



## LA DELINCUENCIA INFORMÁTICA

**Ugarte Almeida Tamara Johanna**

Master en Dirección Estratégica y Gestión de la Innovación  
por la Universidad de Alicante, Universidad Autónoma de Barcelona, Universidad Carlos III de Madrid. Ingeniera en Gestión  
Empresarial Internacional por la Universidad Católica Santiago de Guayaquil. Catedrática de la Universidad de Guayaquil y  
Universidad Católica Santiago de Guayaquil.  
tamy\_ugarte2711@hotmail.com

**Acosta Ramírez Nadia**

Magíster en Educación Superior por la Universidad Católica de Santiago de Guayaquil. Licenciada en Lengua Inglesa por la  
Universidad Laica Vicente. Catedrática de la Universidad Católica Santiago de Guayaquil.  
nadia-acosta@hotmail.com

**Soto Medina Lanny Sofía**

Magíster en Educación Superior por la Universidad de Guayaquil. Licenciada en Lengua Inglesa por la Universidad Laica  
Vicente.  
Catedrática de la Universidad de Guayaquil.  
[sofilu\\_pro-ec@hotmail.com](mailto:sofilu_pro-ec@hotmail.com)

### Resumen

Esta investigación se refiere a la delincuencia informática, que es un delito que vincula a las personas que violan las leyes y es castigado de acuerdo a lo estipulado por la Ley, por hacer daños en contra de otras personas, entidades u organismos que por lo general son utilizados por computadoras y a través del internet. Los delitos informáticos se clasifican en cuatro grupos, el primero Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, como segundo se tiene a los delitos informáticos; en tercer lugar, delitos relacionados con el contenido y el cuarto delitos relacionados con infracciones de la propiedad intelectual y derechos afines. Los tipos de delincuencia reconocidos por las Naciones Unidas son fraudes cometidos mediante manipulación de computadoras, falsificaciones informáticas, daños o modificaciones de programas o datos computarizados, acceso no autorizado a servicios y sistemas informáticos, reproducción no autorizada de programas informáticos de protección legal.

Delincuencia - Informática - Ley - Fraudes - Protección - Legal

### Abstract

This research relates to computer crime, a crime that links people who break the law and is punished according to the stipulations of the law, to do damage against other persons, entities or bodies usually they are used by computers and through the Internet. Computer crimes are classified into four groups, the first Offences against the confidentiality, integrity and availability of computer data and systems, as second you have to cybercrime; thirdly, the content-related offenses and related crimes fourth infringements of intellectual property and related rights. The types of crime recognized by the United Nations is committed fraud by manipulating computers, computer forgery, damage or changes to programs or computer data, unauthorized access services and computer systems, unauthorized reproduction of computer software legal protection.

Crime - Computer - Law - Fraud - Privacy - Legal

## 1. INTRODUCCIÓN

### Delincuencia<sup>1</sup>

Del latín delinquentia, la delincuencia es la cualidad de delincuente o la acción de delinquir. El delincuente es quien delinque; es decir, quien comete delito (un quebrantamiento de la ley).

La delincuencia, por lo tanto, está vinculada a las personas que violan las leyes y al conjunto de los delitos. Por ejemplo: “En este barrio ya no se puede salir a la calle: la delincuencia domina cada rincón”, “El gobierno prometió nuevas medidas para combatir a la delincuencia”, “La delincuencia de la clase dirigente es el principal flagelo de este país”, “Si no enfrentamos a la delincuencia, no tenemos futuro”, “La desigualdad social está vinculada al crecimiento de la delincuencia”.

Al implicar conductas antijurídicas (contrarias al derecho), a la delincuencia le corresponde un castigo según lo estipulado por la ley. Esta pena dependerá del tipo de delito cometido.

Utilizado para nombrar al colectivo de delincuentes, el concepto de delincuencia está asociado a un grupo de gente que está afuera del sistema y que debe ser reinserado en la sociedad. Las penas que se purgan en prisión están orientadas a esa tarea de resocializar a los delincuentes para que puedan volver a formar parte de la sociedad como elementos productivos y no dañinos.

### Tipos de delincuencia<sup>2</sup>

**Delincuencia menor** es comúnmente cometida por un individuo y cuando muchos dos, teniendo por objetivo la comisión de un delito que podría ser desde una falta menor hasta una grave y calificada, y característica de este tipo de delincuencia es que no es cometida por bandas, no existe una gran planeación en los hechos delictivos o no se opera a gran escala, esta delincuencia es la más común, por popular, la que vemos casi a diario y a la que le tenemos más miedo.

