Fondo Editorial de la Universidad Bicentenaria de Aragua
Revista Arbitrada Investigación y Creatividad | Dirección de Investigación
Volumen 22 Nro.2. 2025 (julio-diciembre)
Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

CIBERATAQUE Y SU APLICABILIDAD EN EL DERECHO PENAL VENEZOLANO

Evelyn A. Russián
Magíster en Orientación Educativa
https://0009-0003-2387-4712
Facultad de Ciencias Jurídicas y Políticas
Escuela de Derecho de la Universidad Bicentenaria de Aragua.
evelynarussian@gmail.com

Fecha de aceptación: noviembre 2025 Fecha de publicación: diciembre 2025.

Resumen

Este artículo aborda los ciberataques y sus aplicaciones en el derecho penal venezolano. Describe los principales tipos existentes y su aplicabilidad en dicho derecho para determinar si el marco legal actual es suficiente para abordar la complejidad de estos delitos o si, por el contrario, presenta lagunas y limitaciones que requieren una reforma legislativa. Metodológicamente, se basa en un enfoque cualitativo y exploratorio mediante un estudio documental donde se revisan informes de agencias de seguridad, agencias de ciberseguridad, trabajos académicos y la legislación vigente, con el propósito de obtener hallazgos que sirvan de base para formular recomendaciones para minimizar los ciberataques en el contexto del derecho penal venezolano. Se definieron los tipos más comunes de ciberataques. Se concluye que Venezuela cuenta con un marco legal específico para ciberataques, como la Ley Especial contra los Delitos Informáticos (2001), que permite sancionar diversas conductas ilícitas en el ámbito digital. También es cierto que, la rápida evolución tecnológica y la sofisticación de los ciberdelincuentes exigen una revisión y adaptación continua de la normativa y de las capacidades de los organismos responsables de su aplicación y que solo a través de un enfoque integral, sólido y adaptable se podrá garantizar que los organismos de seguridad estatales, resguarden la seguridad digital y la protección de los bienes jurídicos en la sociedad venezolana.

Palabras clave: cibercriminal, delito informático, derecho penal, disposiciones legales, tecnologías de la información

CYBERATTACK AND ITS APPLICABILITY IN VENEZUELAN CRIMINAL LAW

Abstract

This article addresses cyberattacks and their applications in Venezuelan criminal law. It describes the main types of cyberattacks and their applicability within this legal framework to determine whether the current legal structure is sufficient to address the complexity of these crimes or whether, on the contrary, it presents gaps and limitations that require legislative reform. Methodologically, it employs a qualitative

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

and exploratory approach through a documentary study that reviews reports from security agencies, cybersecurity agencies, academic works, and current legislation. The aim is to obtain findings that will serve as a basis for formulating recommendations to minimize cyberattacks within the context of Venezuelan criminal law. The most common types of cyberattacks are defined. The article concludes that Venezuela has a specific legal framework for cyberattacks, such as the Special Law against Computer Crimes (2001), which allows for the prosecution of various illicit activities in the digital sphere. It is also true that the rapid pace of technological evolution and the increasing sophistication of cybercriminals demand continuous review and adaptation of regulations and the capabilities of the agencies responsible for their enforcement. Only through a comprehensive, robust, and adaptable approach can it be guaranteed that state security agencies safeguard digital security and protect legally protected interests in Venezuelan society.
Keywords: cybercrime, computer crime, criminal law, legal provisions, information technologies

