DERECHO INFORMÁTICO

**Los delitos informáticos que   
prevalecen y crecen en todo el mundo, y en Argentina**

*En Argentina, los ciberdelitos se clasifican en cinco tipos o grupos que forman parte del Código Penal argentino. A pesar de su inclusión en el nuevo Código Penal, los delitos informáticos tienen una continuidad creciente en nuestro País, lo cual significaría una necesidad de mejora de acciones.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Los delitos informáticos son actos, conductas o acciones realizadas por personas físicas mediante medios informáticos o electrónicos, en internet o en el ciberespacio, contra la confidencialidad, integridad y disponibilidad de sistemas informáticos, redes y datos digitales.

También, el mal uso de dichos sistemas, redes y datos.

En definitiva, son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets.

**Una breve introducción.**

La importancia de determinar los diferentes tipos de delitos informáticos existentes, permite tener una herramienta de vanguardia en el ámbito de la seguridad informática, para enfrentar de manera efectiva, las consecuencias personales, económicas y sociales, al momento de ser víctimas de este acto delictivo (Escobar, 2017).

Con referencia a lo anterior y, como usuarios diarios de este tipo de tecnología, es necesario conocer los riesgos que significa, el confiar información de primer nivel (personal, financiera, empresarial), a sitios o aplicaciones que pueden ser vulnerados, por profesionales de oficios (hacker, cracker, phracker y piratas informáticos), para convertir, a estos usuarios, en víctimas de fraude, extorción y chantaje.

El crimen informático, ha llegado a niveles organizacionales, de hecho Fernández (2013) destaca la importancia que reviste la complicidad interna, por intermedio del personal que labora en la misma, quienes sin importar los valores de respeto y lealtad, perjudican la vulnerabilidad de la información de la organización, volviéndose inclusive en algunos casos, en algo codiciado que, además, es muy bien remunerada por los delincuentes cibernéticos, que buscan el desprestigio o robo de información confidencial, con la intención de chantajear o liquidar las empresas.

**Conceptos, prevención y riesgos.**

El uso de la informática a nivel mundial, ha tenido un repunte y una importancia relevante frente a la sociedad. El solo hecho de ofrecer servicios que permitan que los usuarios se les simplifiquen las cosas en un momento determinado, sobre todo para comunicarse e informarse, lo hace una herramienta útil y en muchos casos, necesaria (Márquez y Mousalli, 2016).

En efecto, expresa Trejo (2006) que resulta increíble la posibilidad de acceder a tanta información, tan diversa y tan pública, a la mano de cualquier usuario, en la historia de la humanidad. Hoy en día, existe una gran variedad de contenidos al respecto, tales como wikis, bibliotecas virtuales, chat, correo electrónico, videoconferencias, firmas electrónicas, foros, blogs, robótica, entre otros, que facilitan cualquier tipo de interacción masiva, sin tomar en consideración edad, género o nivel económico, que se apoyan en estos contenidos para entretenerse, socializar, buscar información desde la comodidad de la casa, oficina o cualquier ambiente donde exista la conexión (Márquez et al, 2016).

Ahora bien, hablar de delito es hablar de un estado criminal o ilegalidad de una acción, que compromete la integridad del otro (Tundidor, Nogueira y Medina, 2018). Bajo este contexto, el delito organizado se ha fortalecido a través de los años, debido a la misma evolución del sistema en general y, a la transnacionalización de sus redes delictivas. Son innumerables las actividades delictivas existentes, variando solamente según los entornos, localidades, oportunidades, entre otros, logrando expandirse a numerosos países. Según Torres, (2015) existe una fuerte tendencia a que los hechos delictivos se concentren hacia la parte empresarial, siendo este un blanco elegido por los antisociales, en muchos casos, por descuidos en cuanto al sistema de seguridad de las mismas organizaciones.

La modernización ha traído que el manejo de la información, se realice mediante procesadores informáticos, que permiten almacenar una cantidad considerable de información y, que, al mismo tiempo, se pueda acceder de manera rápida y efectiva a esos datos. La información puede ser de cualquier tipo (personal, empresarial, financiera-bancaria, societaria), siendo esta apetecida por los llamados delincuentes informáticos con la intención de sacar provechos de tipo oneroso, por intermedios del chantaje, desprestigio y hasta secuestro de la información sustraída.

