CAMPAÑA: LOS DESCARADOS
"Protégete contra los Delitos Digitales"

DELITOS INFORMÁTICOS

En la actualidad la informatización y su desarrollo acelerado en medios digitales, permean las actividades diarias realizadas por las organizaciones del sector público y privado, así como también se encuentra presente en la investigación científica, en la producción industrial, en el sistema educativo, y en el ocio; es por ello que el uso de la informática se ha vuelto absolutamente necesario y muy conveniente desde el punto de vista económico. No obstante junto a sus grandes ventajas, comienzan a surgir aspectos negativos como los delitos informáticos y la transgresión de la norma jurídica, como consecuencia de interpretaciones inadecuadas o por la presencia acelerada de delincuentes informáticos que aplican estrategias novedosas para violar la seguridad digital de los ciudadanos.

Las TIC han creado nuevas posibilidades de delincuencia impensables, con consecuencias graves para el patrimonio de los ciudadanos. El fraude desde los computadores y redes sociales con ánimo de lucro, la violación de la privacidad, las ofertas engañosas, entre otros, son algunos de los procedimientos mediante los cuales es posible obtener grandes beneficios o causar importantes daños materiales a los ciudadanos.

Es por ello que abordar el delito informático requiere enfrentarlo con una visión más amplia, ya que el mismo transciende ámbitos locales y las transgresiones pueden ser gestionadas desde cualquier parte del mundo. Es tal sentido es necesario visualizar el delito informático bajo distintos enfoques y entender las visiones de organismos como la Organización de Naciones Unidas e instancias nacionales como la Asamblea Nacional de Venezuela.

El delito informático en el ámbito internacional

La globalización y el uso de internet han marcado la evolución de los delitos tradicionales en el mundo, otorgándole características particulares, provenientes del uso de nuevas tecnologías, configurando nuevas tipologías delitos como la ciberdelincuencia, considerada hoy en día un problema universal. Desde la década de 1960 muchos países han reconocido como delitos ciertos actos relacionados con la informática, como el uso no autorizado de sistemas informáticos y la manipulación de datos electrónicos. Pero ha sido con la llegada de internet que las tecnologías globalizadas de la información y las comunicaciones han empezado a usarse para cometer delitos a escala internacional, en la forma de

ciberdelincuencia que conocemos actualmente.[1]

La Organización para la Cooperación Económica (OCDE) en París en 1983, definió al delito informático como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la trasmisión de datos[2] .

Las Naciones Unidas convienen en denominar este tipo de delito como ***Ciberdelincuencia,*** y reconoce que la ciberdelincuencia no es necesariamente un término jurídico técnico, sino más bien un término genérico para referirse a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos. Otros enfoques se centran en los delitos contra la información computadorizada o el uso de recursos de información con fines ilícitos.

Las Naciones Unidas, consideran como supuestos de hecho para materializar delitos informáticos, "ciberdelincuencia" aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del modus operandi del delito. Algunos ejemplos de los primeros son los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos, como el acceso ilegal a datos o sistemas informáticos. Algunos ejemplos de los segundos son el uso de datos o sistemas informáticos para estafar, robar o causar daño a otras personas, así como los delitos relacionados con contenidos informáticos o de Internet, como los discursos de incitación al odio, la pornografía infantil, los delitos relacionados con la identidad y la venta por internet de mercancías ilícitas[3].