CYBERATTAQUES ET LEUR APPLICABILITÉ EN DROIT PÉNAL VÉNÉZUELIEN

Résumé

Cet article traite des cyberattaques et de leur application en droit pénal vénézuélien. Il décrit les principaux types existants et leur applicabilité dans ce cadre juridique afin de déterminer si le cadre actuel est suffisant pour appréhender la complexité de ces infractions ou s'il présente, au contraire, des lacunes et des limitations nécessitant une réforme législative. Sur le plan méthodologique, cette étude adopte une approche qualitative et exploratoire, fondée sur une analyse documentaire de rapports d'agences de sécurité, d'agences de cybersécurité, de travaux universitaires et de la législation en vigueur. L'objectif est d'obtenir des résultats qui serviront de base à la formulation de recommandations visant à minimiser les cyberattaques dans le contexte du droit pénal vénézuélien. Les types de cyberattaques les plus courants ont été définis. L'étude conclut que le Venezuela dispose d'un cadre juridique spécifique pour les cyberattaques, notamment la Loi spéciale contre la cybercriminalité (2001), qui permet de poursuivre diverses activités illicites dans le domaine numérique. Cependant, il est également vrai que l'évolution technologique rapide et la sophistication des cybercriminels exigent une révision et une adaptation constantes de la réglementation et des capacités des organismes chargés de son application. Seule une approche globale, rigoureuse et adaptable permettra de garantir que les services de sécurité de l'État protègent la sécurité numérique et les intérêts légalement protégés au sein de la société vénézuélienne.

Mots-clés : cybercriminalité, criminalité informatique, droit pénal, dispositions légales, technologies de l'information

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

Introducción

Según Talavera, (2018: 9) un ciberataque es una "acción intencionada que se inicia en un equipo informático, con el objetivo de comprometer la confidencialidad, disponibilidad o integridad del equipo, red o sitio web atacado y de la información contenida o transmitida a través de ellos". Es decir, dirigida a vulnerar la confidencialidad en el ciberespacio informático. El auge de la digitalización ha incrementado vertiginosamente las posibilidades de ataque ocasionando problemas a diversos sectores como la banca, compañías estatales, la seguridad, la defensa, la salud y telecomunicaciones, el comercio, entre otros.

Natalucci, Quereshi y Suntheim (2024:1) han señalado que, "el riesgo de ataques cibernéticos con consecuencias sistémicas ha aumentado debido a una mayor digitalización y tensiones geopolíticas que van en aumento". El ciberataque ha existido desde el surgimiento de la informática. Esta se retrotrae desde la existencia del ábaco -herramienta de cálculo usada por los chinos y japoneses durante siglos, para representar números y usar operaciones aritméticas: suma, resta, multiplicaciones y divisiones; sin embargo, es con el gusano de Morris en 1988 cuando se suscita un evento que marca la evolución del malware, sin embargo, investigaciones desde la Universidad de Monroe han sostenido que, "las mayores violaciones de datos de la historia han ocurrido desde 2005. A medida que las empresas y los gobiernos pasaron del papel a los registros e información digitales, las violaciones de datos aumentaron en frecuencia e intensidad"

Concebir los ciberataques en este contexto, es fundamental para atenuar los riesgos relacionados y asociados a estos delitos y proteger la integridad de la información y los sistemas críticos. Según el informe de la Organización de los Estados Americanos (OEA, 2020), los ciberataques en América Latina han crecido a un ritmo alarmante, evidenciando la necesidad de marcos legales vigorosos. La era digital ha acelerado las interacciones humanas, la economía, al igual que la gestión pública, propiciando un desarrollo tecnológico sin precedentes; pero a pesar

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

de estos avances comunicacionales, también han permitido nuevas maneras de amenazas delincuenciales, verbigracia, los ciberataques. Según Almario, (2022: 22)

> Ante la constante evolución de los sistemas informáticos, es importante mencionar que a nivel mundial ha surgido la necesidad de proponer regulaciones y debates acerca del ámbito cibernético, con el fin de sugerir medidas de seguridad en el ciberespacio, teniendo en cuenta que este tipo de afectaciones puede perturbar la economía y estabilidad de los países.

Esto pasa por la interrupción de servicios esenciales hasta el robo masivo de datos personales, incidentes estos que impactan intensamente la seguridad individual, empresarial y estatal. La globalización del ciberespacio implica que, un ataque originado en cualquier parte del mundo puede repercutir en distintas y distantes jurisdicciones planteando desafíos significativos para la atribución de responsabilidad y la cooperación internacional.

En el contexto venezolano, se han dado pasos legislativos importantes con la promulgación de la Ley Especial Contra los Delitos Informáticos (LECDI: 2001), sin embargo, la dinámica evolutiva de la ciberdelincuencia exige una revisión constante de la normativa vigente. En este sentido, se clasifican los tipos de ciberataques más relevantes en la actualidad y, en consecuencia, verificar cómo el derecho penal venezolano, particularmente la (LECDI:2001), contempla y sanciona estas conductas. Este artículo a través de una revisión profundiza acerca del ciberataque y su aplicabilidad en el derecho penal venezolano, busca determinar si el marco legal actual es suficiente para enfrentar la complejidad de estos delitos o si, por el contrario, presenta vacíos y limitaciones que requieran una reforma legislativa.