Se vive una época, donde los cambios se presentan de manera vertiginosa. Al respecto explica España (2010), que en tiempos pasados se podía tener la seguridad que muy pocas personas o, casi nadie, podía acceder a información sobre nuestras vidas privadas por intermedio del Internet. Respecto a esto, destaca Riestra (2016), que la información de la informática se convirtió en la cotidianidad en la vida personal de algunos seres humanos. Esto ha producido que se convierta en una información muy bien cotizada. Esto sin duda alguna, hace crecer la amenaza de los mismos. Existen personas que se dedican exclusivamente a este tipo de delitos, con la intención de enriquecerse o, de generar cualquier revuele noticiosos de un caso específico.

Cuando se habla de delito informático, Fuentes, Mazún y Cancino (2018) la definen como el conjunto de comportamientos que genera delito penal y, que debe ser tratado legalmente ya que el mismo tiene por objeto daños a terceras personas, ocasionando diferentes lesiones y, en algunos casos pérdidas de bienes jurídicos. Es necesario aclarar, que este tipo de delitos suceden en el ciberespacio. En este mismo orden y dirección, Ruiz (1996), expresa una definición apegada a la Organización para la Cooperación y el Desarrollo Económico [OCDE] (2014) donde expresa que el delito informático viene dado al comportamiento de manera ilegal que es contraria a la ética y, no es autorizada si divulgación y transmisión de datos de la red.

Es importante conocer que no existe un consenso en cuanto al término como tal, ya que también el delito informático puede ser conocido como delitos telemáticos, crímenes virtuales, cibercrímenes, ciberterrorismo, entre otros. Lo importante en todo esto, es conocer la manera de proteger y resguardarse de manera efectiva, sea de forma Legal o por intermedio de programas de seguridad interna, la información que se tiene en los servidores y en la red. El simple hecho de perder la privacidad en este sentido, aumenta notablemente el riesgo de un ataque cibernético, por intermedio de técnicas que permiten el acceso a la información.

Con relación a los riesgos que condiciona a los delitos informáticos, los mismos provienen de combinaciones de situaciones y generalmente se conocen como atentados y amenazas a los sistemas de información. Entre los tipos de riesgos más conocidos se nombran: riesgos de integridad, riesgos de relación, riesgos de acceso, riesgos de utilidad, riesgos en la infraestructura, riesgos de seguridad general, concentración de procesamiento de aplicaciones más grandes y de mayor complejidad, dependencia en el personal clave y desaparición de los controles tradicionales. Todos cumplen roles según el tipo de delito que se cometa.

En definitiva, el delito informático es una forma de delinquir extrayendo información personal directamente del ciberespacio, el cual abarca el problema amenazando los entornos privados de la sociedad en general, además de adicionar posibles daños patrimoniales tanto personales como empresariales, producidos por el abuso de datos extraídos. Generalmente tiene carácter transfronterizo, que exige una respuesta adecuada y rápida y, por lo tanto, se necesita actualizar una debida adaptación de las Leyes según la naturaleza del delito y la seguridad adecuada para el resguardo de la información y la defensa del territorio cibernético.

**Tipos de delitos informáticos.**

El acceso no autorizado: no se tiene acceso sin derecho a un sistema o a una red cualquiera, violándose todas las medidas de seguridad existentes. Generalmente son operadas por genios de la informática conocidos como Hackers.

El daño a los datos o programas informáticos: es la eliminación o barrado total, descomposición, deterioro o erradicación de los datos o de los programas informáticos, sin que la persona ejecutante tenga derecho o acceso a realizar esa acción.

El sabotaje informático: va direccionado a la alteración y eliminación total de datos o programas. Producen una interferencia, para bloquear los sistemas informáticos con la finalidad de obstruir el funcionamiento de las redes en su totalidad.

La interceptación no autorizada: se refiere a la captación que se realiza sin autorización previa, tomando en consideración mecanismos tecnológicos tradicionales.

El espionaje informático: es la adquisición, revelación y transferencia de información cibernética, de tipo confidencial, comercial; sin permiso o autorización del propietario de la información, con el propósito de causar pérdidas económicas o de obtener algún beneficio oneroso.

En una investigación realizada por Luna (2018), uno de los delitos de informática más utilizados por los ciberdelincuentes, es el espionaje informático. Explica el autor, que el mismo actúa como acechador, instigador y vigila de manera disimulada, a una persona clave para luego abordarla y obtener información sobre alguien o de una empresa o del gobierno. El espionaje industrial, ha cobrado mucho auge mediante la tecnología y, representa una buena plaza donde los cibercriminales pueden obtener mejores ganancias metálicas.

A pesar de la existen todavía de herramientas que se utilizan para aplicar el espionaje, tales como: tintas invisibles, micrófonos, grabadoras y microcámaras, son las computadoras y sus aplicaciones, entre ellos los móviles, las herramientas más utilizadas actualmente para llevar a cabo este delito. Hay dos tipos de espionaje que sobresalen de los demás. Uno es el industrial y otro el informático.