**La delincuencia circunstancial** es la comisión de delitos o crímenes por parte de personas comunes y corrientes, que de la noche a la mañana se ven envueltos en hechos delictivos determinados por el contexto y las circunstancias. En esta categoría no existe planificación, ni premeditación, no obstante la delincuencia circunstancial se diferencia de un accidente, porque en ella pueden establecerse elementos de Juicio que pueden ser agravantes de responsabilidad criminal, el dolo es la intención con la que se comete, contumacia y la alevosía, en ensañamiento con el que se comete la delincuencia.

**La delincuencia instrumental** es la expresión más común y guarda directa relación con los delincuentes crónicos, de carrera u oficio cuya forma vivir y de ser no coincide al respecto de los parámetros que fija la ley, los actos o la conducta delictiva es concebida como medio que sirve para lograr la consecución de bienes materiales, especies y montos de dinero que de otra manera o bajo las normas que dicta la ley, serían imposibles de lograr o conseguir.

**La delincuencia expresiva** corresponde a una categoría de delitos o crímenes determinados por disfunciones psicopatológicas, por tanto su estricta atribución es individual es decir de persona a persona y no es aplicable a organizaciones o regímenes ya sean autoritarios o dictatoriales esta categoría se reconoce como cuando quien al momento de cometer un delito o crimen, incurre en la exageración o desproporción irracional entre la forma delictiva y el logro de objetivos.

---

<sup>1</sup> Definición de delincuencia. Qué es, Significado y Concepto. Disponible en: <http://definicion.de/delincuencia/#ixzz3ab9uSmEk>

<sup>2</sup> Gordillo Hernández Rebeca Berenice. (2014, agosto 8). *Delincuencia y su clasificación*. Disponible en: <http://www.gestiopolis.com/delincuencia-y-su-clasificacion/>

**La delincuencia juvenil** estos delitos son cometidos por jóvenes o menores de edad, este tipo de delincuencia suele recibir gran atención de los medios de comunicación y políticos. Es así porque el nivel y los tipos de crímenes juveniles pueden ser utilizados por los analistas y los medios como un indicador del estado general de la moral y el orden público en un país y como consecuencia pueden ser fuente de alarma y de pánico moral, los crímenes cometidos por jóvenes se ha incrementado desde mediados del siglo XX.

### **Delincuente<sup>3</sup>**

La palabra delincuencia es el término a través del cual, en nuestro idioma, expresamos la acción de perpetrar delitos. La delincuencia en esta comunidad es cada vez más violenta.

Y también a la serie de acciones delictivas vinculadas a una época y lugar, asimismo, se la denomina con este término.

### **Criminal<sup>4</sup>**

Se entiende por criminal a todo individuo que comete un crimen o que está implicado en algún tipo de delito. Como adjetivo calificativo, el término también puede aplicarse a organizaciones delictivas como así mismo a aquellas que luchan en contra de las primeras. Finalmente, también puede ser criminal un acto o hecho que interrumpa el designio de la ley e implica el cumplimiento de algún tipo de delito.

### **Diferencia entre delito y crimen<sup>5</sup>**

Si bien los delitos pueden definirse como las acciones u omisiones dolosas o imprudentes penadas por la ley, según nivel de “afección social” se establecen diferencias entre éstos y los crímenes.

La gravedad que separa delitos de crímenes, se determina por el tipo de pena que conlleva tal o cual infracción de ley (hecho conductual antijurídico). A su vez, la gravedad de la pena depende de algunos criterios tales como:

- Valoración del daño para la víctima.
- Valoración del daño para la sociedad.
- Tipo de presidio.
- Duración del presidio.
- Medidas cautelares.
- Beneficios e Inhabilidades civiles, entre otras.

Por tanto, el crimen se diferencia del delito y las faltas, porque el primero conlleva daños irreparables a los diferentes tipos de víctimas, implica un riesgo objetivo para la sociedad y la aplicación de ley considera en su resolución penas de larga duración, presidio o reclusión efectiva, ausencia de beneficios e inhabilidades públicas perpetuas.

### **Informática<sup>6</sup>**

El término proviene del francés “informatique” (mezcla de las palabras “information” y “automatique”), se trata de la rama ingenieril relativa al tratamiento de información automatizado mediante máquinas. Este campo de estudio, investigación y trabajo comprende el uso de la computación para resolver problemas mediante programas, diseño, fundamentos teóricos científicos y diversas técnicas.