En abril del año 2017, se reunieron en Viena, un grupo de expertos de las Naciones Unidas, encargado de realizar un estudio exhaustivo sobre el Delito Cibernético, se discutió ampliamente sobre la necesidad de establecer normativa jurídica de carácter internacional, a continuación, se presenta el resumen de las deliberaciones del grupo de expertos[4]:

- La prevalencia y el papel que desempeñaban las tecnologías de la información y las comunicaciones en sus países y cómo esos factores están vinculados con la ciberdelincuencia. La mayoría de los expertos señalaron que el delito cibernético iba en aumento. También señalaron que existían vínculos concretos y complejos entre a) la prevalencia y el uso de las tecnologías, tanto en los Estados Miembros como a nivel regional y b) la evolución de la ciberdelincuencia. Se señaló que la difusión de las tecnologías y el problema conexo de la ciberdelincuencia también planteaban cuestiones relacionadas con la soberanía nacional, la independencia, la gobernanza, los derechos humanos y la cultura. Varios expertos mencionaron la necesidad de respetar la independencia soberana y la diversidad cultural, tanto al elaborar las definiciones de ciberdelincuencia como al estudiar las respuestas nacionales, transnacionales y mundiales ante ella.
- La necesidad de disponer de datos mundiales fiables y exhaustivos sobre la naturaleza y la extensión del problema. Entre las dificultades más importantes a ese respecto figuraban el muy amplio alcance del problema, la gama de fuentes de información que debían tenerse en cuenta y la necesidad de actualizar constantemente los datos y los

[1] 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal
[2] https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf
[3] 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Doha, 12 a 19 de abril de 2015
[4] rg/documents/organized-crime/cybercrime/Cybercrime-April-2017/UNODC-CCPCJ-EG-4-2017-2/V17 01129_S.pdf

análisis para reflejar su evolución dinámica.

- La cuestión de los marcos jurídicos o de otro tipo para reglamentar y coordinar las respuestas internacionales al delito cibernético. Se expresaron opiniones divergentes. Algunos expertos sostuvieron que se necesitaba un nuevo instrumento jurídico internacional amplio y universal sobre el delito cibernético para establecer un consenso mundial sobre respuestas eficaces y proporcionar una base jurídica internacional clara para esas respuestas. Otros opinaron que sería más eficaz el uso de los regímenes jurídicos nacionales e internacionales existentes y enfoques más a medida para la cooperación caso por caso y la prestación de asistencia técnica.
- Varios expertos y representantes del sector privado destacaron la importancia de la prevención. Se mencionaron los medios técnicos, como el uso de aplicaciones de seguridad para proteger la integridad de los sistemas y los datos, y los medios sociales, como la educación de los usuarios de los sistemas y la inclusión de elementos relativos a la ciberdelincuencia en los programas escolares y universitarios pertinentes.
- Los expertos dijeron que era posible y deseable cooperar en un amplio conjunto de ámbitos específicos, como la prevención, la cooperación en las investigaciones, la reunión de información de carácter más general sobre la evolución de la delincuencia y sus tendencias y la formación de investigadores y expertos forenses en las nuevas tecnologías a medida que se creaban y comercializaban.

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos[5]:

1. 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 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.
- 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 equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. 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

[5] https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

transfieren a otra.

2. 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. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras 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.

3. 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.
    - Gusanos: se fabrica 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. 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 eventualmente 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 en donde se halla la bomba.

- **Acceso no autorizado a servicios y sistemas informáticos**: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. Piratas informáticos o hackers: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. 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**: ésta 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. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Con lo anterior se observa que en el ámbito internacional existe un movimiento importante que busca identificar los riesgos de los delitos informáticos y diferenciar los distintos tipos de delitos, así como también crear conciencia sobre la necesidad de la prevención y educación de los ciudadanos como de los gobiernos.

EL DELITO INFORMÁTICO EN VENEZUELA

En Venezuela la legislación que regula los delitos informáticos es de reciente data, fue publicada por la Asamblea Nacional el 30 de octubre de 2001, en Gaceta Oficial número 37.313, y denominada Ley Especial contra Delitos Informáticos[6] (LEDI). El Objeto de la Ley lo encontramos en su artículo 1:

"La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley".

La legislación especial relacionada con delitos informáticos surge, como consecuencia de regular conductas ilícitas nuevas, en la comisión de delitos ya previstos en el Código Penal, pero con la característica de un nuevo modus operandi, apoyado en el uso de tecnologías, convirtiéndolo en delitos emergentes, y dejando sin posibilidad de aplicación la regulación existente.

