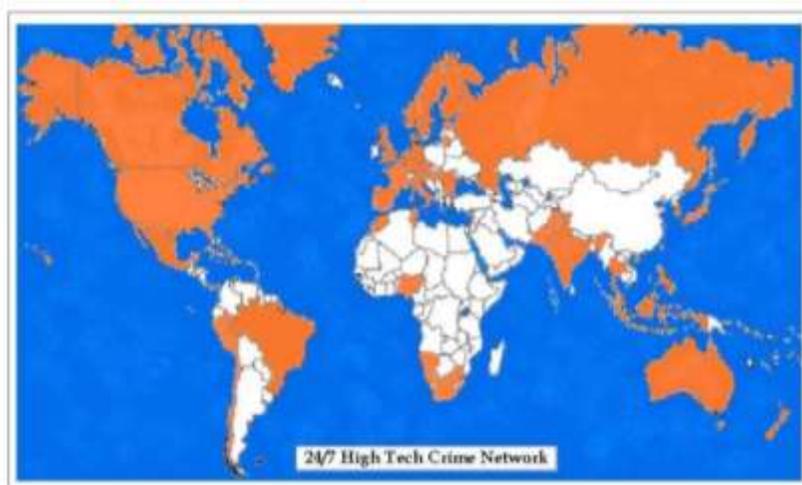
---

<sup>21</sup> La red G8 24/7 Para la Conservación de Información Declarada de Protocolo.  
[http://www.oas.org/juridico/english/cyb\\_pan\\_G8\\_sp.pdf](http://www.oas.org/juridico/english/cyb_pan_G8_sp.pdf)

La primera opción que resulta al revisar los convenios internacionales de seguridad informática es la falta de acuerdos entre ellos, con el agravante que cada país tiene diferente concepción según el caso y cuando un crimen cibernético se convierten en transnacionales su castigo debe de ser penalizado por una cooperación mancomunada de los países inmersos en un determinado problema.

Figura 14: Mapa del G8

### La Red 24/7 del G8 para Delitos de Alta Tecnología



Fuente: [http://www.oas.org/juridico/english/cyb\\_mex\\_coop.pdf](http://www.oas.org/juridico/english/cyb_mex_coop.pdf)

Una de las redes internacionales mayormente conocidas es la red de contacto llamada G8 24/7 cuyo objetivo es tratar delitos de alta tecnología cuando representan retos significativos a los países o estados participantes, su nombre viene de la acción continua y perenne las 24 horas del día entre los agentes homologados encargados en cada país, para esto se utiliza un proceso de Asistencia Jurídica Mutua (MLAT) para intercambio de información.

Para el 2007 contaba con 48 miembros y los contactos deben tener como requisitos el hablar el inglés, como forma de establecer contactos sin barreras idiomáticas, al mismo tiempo el contacto debe poseer conocimientos técnicos, tener la disponibilidad extendida como su nombre lo indica, las 24 horas del día los 7 días de la semana, finalmente el contacto debe poseer conocimientos jurídicos tanto de su país como de cualquier otro de los estados asociados.

#### f. Alcances.

Los gobiernos, específicamente el de Estados Unidos está estudiando una oferta, así lo señala el sitio web: [www.fayerwayer.com](http://www.fayerwayer.com),<sup>22</sup> el mismo trae a colación una propuesta que estaría en estudio, donde el Gobierno de Estados Unidos estaría por respaldar un proyecto para espiar las comunicaciones a través del Internet. El mismo indica: (FBI, 2013). “El FBI quiere tener acceso a ciertas conversaciones por chat o VoIP, tal como actualmente puede escuchar conversaciones telefónicas”.

Los Estados Unidos pretenden impulsar el proyecto del FBI tratando de reducir al mínimo las conversas empleando el internet aplicando multas de \$25000 diarios si no se cumple la normativa.

Lo que quería la FBI era usar VoIP como medio obligado para espiar los chateos pero se prefirió hacerlo tan solo con las empresas incumplidas de la norma, en la actualidad las compañías ratifican que el método no resultó, en base a lo nuevo que se propone no podrían ejercer control. (NYTimes).

### **3. CONCLUSIONES.<sup>23</sup>**

Toda persona que trabaja en internet debe estar bien claro que está realizando una actividad abierta, pública, totalmente reconocible, todo lo que expone es seguido por el proveedor, incluso lo que se trata de investigar ya que existen una serie de dispositivos, cookies, spam y demás, esa información es rápidamente recopilada, filtrada, investigada, además que el módem que permite el acceso a internet es la puerta que utiliza el hacker o cracker para realizar su trabajo de pirateaje y peor si utilizan una broadband, en resumen, el internet es incontrolable y las posibilidades de librarse de ataque es imposible, sin embargo hay métodos sencillos que pueden ayudar en algo para hasta cierto punto librarnos de inclusiones:

Utilizar software libre: este tipo de programas tiene la característica de poseer un open source editable, que lo hace poco común frente a los programas estándar, hasta cierto punto es una gran ventaja.

Evitar toda transacción comercial en especial si no se tienen referencias de la compañía a usar, las páginas más seguras acaba en “s” luego del http.

En los correos se pretende usar la opción de “correo oculto” para que éstos se vean como privados.

---

<sup>22</sup> FayerWayer (2013). *Gobierno de EE.UU. podría respaldar proyecto para espiar comunicaciones a través de Internet*, Recuperado el 31 de enero del 2015 de <https://www.fayerwayer.com/2013/05/gobierno-de-ee-uu-podria-respaldar-proyecto-para-espiar-comunicaciones-a-traves-de-internet/>

<sup>23</sup> Pc World. (2009). *El futuro de internet: lo que nos queda por ver*: Recuperado el 25 de Enero de 2015 de <http://www.pcworld.com.mx/Articulos/5307.htm>.

