****

**UNIVERSIDAD NACIONAL AUTÓNOMA**

**DE HONDURAS**

**TECNOLÓGICA DANLÍ**



**Asignatura**:

Administración Pública y Políticas de Informática.

**Catedrático**:

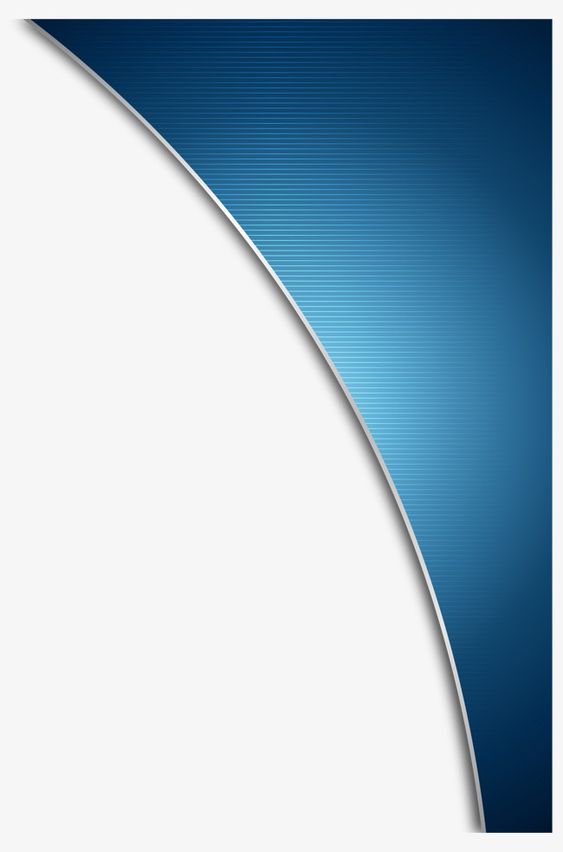
Lic. Wilson Aguilar

**Evaluación**:

Investigación y exposición sobre

Delitos Informáticos

Danlí, El Paraíso 2021

****

**Delitos Informáticos**

**INTEGRANTES:**

Bessy Karina Montiel 20162500075

Claudia Waleska Molina 20162530072

Daniela G. Murillo 20152500049

Gaby Marisol Díaz 20152502062

Luis Fernando Chacón 20152500060

Tania Melissa Sánchez 20142500167

**Índice**

[**Introducción** 4](#_Toc65336670)

[**1.** **MARCO TEÓRICO** 5](#_Toc65336671)

[**1.1** **Delito.** 5](#_Toc65336672)

[**2.** **Delito Informático.** 5](#_Toc65336673)

[**3.** **Delimitación del Fenómeno de la Delincuencia Informática.** 5](#_Toc65336674)

[**4.** **Sujetos del Delito Informático.** 6](#_Toc65336675)

[**4.1.** **Sujeto Activo:** 6](#_Toc65336676)

[**4.2.** **Sujeto Pasivo:** 12](#_Toc65336677)

[**5.** **Tipos de Delitos informáticos** 12](#_Toc65336678)

[**5.1.** **Los Fraudes:** 12](#_Toc65336679)

[**5.2.** **El sabotaje informático:** 13](#_Toc65336680)

[**5.3.** **El espionaje informático y el robo o hurto de software:** 14](#_Toc65336681)

[**5.4.** **El acceso no autorizado a servicios informáticos:** 15](#_Toc65336682)

[**6.** **Delitos Informáticos en Honduras** 16](#_Toc65336683)

[**7.** **Conclusiones** 19](#_Toc65336684)

# **Introducción**

En el presente informe se busca dar a conocer los principales delitos informáticos y los riesgos que estos generan para la sociedad, las empresas y los gobiernos. Asimismo, de las principales leyes que existen en Honduras para encauzar este tipo de delitos y de los acuerdos internacionales que los países han firmado y desarrollado con el fin de combatir este problema.