La LEDI, contempla en su articulado el principio de extraterritorialidad, relacionado a la sujeción de la jurisdicción nacional para quienes cometan los delitos tipificados en la norma, señala la LEDI, que cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros[7].

[6] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf
[7] Artículo 3 de la Ley Especial de Delitos Informáticos

Tipos de delitos informáticos

La LEDI, agrupa en cinco categorías los distintos tipos de delitos que en el área informática se pueden cometer:

1. Delitos Contra los Sistemas que Utilizan Tecnologías de Información.
2. Delitos Contra la Propiedad
3. Delitos Contra la Privacidad de las Personas y de las Comunicaciones
4. Delitos Contra Niños, Niñas o Adolescentes
5. Delitos Contra el Orden Económico

A continuación, se describen los distintos tipos de delitos informáticos previstos en la norma jurídica especial creada al efecto por la Asamblea Nacional de la República Bolivariana de Venezuela[8]:

TIPOS	CONCEPTUALIZACIÓN DEL DELITO	SANCIÓN
Delitos Contra los Sistemas que Utilizan Tecnologías de Información	**Acceso indebido**. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información.	Prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
	Sabotaje o daño a sistemas. Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman.	Prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias
	Favorecimiento culposo del sabotaje o daño. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.	
	Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.	
	Posesión de equipos o prestación de servicios de sabotaje. Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.
	Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de

[8] http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf

		un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.
	Falsificación de documentos. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.
Delitos Contra la Propiedad	**Hurto.** Quien, a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias
	Fraude. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno.	Prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.
	Obtención indebida de bienes o servicios. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
	Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos,	Prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.
	Apropiación de tarjetas inteligentes o instrumentos análogos. Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora,.	Prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias
	Posesión de equipo para falsificaciones. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos.	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias
Delitos Contra la Privacidad de las Personas y de las Comunicaciones	**Violación de la privacidad de la data o información de carácter personal**. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

	sistema que utilice tecnologías de información.	
	Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias
	Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
Delitos Contra Niños, Niñas o Adolescentes	**Difusión o exhibición de material pornográfico**. Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes.	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
	Exhibición pornográfica de niños o adolescentes. Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos.	Prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias
Delitos Contra el Orden Económico	**Apropiación de propiedad intelectual.** Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.	Prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.
	Oferta engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores.	Prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Sanciones aplicables

Las sanciones por los delitos previstos en la LEDI, pueden ser principales y accesorias, y consisten en multas establecidas en unidades tributarias y/o penas privativas de libertad (prisión), las cuales oscilan desde 100 a 1000 unidades tributarias y prisión que va desde un (01) año a ocho (08) años de prisión, dicha sanción se encuentra prevista en la LEDI, en los artículos donde se tipifican los delitos.

Tendencias de los delitos informáticos en Venezuela

El presente apartado tiene como finalidad indagar sobre las tendencias y evolución de los delitos informáticos cometidos en Venezuela en el periodo 2002 al 2019, tomado como referencia lo establecido en La LEDI.

Año	Reporte de Caso	Fuente	Tipificación del Delito Informático
2002	El Paro Petrolero de 2002: Durante esa época, la situación política dio lugar a numerosas denuncias sobre ataques	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude electrónico (bancario)