De no tomar con seriedad el tema de la seguridad para proteger las informaciones, el espionaje informático ganará más terreno, aumento el riesgo de que las informaciones confidenciales se filtren. Una vez que una persona, o una empresa en general entran al mundo de las redes sociales, o por lo menos navegue en el Internet, da la posibilidad de ser identificado y plagiado mediante este procedimiento. Se observa como a nivel organizacional, el tráfico de información se vuelve un problema axiológico, al momento de vender los datos a otros competidores o al gobierno. Nos encontramos a un clic, de perder nuestra identidad y nuestra visión de negocios, por culpa de la codicia, la deslealtad y la falta de valores éticos y morales.

El delito informático, como se ha indicado en otros puntos anteriores, es un tipo de delincuencia producto de las nuevas tecnologías, el cual se da en diferentes campos de la vida diaria y muy especial en las organizaciones y corporaciones, el cual deben pagar cuantiosas cantidades de dinero para resguardar la información. Sin embargo, no se puede descuidar todos los vacíos jurídicos que surgen a través de estos temas, donde la integridad, ética e intelecto de una persona u organización empresarial se pueden ver afectados. Para Le Clerq (2015), dichos vacíos legales solo logran crear los conocidos y mal llamados «paraísos informáticos» o «cibernéticos», los cuales nacen cuando un ente específico aprovecha la deficiencia de una Normativa o Ley que sea relativa, en este caso, al delito de informática.

Una vez más queda en evidencia que uno de los factores comunes encontrados en las investigaciones, los cuales permiten que sucedan este tipo de delitos, es la falta de seguridad en los datos cibernéticos, poniendo en riesgo de que ocurra el hecho.

Esto ha traído la atención a nivel mundial, a tal punto que estas actividades cibercriminales han causado alarma en todos los Gobiernos y mercados del mundo, el cual han tomado en serio la importancia que reviste la data informática y sobre todo medidas de seguridad que permita contrarrestar el problema.

El esfuerzo mundial para prevenir y castigar este tipo de criminalidad, ha llevado a elaborar un convenio de cibercriminalidad, el cual fue suscrito en Budapest (Hungría) en 2001

Dicho convenio destaca la necesidad de descubrir delitos tales como: el acceso ilícito a los sistemas informáticos, la interceptación de las redes comunicacionales, la producción y venta de dispositivos y programas que permitan la intrusión en un sistema, la alteración o borrado de datos, los fraudes por internet, el espionaje cibernético, y los ataques a la propiedad intelectual y a los derechos afines.

En definitiva, la impunidad de los delitos informáticos es una situación que se debe abordar desde los puntos de vistas legales, axiológicas y de seguridad. Las organizaciones, han tenido ciertos problemas acerca de la seguridad de su base de datos, el cual los coloca en una situación no privilegiada para salvaguardar su data. Por supuesto como se ha indicado, esto favorece en cierta forma, el aumento de la cibercriminalidad, pues el delincuente se apoya en esa falencia, para cometer el delito. Darle relevancia a cumplir con las normas y parámetros legales, permitirá en cierta forma, respaldar a todos aquellos que se encuentran desprotegidos de esta situación.

Los delitos informáticos representan un acto ilícito existente en las redes de información (web), que atenta contra la propiedad privada intelectual de la sociedad, las organizaciones y el Estado en general. Cada día se observa, como los delitos informáticos van en ascenso, y parte del mismo, se debe en muchos casos, al descuido en cuanto a la protección de la data por parte de los usuarios. De esta forma, los delincuentes cibernéticos encuentran oportunidades para extraer información que atenta con la integridad y con la estabilidad organizacional de los dueños de la información.

La cautela, el escepticismo y la prevención, deben ser los elementos que permitan a los propietarios de la información, a resguardar la misma. Más aún cuando se trata de data que pueda dañar de manera directa, una identidad o una organización. La contratación de expertos en seguridad cibernética, no debe ser vista como un gasto agregado, más bien, es un valor intangible que necesaria para salvaguardar la información, ante la cantidad de ciberdelincuentes que bordean la web, donde su única intención es perjudicar a terceros y enriquecerse de manera ilícita, apoyados en muchos casos por el descuida, la confianza en cuanto al manejo de la data.

Cada día los delitos informáticos van tomando auge en todos los niveles cibernéticos. Los infractores crean y activan diferentes modalidades que les permitan delinquir tales como, el hurto, estafas, chantajes, entre otros, perjudicando de manera fehaciente la privacidad e identidad de cualquier persona o entidad. La necesidad de instaurar sistema de seguridad, que permita el resguardo de la información, cada día toma más relevancia, sobre toda cuando la información que se maneja es de primera línea.