Investigar el delito desde cualquier perspectiva es una tarea compleja; de eso no hay duda. Ahora bien, el fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la manifestación de esta clase de delitos y tecnificando a otra clase de como son los llamados “Delitos Informáticos”.

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación. La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los procesos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

Por tanto, abordar el estudio de las implicaciones de la informática en el fenómeno delictivo resulta una cuestión apasionante para quien observa el impacto de las nuevas tecnologías en el ámbito social. Efectivamente, el desarrollo y masificación de las nuevas tecnologías de la información ha dado lugar a cuestiones tales como el análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones los nuevos escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo contemporáneo.

1. **MARCO TEÓRICO**
   1. **Delito.**

Un delito es un comportamiento que, ya sea por propia voluntad o por imprudencia, resulta contrario a lo establecido por la ley. El delito, por lo tanto, implica una violación de las normas vigentes, lo que hace que merezca un castigo o pena.

Más allá de las leyes, se conoce como delito a toda aquella acción que resulta condenable desde un punto de vista ético o moral.

1. **Delito Informático.**

Los delitos informáticos son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades.

Conocidos también con el nombre de delitos cibernéticos o electrónicos, abarcan un amplio espectro de acciones ilegales de diferente naturaleza. Todos tienen en común las tecnologías de la información, sea estas el medio o el objetivo en sí mismo.

Las personas que cometen delitos informáticos son expertas en el uso de las tecnologías, y sus conocimientos les permiten no sólo saber cómo utilizarlas, sino estar en posiciones laborales que les facilitan sus propósitos. De allí que gran parte de los delitos cibernéticos contra empresas sean cometidos por sus propios empleados.

Los delincuentes informáticos son llamados sujetos activos. En contrapartida, las personas o entidades que son víctimas de tales delitos se denominan sujetos pasivos.

Los delitos informáticos son muy difíciles de identificar. A esto se suma el hecho de que los sujetos pasivos muchas veces no los denuncian. En el caso de las empresas que son víctimas de estos delitos, el silencio se funda en el temor a perder su prestigio. Por lo tanto, poco llega a saberse sobre el alcance de estos delitos.

1. **Delimitación del Fenómeno de la Delincuencia Informática.**

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato.

En nuestro país, el fenómeno de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía una importancia mayor, esto por cuanto no se conoce en nuestro entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta, es porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual. (Problema que no solo es en el área Penal si no en todo el ordenamiento jurídico nacional).

1. **Sujetos del Delito Informático.**
   1. **Sujeto Activo:**

Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Las personas que cometen los “Delitos Informáticos” son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

A pesar de esto las incursiones de estos piratas y corsarios son diferentes y responden a distintas motivaciones y momentos en el desarrollo computacional.

A comienzos de los ’90, Internet era todavía un fenómeno lejano, al que pocos

tenían acceso, más la información restringida y confidencial atrajo a los primeros criminales informáticos.

En aquel tiempo eran catalogados como:

* **Sombrero Negro:** calificados como terroristas y mercenarios, usaban sus conocimientos para acceder a bases de datos que luego vendían.
* **Sombrero Gris:** este tipo de piratas se dedicaba a demostrar cuanto sabia y cuál era su capacidad para vulnerar sistemas. Su acción nunca fue con la intención de causar daño.
* **Sombrero Blanco:** detectaban errores y fallas en los sistemas de seguridad y advertían como remediar el problema.

Con Internet el pirateo se simplificó porque los programas fueron puestos a disposición del público en la misma red. Desde entonces, la distinción se hace por los grados de conocimiento y la esfera de su actuar. Así nos encontramos con los Hackers, los Crackers y losPhreaks, quienes son los tres grupos originarios de los que se subdividen otros tantos.

A continuación, distinguiremos cada uno de ellos:

* **HACKER**: Es una persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. La palabra es un término inglés que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear sus propios softwares para entrar a los sistemas.

Toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético:

* El acceso a los ordenadores y a cualquier cosa le pueda enseñar cómo funciona el mundo, debería ser limitado y total.
* Desconfía de la autoridad. Promueve la descentralización.
* Los Hackers deberán ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza, o posición social.
* **CRACKER**:

Personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

El Pirata informático. Tiene dos variantes:

* El que penetra en un sistema informático y roba información o se produce destrozos en el mismo.
* El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia.

Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

* **PHREAKER**:

Es el especialista en telefonía (Cracker de teléfono). Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles.

En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo, es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Estos buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades (en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación), pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de “Hacking” a sus servidores.

Dentro de las actuales manifestaciones de phreaking podríamos distinguir:

* **Shoulder-surfing:** esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.
* **Call-sell operations:** el accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas.
* **Diverting:** consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas, con el fin de hacer más difícil su detección.
* **Acceso no autorizado a sistemas de correos de voz:** el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio. A través de esta conducta el sujeto activo puede perseguir diversos objetivos:
* **Monitoreo pasivo:** por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.
* **LAMMERS**:

Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.

* **GURUS**:

Son los maestros y enseñan a los futuros Hackers. Normalmente se trata de personas adultas, me refiero a adultas, porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El gurú no está activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas.

* **BUCANEROS**:

En realidad, se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers, crean. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero sí de negocios. El bucanero compra al CopyHacker y revende el producto bajo un nombre comercial. En realidad, es un empresario con mucha afición a ganar dinero rápido y de forma sucia.

* **NEWBIE**:

Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicial-mente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la página WEB para seguir las instrucciones de nuevo. Es el típico tipo, simple y nada peligroso. Está apartado en un rincón y no es considerado.

* **TRASHING**:

Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas.

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

Entre los métodos preferidos por estos delincuentes para desarrollar su actuar son:

* **Puertas falsas:** puertas de entrada “que sirven para hacer la revisión o la recuperación de información en caso de errores en el sistema Consiste en aprovechar los accesos”.
* **Llave maestra(superzapping):** El uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora, aunque se halle protegido por medidas de seguridad.
* **Pinchado de líneas:** Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.
  1. **Sujeto Pasivo:**

Sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los “delitos informáticos” las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los “delitos informáticos”, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Este, la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

1. **Tipos de Delitos informáticos**
   1. **Los Fraudes:**

* LOS DATOS FALSOS O ENGAÑOSOS (Data diddling), conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, 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.
* MANIPULACIÓN DE PROGRAMAS O LOS “CABALLOS DE TROYA” (Troya Horses) 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 tienen 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.
* LA TÉCNICA DEL SALAMI (Salami Technique/Rounching Down), Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.
* 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.
* MANIPULACIÓN DE LOS DATOS DE SALIDA esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente 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.

* PISHING. - Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.
  1. **El 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:

* BOMBAS LÓGICAS (LOGIC BOMBS), es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un futuro.

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 en donde se halla la bomba.

* GUSANOS. Se fábrica de 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. 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.
* VIRUS INFORMÁTICOS Y MALWARE, son elementos informáticos, que, como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.
* CIBERTERRORISMO: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.
* ATAQUES DE DENEGACIÓN DE SERVICIO: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a muchos usuarios.
  1. **El espionaje informático y el robo o hurto de software:**
* FUGA DE DATOS (DATA LEAKAGE), también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. La forma más sencilla de proteger la información confidencial es la criptografía.
* REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL. Esta 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. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.
* HURTO DEL TIEMPO DEL COMPUTADOR. Consiste en el hurto del tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.
* APROPIACIÓN DE INFORMACIONES RESIDUALES (SCAVENGING), es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajopreviamente autorizado. To scavenge, se traduce en recoger basura.
* PARASITISMO INFORMÁTICO (PIGGYBACKING) Y SUPLANTACIÓN DE PERSONALIDAD (IMPERSONATION), figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático
  1. **El acceso no autorizado a servicios informáticos:**
* LAS PUERTAS FALSAS (TRAP DOORS), consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.
* LA LLAVE MAESTRA (SUPERZAPPING), es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.
* PINCHADO DE LÍNEAS (WIRETAPPING), consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.
* 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.