	informáticos a PDVSA en donde se hablaba de robo de archivos electrónicos, información de cuentas en el exterior, entre otros. Fueron abiertos varios expedientes que muchos de ellos aún, siguen pendientes.		
2005	En el año 2005 un SpyBanker capturo información de toda la banca venezolana, tomando fotografías de las pantallas de los empleados a medida que avanzaban en las acciones de tecleo, enviando los datos a destinos remotos. Las autoridades lograron detectar la computadora con la cual se cometió el delito, pero aún no hay capturas por este hecho.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude electrónico (bancario)
2007	La División Contra Delitos Informáticos del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) develó que entre los primero seis delitos cometidos por medio de la tecnología se encontraba el "fraude electrónico" señalando un aumento considerable en el perfeccionamiento de los métodos y en el número de irregularidades cometidas. Esta instancia registró 170 denuncias de delitos informáticos durante el año.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude electrónico (clonación de tarjetas de crédito y débito, obtención de información de cuentas bancarias)
	Delito de pornografía infantil en medios digitales.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Pornografía infantil
	Caso de un niño de tan solo 11 años de edad, residenciado en Barquisimeto, el cual logró estafar electrónicamente a un número no menor de 25 personas. Este pequeño trabajaba con la cuenta de su padre y cuando fue detenido señaló que hacía esto por simple diversión, dicha versión, aparentemente, fue creída por los cuerpos policiales ya que, al verificar la cuenta donde se depositaban los fondos se percataron de que el dinero estafado no había sido utilizado.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/ Nota: Según la División de Delitos informáticos para marzo del año 2007, se habían recibido 170 denuncias de delitos informáticos y el número actualizado no fue dado a conocer por falta de autorización del Ministerio del Interior y Justicia.	Fraude electrónico (este caso denota la vulnerabilidad de los sistemas de seguridad de las empresas financieras o bancos que operan en nuestro país)
2012	El CICPC capturó a varios empleados del Banco Bicentenario los cuales utilizaron información suministrada por clientes del banco para ingresar en sus cuentas de usuarios de CADIVI y apoderarse de un monto de 42 mil dólares.	http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/	Fraude bancario
2017	La CICPC recibe a través de la división de delitos informáticos de 15 a 20 denuncias diarias relacionadas con estafas mediante ofertas engañosas publicadas en las redes sociales, en la mayoría de estos casos los compradores llegan a un acuerdo con el supuesto vendedor acordando fecha, hora y lugar para realizar la entrega, sin embargo este proceso no se	http://www.correodelorinoco.gob.ve/cicpc-combate-proliferacion-delitos-redes-sociales/	Ofertas engañosas

	concreta porque tan pronto, el estafador se percata que tiene el dinero, vía transferencia electrónica desparece o no contesta el teléfono.		
	La segunda denuncia más frecuentes que recibe la CICPC es la modalidad de fraude mediante el cambio o reemplazo de la tarjeta de débito o tarjeta de crédito por una falsa que no le pertenece a la víctima y que la realizan en cajeros automáticos o en los puntos de venta", informó la funcionaria del CICPC.		Fraude
2019	El inspector agregado del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), Alberto José Dugarte, reveló un incremento en los delitos informáticos en Venezuela, y resaltó que uno de los más frecuentes es el que se registra ante el acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos.	https://www.vtv.gob.ve/inspector-cicpc-acceso-indebido/	Ofertas engañosas
Septiembre 2019	Cicpc desmanteló dos laboratorios de pornografía en Caracas el director de la policía científica, C/G Douglas Rico, en compañía de funcionarios de la División Contra los Delitos Informáticos y División de Experticias Informáticas efectuaron un allanamiento en las instalaciones del edificio Ciencias Naturales ubicado en Caracas, donde operaba una red pornografía. Mediante labores de patrullaje informáticos, se determinó que estos operaban bajo un falso Call Center, donde al menos 70 personas, entre ellos 5 menores de edad, manejaban sitios web de pornografía, en el que ofrecían a diferentes costos dicho material, generando una de estas páginas en tan sólo un mes, 18 mil 500 dólares.	https://talcualdigital.com/index.php/2019/09/12/cicpc-desmantelo-dos-laboratorios-que-gestionaban-paginas-web-pornograficas-en-caracas/	Pornografía infantil
Agosto 2019	El inspector agregado del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), Alberto José Dugarte, reveló un incremento en los delitos informáticos en Venezuela, y resaltó que uno de los más frecuentes es el que se registra ante el acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos. https://vtv.gob.ve/wp-content/uploads/2019/07/CICPC.mp4 (Video)	http://www.ultimasnoticias.com.ve/noticias/sucesos/cicpc-combate-delitos-cometidos-en-redes/	Acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos.