---

<sup>3</sup> Delincuente. Definición ABC Disponible en: <http://www.definicionabc.com/general/delincuencia.php>

<sup>4</sup> Criminal. Definición ABC. Disponible en: <http://www.definicionabc.com/social/criminal.php>

<sup>5</sup> Diferencia entre delito y crimen. Tipos de delincuencia. Disponible en: <http://cristianaraos.com/2012/03/05/tipos-de-delincuencia-clasificacion-general-delito-y-delincuentes/>

<sup>6</sup> Informática. Definición ABC. Disponible en: <http://www.definicionabc.com/tecnologia/informatica.php>

Se considera que una información es tratada de forma automática cuando el proceso comprende la entrada de datos, su procesamiento, y salida.

## 2. CONTENIDO

### Delincuencia<sup>7</sup>

Es un concepto que se usa cotidianamente para referirnos a distintas situaciones. Cuando se habla de delincuencia estamos haciendo referencia al hecho de cometer uno o varios delitos, es una acción que ejercen personas al violar las leyes y por las cuales, en caso de ser condenadas por tales hechos, se deben cumplir un castigo impuesto por un juez.

Por lo tanto, el término “delincuentes” trata de un grupo de individuos que van en contra de las reglas sociales.

### Delincuencia Informática<sup>8</sup>

Son todos aquellos actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de las computadoras y a través del mundo virtual del internet.

Los delitos informáticos no necesariamente pueden ser cometidos totalmente por estos medios, sino también a partir de los mismos.

Por otro lado otros de los muchos ataques que pueden ser dañinos y hasta resultar destructivos siendo realizados por medio de las computadoras y en algunas ocasiones con la ayuda de terceros, estos son algunos casos a mencionar:

- La expansión de virus informáticos
- El envío intensivo de SPAM o como se conoce comúnmente, correo no deseado.
- La falsificación de los remitentes de mensajes con la técnica SPOOFING
- El envío o entrada oculta de los archivos espías o los KELOGGERS

El uso de troyanos/backdoors para controlar determinados sistemas o en su efecto para sustraer información. Como se puede observar cada día aumentan las víctimas de esta forma de delincuencia debido en parte a los avances tecnológicos y la falta de conocimiento del uso apropiado de estas nuevas herramientas, los smartphones han servido para agilizar procesos que solo se podían realizar en una computadora, ahora desde un teléfono puede conectarse al internet y de ahí conectarse a las cuentas bancarias, muchas de estas instituciones han sacado múltiples aplicaciones conocidos como app donde el manejo es más sencillo, que cuando se tratan de conectar desde la computadora, pero de igual forma en ambos casos deben tomarse precauciones y seguridades.

**Imagen No. 1** Delincuencia Informática



<sup>7</sup> Concepto de Delincuencia. Qué es, Significado y Definición. Disponible en: <http://concepto.de/delincuencia/#ixzz3abAxxxBz>

<sup>8</sup> Delitos informáticos. Myprofeciencias. Disponible en: <https://myprofetecnologia.wordpress.com/2011/01/30/delitos-informaticos/>

**Fuente:**<http://www.bsecure.com.mx/featured/symantec-denuncia-ciberespionaje-contra-48-companias/>

### **Clasificación de los delitos informáticos en cuatro grupos:<sup>9</sup>**

#### **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.
- Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

#### **Delitos informáticos:**

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

#### **Delitos relacionados con el contenido:**

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

#### **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**

- Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el “Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa” que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

### **Tipos de delitos informáticos reconocidos por Naciones Unidas<sup>10</sup>**

Son varios los diferentes tipos de delitos informáticos, se puede mencionar algunos de ellos:

---

<sup>9</sup> Tipos de delitos informáticos. Convenio sobre la Ciberdelincuencia. 1/11/2001. Disponible en: [http://www.delitosinformaticos.info/delitos\\_informaticos/tipos\\_delitos.html](http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html)

<sup>10</sup> Tipos de delitos informáticos reconocidos por Naciones Unidas. Delitos Informáticos. Disponible en: <http://www.criminalistica.com.mx/areas-forenses/seguridad-publica/548-delitos-informcos>

## **Fraudes cometidos mediante manipulación de computadoras.**

Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

La manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

**Imagen No. 2** Accesos no autorizados



**Fuente:** <http://www.diariodecultura.com.ar/costumbres-y-tendencias/los-cinco-asuntos-de-mail-mas-usados-para-robar-datos-privados/>