1. **Delitos Informáticos en Honduras**

En Honduras lo que respecta a daños a sistemas informáticos y datos se sanciona con 3 a 5 años de cárcel y multas que van desde los cincuenta mil lempiras.

Se lee en la normativa penal vigente: “Se impondrá reclusión de tres (3) a cinco (5) años a quien destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos”.

Sin embargo, pese a que en el Nuevo Código Penal los delitos informáticos son clasificados en cuatro: Acceso no autorizado a sistemas informáticos, Daños a datos y sistemas informáticos**,** Abuso de dispositivos y Suplantación de identidad**,** con “el detalle” que las sanciones no concuerdan con los daños ocasionados por los ciberdelincuentes o quienes utilizan el internet para provocar destrucción de información, daños a páginas web y sustracción y daños a la propia data del Estado.

En el Título XXII Seguridad de las Redes y Sistemas Informáticos establece en el Artículo 398.- Acceso No Autorizado a Sistemas Informáticos, “debe ser castigado con pena de prisión de seis a dieciocho meses o multa de cien a doscientos días quien, vulnerando las medidas de seguridad establecidas para impedirlo, accede sin autorización a todo o en parte de un sistema informático.

Artículo 399.- Daños a Datos y Sistemas Informáticos. Quien por cualquier medio y sin autorización introduce, borra, deteriora, altera, suprime o hace inaccesible de forma grave datos informáticos, debe ser castigado con la pena de prisión de uno a dos años o multa de cien a trescientos días.

En lo que respecta a Abusos de Dispositivos, “la fabricación, importación, venta, facilitación o la obtención para su utilización de dispositivos, programas informáticos, contraseñas o códigos de acceso, destinados o adaptados para la comisión de los delitos de daños informáticos o de acceso ilícito a sistemas informáticos, debe ser castigada con la pena de prisión de seis meses a un año o multa de cien (100) a doscientos (200) días. Artículo 400.

Asimismo, en referencia a Suplantación de Identidad, en el artículo 401: “debe ser castigado con la pena de prisión de seis meses a un año o multa de cien a trescientos días, quien con ánimo defraudatorio y a través de las tecnologías de la información y la comunicación, suplanta la identidad de una persona natural o jurídica.

El nuevo Código Penal hace varias clasificaciones del ciberdelito, las cuales se detallan a continuación:

* Espionaje Informático: Consiste en entrar en un sistema informático ajeno con la intención de acceder a su información sensible para utilizarla posteriormente en perjuicio de la víctima y en beneficio de los autores.
* Sabotaje Informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.
* Abuso de dispositivos: La fabricación, importación, venta, facilitación o la obtención para su utilización de dispositivos, programas informáticos, contraseñas o códigos de acceso, destinados o adaptados para la comisión de los delitos de daños informáticos o de acceso ilícito a sistemas informáticos
* Suplantación de identidad: Es una expresión informática que se emplea para referirnos a los abusos informáticos cometidos por delincuentes para estafar, obtener información personal, contraseñas, clonación de tarjetas de crédito, etc. de forma ilegal.
* Ciberterrorismo: Acceso no autorizado a un sistema informático de la administración pública del Estado.
* Piratería Informática: Es quien adopta por negocio la reproducción, apropiación y distribución con fines lucrativos y a gran escala de software, videos, música de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador.

1. **Conclusiones**

* Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que, a nivel general, se poseen pocos conocimientos y experiencias en el manejo de esta área. Desde el punto de vista de la Legislatura es difícil la clasificación de éstos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante [innovación tecnológica](https://www.monografias.com/trabajos37/innovacion-tecnologica-empresarial/innovacion-tecnologica-empresarial.shtml) obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.
* La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.