Cambiar constantemente de claves de usuarios y actualización de sistema operativo, esto haría más problemático el acceso a un usurpador.

La decadencia del "internet explorer" como buscador predeterminado ha sido la causa de serios conflictos delincuenciales de ahí su futuro final al igual que el Outlook.

El empleo de todo tipo de protectores actualizados: antivirus, antispyware, firewalls, ayudan de forma sustancial.<sup>24</sup>

#### 4. REFERENCIAS BIBLIOGRAFICAS

##### Bibliografía

- Avilés Gómez, M. (2010). *Delitos y delincuentes*. Club Universitario. Obtenido de <https://books.google.es/books?id=vnFelnQCH2sC&pg=PA119&dq=delitos+informaticos&hl=es&sa=X&ei=9k6TVPO0Hle5OLb4gagC&sqi=2&ved=0CE8Q6AEwBw#v=onepage&q=delitos%20informaticos&f=true>
- Carlos, V. (1988). *Poder Informático y seguridad jurídica*. Madrid: Fundesco.
- Carrion, D. (2002). *Presupuestos para la incriminación del Hacking, Derecho informático y las nuevas tecnologías*. nd: nd.
- Hernandez, V. (23 de Diciembre de 2014). *Los 6 ataques de seguridad virtual más famosos de 2014*. Recuperado el 27 de Enero de 2015, de <http://acn.com.ve/especial-los-6-ataques-de-seguridad-virtual-mas-famosos-de-2014/>
- iLifebelt Times. (16 de noviembre de 2012). *Uso y Estadísticas de Internet en Latinoamérica al año 2012: iLifebelt Times*. Obtenido de iLifebelt Times: <http://ilifebelt.com/uso-de-internet-en-latinoamerica-infografia/2012/11/>
- Joinson, A. N. (2003). Understanding the psychology of internet behaviour. Virtual worlds, real lives. *Revista iberoamericana de educación a distancia*, 6(2), 190.
- Juanes Peces, A. (2012). *Reformas del Código Penal, Perspectiva Económica tras la entrada en vigor de la ley Organica 5/2010 de 22 de junio. Situación jurídico-Penal del Empresario*. Madrid: El Derecho y Quantor, S. L. c/Lagasca. Obtenido de <https://books.google.es/books?id=Q6xIQe8YKSYC&pg=PA124&dq=delitos+ciberneticos&hl=es&sa=X&ei=seySVKXWHcTtgwSHtoGAAQ&ved=0CEQQ6AEwBQ#v=onepage&q=fals>e
- Lopez, J. (2001). *World Wide Web como vehiculo de delincuencia: Supuestos frecuentes*. nd: nd.
- Moles, R. (2003). *Derecho y control en Internet. La regulabilidad de Internet*. nd: Ariel.
- Moron, E. (2002). *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*. (2da. ed.). Pamplona: Aranzadi.
- Naciones Unidas. (2010). 12 Congreso de las Naciones Unidas sobre Prebención del Delito y Justicia Penal. *A/Conf.213/9* (pág. nd). Salavador Brasil: nd.

---

<sup>24</sup> Seguridad en Internet (n.d) Recuperado el 26 de enero de 2015, <http://www.eumed.net/coursecon/ecoinet/seguridad/>

- Pérez Álvarez, F. (2007). *De los delitos informáticos al Cibercrimen*. Salamanca: Universidad de Salamanca y los autores, 1ra. edición. Obtenido de [https://books.google.es/books?id=\\_qi1P44Vay8C&pg=PA669&dq=delitos+ciberneticos&hl=es&sa=X&ei=seySVKXWHcTtgwSHtoGAAQ&ved=0CFoQ6AEwCQ#v=onepage&q&f=true](https://books.google.es/books?id=_qi1P44Vay8C&pg=PA669&dq=delitos+ciberneticos&hl=es&sa=X&ei=seySVKXWHcTtgwSHtoGAAQ&ved=0CFoQ6AEwCQ#v=onepage&q&f=true)
- Reuters, Thomson. (8 de Diciembre de 2014). *Hackers atacan tienda online de PlayStation de Sony: Reuters*. Obtenido de <http://lta.reuters.com/article/entertainmentNews/idLTAKBN0JM1TW20141208>
- Thomas, D. y. (2000). *Ciberdelincuencia: Las Fuerzas del orden, la seguridad y la vigilancia en la era de la información*. Londres: Routledge.
- Tovar, C. (2014, 06 de septiembre). El ciberespacio profundo alimenta el porno infantil. *EL Mañana* [en línea]. Disponible en: <http://www.elmanana.com/elciberespacioprofundoalimentaelporno infantil-2560691.html>
- Trujillo, V. (2012). *Implicaciones sociales de la informática*. Recuperado: 28 de enero de 2025. Disponible: <http://www.buenastareas.com/ensayos/Implicaciones-Sociales-De-La-Informatica/5366745.html>
- Katz, J. E., & Rice, R. E. (2006). *Consecuencias sociales del uso de Internet*. Editorial UOC. <https://books.google.es/books?hl=es&lr=&id=4tTtCNrkhKkC&oi=fnd&pg=PA9&dq=implicaciones+sociales+por+el+uso+del+internet&ots=SxK4oEldPQ&sig=J21U0EfVmmGVKsoh5K3iVf67nSY>
- Krone, T. (2005). High Tech Crime Brief. Australian Institute of Criminology. Canberra, Australia. ISSN 1832-3413.
- Zeviar-Geese, G. (1997-98). The State of the Law on Cyberjurisdiction and Cybercrime on the Internet. California Pacific School of Law. Gonzaga Journal of International Law. Volumen 1.