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

## **Falsificaciones informáticas.**

Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

**Imagen No. 3** Falsificación de documentos



**Fuente:** <http://www.legalcity.es/sentencia-del-tsj-sobre-falsificacion-de-documentos/>

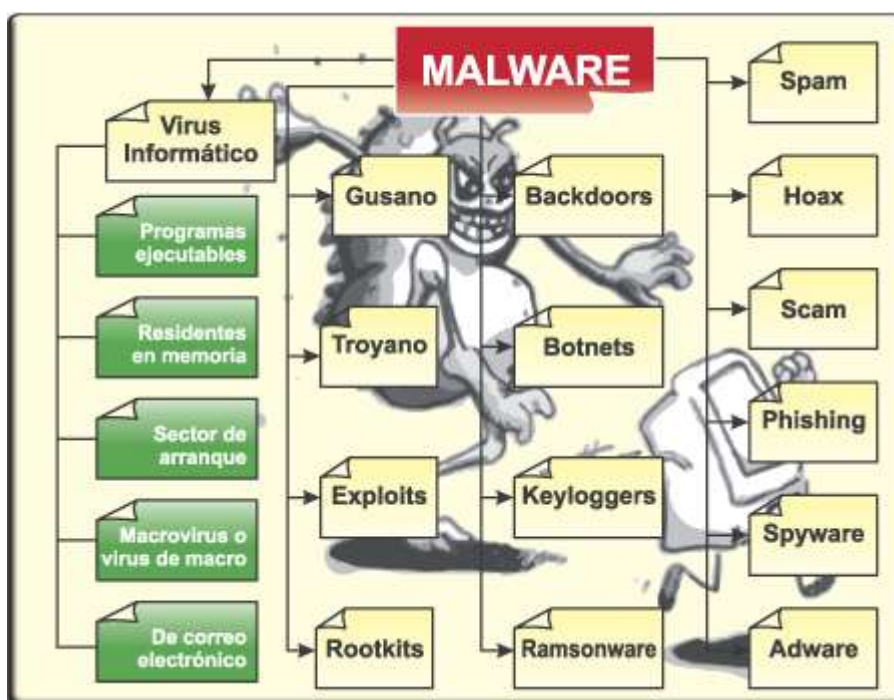
Cuando empezó a disponerse de fotocopadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

#### **Daños o modificaciones de programas o datos computarizados.**

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

**Imagen No. 4** Falsificación de documentos



**Fuente:** <http://virusyconsecuencias.blogspot.com/>



Gusanos. Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

#### **Acceso no autorizado a servicios y sistemas informáticos.**

Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

**Imagen No. 5** Accesos no autorizados



**Fuente:** <http://www.iprofesional.com/notas/146237-Conozca-6-tecnologas-para-aumentar-la-seguridad-de-su-empresa-ante-delincuentes-informticos-y-reales>

Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

#### **Reproducción no autorizada de programas informáticos de protección legal.**

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

**Imagen No. 6** Copias de Programas



**Fuente:** [http://www.rialproducciones.com/duplicaciones\\_cd.php](http://www.rialproducciones.com/duplicaciones_cd.php)

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

#### **Los cuidados que debemos tener ante la delincuencia informática.<sup>11</sup>**

Los ciberataques no solo van dirigidos a robar dinero e información, también buscan dañar nuestros equipos (hardware) sin ningún motivo aparente. Para ello, los terroristas informáticos se sirven de diversas “maniobras”:

**Introducción de datos falsos:** por esta técnica se logra que se emita información falsa desde el mismo dispositivo del usuario afectado haciendo ver que el propio usuario está publicando o transmitiendo esa información.

**Caballo de Troya:** esta técnica consiste en introducir un programa o rutina dañina escondida en un programa o aplicación aparentemente inofensiva que infecta el dispositivo cuando el usuario instala inadvertidamente.

**Redondeo:** consiste en infectar un ordenador que maneje cuentas de pago o banca electrónica para que transfiera cantidades muy pequeñas (casi imperceptibles) de manera continuada a una cuenta específica de destino.

**Uso de llaves maestras virtuales:** estos programas decodifican cualquier contraseña o código de seguridad para tener vía libre para operar abiertamente con los datos protegidos almacenados en el ordenador.

**Bombas lógicas:** son programas de destrucción o inhabilitación de datos creados para actuar en un momento específico, incluso mucho después de haber sido introducido en el sistema.

El avance de la tecnología ha acabado con muchos de los modos “clásicos” de terrorismo informático. Técnicas como el Piggybacking (colarse a un sistema con una cuenta de alguien autorizado), Scavenging (análisis de basura para obtener información desechada accidentalmente) y el “pinchado” de líneas telefónicas se han vuelto inútiles luego de que se adaptara la digitalización de documentos y las conexiones por marcado telefónico cayeran en obsolescencia.