**Tipos de delitos informáticos en Argentina.**

En Argentina, los ciberdelitos se clasifican en 5 tipos o grupos que forman parte del Código Penal argentino:

* Delitos informáticos contra la integridad sexual.
* Delitos informáticos contra la libertad.
* Delitos informáticos contra la propiedad.
* Delitos informáticos contra la seguridad pública que atentan contra los medios de comunicación.
* Delitos informáticos contra la Administración pública.
* Delitos informáticos contra la integridad sexual.

**Ciberdelitos contra la integridad sexual.**

* Producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir cualquier representación de una persona menor de 18 años dedicada a actividades sexuales explícitas o de sus partes genitales.
* Tener representaciones de personas menores de edad de actividades sexuales explícitas o de sus partes genitales para distribuirlas o comercializarlas.
* También sanciona el ciberacoso a personas menores de edad (grooming).
* Delitos informáticos contra la libertad.

**Contra la libertad.**

* Acceder, apoderarse, suprimir o desviar una comunicación electrónica que no le esté dirigida; la pena es mayor si el contenido de la comunicación electrónica se publica.
* Acceder ilegítimamente a un sistema o dato informático de acceso restringido. La pena se agrava cuando el acceso es en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
* Publicar indebidamente una comunicación electrónica no destinada a la publicidad cuando esto cause perjuicio a otros. No tiene responsabilidad penal el que actúa para proteger un interés público.
* Revelar documentos informáticos oficiales que por ley deben ser secretos.
* Acceder de manera ilegítima a bancos de datos personales, revelando información o insertando datos en un archivo de datos personales. Si el autor es funcionario público, sufre además pena de inhabilitación.

**Delitos informáticos contra la propiedad.**

* La estafa mediante el uso de tarjeta magnética o de los datos de la tarjeta.
* La defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
* El daño informático, que consiste en alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; vender distribuir, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños.
* La pena es mayor en caso de dañar datos, documentos, programas o sistemas informáticos públicos; causar daño en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

**Contra la seguridad pública que atentan contra los medios de comunicación.**

* Sustraer, alterar, ocultar, destruir o inutilizar registros o documentos electrónicos confiados a la custodia de un funcionario público o de otra persona en interés del servicio público.
* Delitos informáticos contra la Administración Pública
* Sustraer, alterar, ocultar, destruir o inutilizar registros o documentos electrónicos confiados a la custodia de un funcionario público o de otra persona en interés del servicio público.

**Leyes de Argentina contra los ciberdelitos.**

* Código Penal de la Nación Argentina.
* Ley 26.388, Ley de Delitos Informáticos.
* Ley 27.411, Convenio de Budapest.

**Delitos informáticos más comunes o frecuentes (Argentina).**

* Calumnias, calumnias y difamaciones, artículos 109 a 117 bis Código Penal Argentino, ley 26.551.
* Amenazas, artículos 149 bis y 149.
* Delitos contra la propiedad intelectual, ley 11723 artículos 71 y 72, y ley 25036.
* Pornografía infantil, artículo 128 Código Penal Argentino.
* Acceso indebido a sistemas informáticos, artículos 153 y 153 bis Código Penal Argentino.
* Fraude informático (phishing), artículos 172 y 173 Código Penal Argentino.
* Instigación a cometer delitos, artículo 209 y 209 bis Código Penal Argentino. Apología del delito, artículo 213 Código Penal Argentino.
* Grooming, artículo 131 Coding Penal Argentino.
* Extorsión, artículo del Código Penal Argentino.
* Daño informático: destrucción de sistemas informáticos y/o su contenido, artículo 183 Código Penal Argentino.

**Denunciar un delito informático en Argentina.**

Lo primero que se debe hacer es la denuncia en la comisaría o en la oficina receptora de denuncias que corresponda a tu domicilio. Además, se puede reportar el caso a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) enviando un correo a denunciasufeci@mpf.gov.ar.

También, se puede recurrir a la División Delitos Tecnológicos de la Policía Federal Argentina al correo electrónico: judiciales-delitostecnologicos@policiafederal.gov.ar. Tienen obligación de tomar tu denuncia.

A los fines de resguardar correctamente la prueba, una vez realizada la denuncia, se debe proceder de la forma en que el investigador lo indique.

Hay que tener en cuenta que ante contenidos de carácter discriminatorio en Internet también es posible recurrir al Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI), dependiente del Ministerio de Justicia y Derechos Humanos, correo electrónico, 0800@inadi.gob.ar.