Según se evidencia de los casos registrados o denuncias efectuadas ante la División de Delitos Informáticos del CICPC, el fraude y la oferta engañosa, incluidos dentro de los Delitos Contra la Propiedad y Delitos Contra el Orden Económico, son los que más se cometen en Venezuela, dada las condiciones políticas, económicas y sociales, muestran un crecimiento acelerado, igual importancia revisten los delitos contra los Niños, Niñas y

Adolescentes, producto de la pornografía infantil. En este sentido en el 2017 la CICPC desarrolló campañas comunicacionales como la de "No te Enredes con las Redes", dirigida a más de mil doscientos alumnos pertenecientes a diez instituciones educativas de la Gran Caracas, con el objetivo de informar a las niñas, niños y adolescentes en cuanto al uso adecuado, manejo y prevención de las diversas redes sociales.

Hechos delictivos en las redes sociales en Venezuela

Uno de los principales delitos informáticos que se cometen en Venezuela, a través de las redes sociales es el fraude, aunque el sabotaje y desmejoramiento de los servicios públicos también se presentan. Según CONATEL la delincuencia organizada de Venezuela encuentra en las redes sociales el lugar ideal para cometer delitos cibernéticos, el cual han venido aumentando desde el año 2012[9].

Los principales fraudes que se cometen a través de redes sociales en Venezuela son:

- **Transacciones comerciales** Es uno de los delitos virtuales más frecuentes en Venezuela. Los estafadores suelen ofrecer algún producto o servicio en un portal web o cuenta en redes sociales. El fraude ocurre, cuando el comprador, tras haber cancelado el importe del producto, nunca lo recibe. El principal fraude que se comete a través de las redes sociales deriva de las transacciones comerciales, y se materializa cuando el comprador, tras haber cancelado el importe del producto, nunca lo recibe.
- **El phishing** es un término informático que denota ingeniería social para adquirir información confidencial de forma fraudulenta. Por lo general el fraude es cometido con el envío de información engañosa, como el hacer creer que el usuario se ha ganado un premio y que para obtenerlo debe ingresar datos personales, como nombres y números de cuentas bancarias.
- **Catfish**, mejor conocido como identidad falsa. La implementación más común de este tipo de fraude es cuando las personas mienten sobre su identidad en la web con el fin de crear relaciones románticas y obtener beneficios económicos de esto. Las personas más vulnerables a este tipo de ataques cibernéticos son las niñas, niños y adolescentes, pues crean un vínculo con el estafador, quien, basándose en un sentimiento de amor, amistad o lástima, exige dinero a las víctimas.
- **Estafas por venta de divisas,** el delincuente usurpa la identidad de una persona en las redes sociales y oferta divisas, los estafados realizan la trasferencia del dinero y el delincuente desaparece. Posteriormente, los ciudadanos acuden al usurpado para exigir los montos equivalentes y el titular de la cuenta desconoce la operación[10].
- **Estafas por trámites para gestionar documentos oficiales,** los delincuentes ofrecen gestionar pasaportes y cédulas a través de las instituciones correspondientes, le exigen grandes cantidades de dinero a los ciudadanos para realizar el trámite, los ciudadanos transfieren los montos y después desaparecen los delincuentes[11].

También se pueden cometer a través de redes sociales delitos informáticos distintos al fraude enfocados en el sabotaje y desmejoramiento de los servicios públicos.

[9] http://www.conatel.gob.ve/el-fraude-y-las-redes-sociales-en-venezuela/
[10] https://twitter.com/leoperiodista/status/1186041936911781890?s=03
[11] https://twitter.com/noticias24/status/1190249675795968003