#### **Prácticas que te permitirá mantener la seguridad de tu cuenta de email.<sup>12</sup>**

---

<sup>11</sup> ¿De qué nos tenemos que cuidar?. Delito de espionaje informático, cómo se comete este delito informático. Disponible en: <http://www.delitosinformaticos.com/10/2013/delitos/espionaje/delito-de-espionaje-informatico-como-se-comete-este-delito-informatico>

- Si te llegan mails de remitentes desconocidos con archivos adjuntos, no los abras.
- No hagas clic en los links que vienen en los correos de remitentes que no conoces
- No des información confidencial: Los bancos generalmente no piden a los clientes datos privados por email por lo que si recibes uno que te solicita información confidencial, duda.
- Habilita el filtro anti-spam
- Créate diferentes cuentas de correo electrónico: De esta forma, en una de ellas podrás recibir promociones y otras informaciones de baja importancia y reservar otra para los mails más relevantes.
- Usa contraseñas seguras: Para garantizar la seguridad de la misma debes incluir mayúsculas, minúsculas, números y ser mayor a los diez caracteres.
- No accedas a tu cuenta desde equipos públicos
- Ten cuidado a la hora de usar redes públicas de Wi-Fi: Puede haber alguien que esté queriendo descifrar tu contraseña.
- Utiliza la opción de copia oculta: Será bueno que la uses cuando debas enviar un mismo material a varios destinatarios y para que no queden visibles las direcciones.
- Infórmate sobre seguridad informática

---

<sup>12</sup> Eset. Decálogo de buenas prácticas que te permitirá mantener la seguridad de tu cuenta de email. Disponible en: <http://www.muyinteresante.es/>

### 3. CONCLUSIONES

La delincuencia informática es aquella que produce crimen electrónico que tiene como fin destruir los ordenadores, medios electrónicos y redes de internet, además incluye delitos tradicionales como falsificación, fraude, robo, extorsión, entre otros, que son delitos cometidos mediante computadoras y equipos tecnológicos.

La problemática jurídica de los sistemas informáticos debe considerar la tecnología de información que incluye en su conjunto de chips, redes, entre otros; por lo tanto, se debe establecer tratados de extradición o acuerdos de ayuda mutua entre los países. El estado debe aparecer como el principal regulador de esta actividad del control informativo a través del internet o redes sociales.

Es importante destacar que la delincuencia informática se apoya en el delito del uso de ordenadores a través de redes u otros, cada vez hay crecientes delitos que se puede llamar criminalidad informática que constituye un reto de todo país que deben de tener leyes apropiadas como ente regulador de la actividad informática.

### REFERENCIAS BIBLIOGRÁFICAS

Definición de delincuencia. Qué es, Significado y Concepto. Disponible en:  
<http://definicion.de/delincuencia/#ixzz3ab9uSmEk>

Delincuente. Definición ABC Disponible en: <http://www.definicionabc.com/general/delincuencia.php>

Criminal. Definición ABC. Disponible en: <http://www.definicionabc.com/social/criminal.php>

Diferencia entre delito y crimen. Tipos de delincuencia. Disponible en:  
<http://cristianaraos.com/2012/03/05/tipos-de-delincuencia-clasificacion-general-delito-y-delincuentes/>

Informática. Definición ABC. Disponible en: <http://www.definicionabc.com/tecnologia/informatica.php>

Concepto de Delincuencia. Qué es, Significado y Definición. Disponible en:  
<http://concepto.de/delincuencia/#ixzz3abAxxxBz>

Delitos informáticos. Myprofeciencias. Disponible en:  
<https://myprofetecnologia.wordpress.com/2011/01/30/delitos-informaticos/>

Tipos de delitos informáticos. Convenio sobre la Ciberdelincuencia. 1/11/2001. Disponible en:  
[http://www.delitosinformaticos.info/delitos\\_informaticos/tipos\\_delitos.html](http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html)

Tipos de delitos informáticos reconocidos por Naciones Unidas. Delitos Informáticos. Disponible en:  
<http://www.criminalistica.com.mx/areas-forenses/seguridad-publica/548-delitos-informcos>

¿De qué nos tenemos que cuidar? Delito de espionaje informático, cómo se comete este delito informático. Disponible en: <http://www.delitosinformaticos.com/10/2013/delitos/espionaje/delito-de-espionaje-informatico-como-se-comete-este-delito-informatico>

Eset. Decálogo de buenas prácticas que te permitirá mantener la seguridad de tu cuenta de email. Disponible en: <http://www.muyinteresante.es/>

NACIONES UNIDAS. Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990. (A/CONF. 144/28/Rev.1) Nueva York, Naciones Unidas. 1991.

Gordillo Hernández Rebeca Berenice. (2014, Agosto 8). *Delincuencia y su clasificación*. Disponible en: <http://www.gestiopolis.com/delincuencia-y-su-clasificacion/>