Metodológicamente se basa en un enfoque cualitativo y exploratorio, a través de un estudio documental donde se revisan informes de organismos de seguridad, agencias de ciberseguridad, trabajos académicos y la legislación vigente, para obtener hallazgos que puedan dar pie o base, a la formulación de recomendaciones

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

en procura de minimizar los ciberataques en el contexto del derecho penal venezolano. En este orden de ideas, el artículo 1 de la (LECDI: 2001), establece:

> 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.

Se evidencia del artículo citado, cómo establece la protección integral de los sistemas que usan las tecnologías de información, resaltando las medidas preventivas, así como el castigo o sanción contra quienes cometan delitos previstos en esta Ley, cualquiera sea sus componentes. Al revisar la literatura sobre el ciberataque, se encuentran diversos tipos que, a los efectos de mejor comprensión, se abordan de manera sistémica, comenzando por los más comunes. Así se tiene:

Los ciberataques que afectan la confiabilidad de la información

En este renglón se halla el *Phishing*: (estafa informática) que es un tipo habitual de ataque cometido por la ciberdelincuencia y consiste en engañar a las personas a través de un mensaje de texto, correo electrónico, whatsapp, redes sociales, portales web, motores de búsqueda, spam, haciendo creer que provienen de instituciones fiables, con la intención de que la víctima revele informaciones confidenciales tales como datos bancarios, contraseñas, los números y claves de tarjetas. La Federal *Bureau of Investigation*)-Oficina Nacional de Identificación Criminal- (FBI:1896) señala:

> En una estafa de phishing, podrías recibir un correo electrónico que parece provenir de una empresa legítima y te pide que actualices o verifiques tu información personal respondiendo o visitando un sitio web. La dirección web podría ser similar a alguna que hayas usado antes. El correo electrónico podría ser lo suficientemente convincente como para que realices la acción solicitada.

De igual forma está el *Smishing*: este similar al *phishing*, pero usa mensajes SMS (servicio de mensajes cortos) para engañar a las víctimas. Según la empresa Proofpoint, (2025:1) "es un ciberataque que se dirige a las personas a través de SMS

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

o mensajes de texto. El término es una combinación de "SMS" y "*phishing*". También está el *Malware* (Software Malicioso) que según Proofpoint, (2025:1)

> Se usa para designar a una amplia gama de programas malintencionados que se insertan e instalan en los sistemas y servidores de los usuarios finales. Estos ataques están diseñados para dañar un ordenador, una red de ordenadores o un servidor, y son usados por ciberdelincuentes para obtener datos para conseguir ganancias financieras.

Debe señalarse que, dentro de este *Software* maliciosos, existen otras categorías de este como: *Ransomware:* estos son comunes hoy en día, y cifra los archivos, que no se pueden recuperar a menos que la víctima pague un rescate. Plaza, (2021:1) señala que son "conocidos con el nombre de extorsión digital o chantaje digital, son un tipo de ataques que bloquean el acceso a la información personal y archivos propios de un dispositivo".

De igual forma se habla de Virus: el cual infecta a un ordenador y. puede corromper archivos, destruir sistemas operativos, eliminar o desplazar archivos o desplegar una carga útil en una fecha dada. Según el Glosario de Términos de la Tecnología de la Información y Comunicación (Glosario TIC ALFAFAR: 2014:96)

> Un virus informático es un programa de ordenador que puede infectar otros programas modificándolos, para incluir una copia de sí mismo. Los virus pueden destruir intencionadamente datos en la computadora, aunque también existen otros más benignos, que se caracterizan solo, por las molestias que ocasionan. Según lo infectado, se denominan: virus de acción directa, residentes, de archivos, del sistema operativo, etc. Según su comportamiento, se denominan: Virus uniformes, encriptados, de sobre escritura, silenciosos, etc.Es sabido que estos virus generalmente atacan o bloquean el acceso a la información personal y a los archivos de los dispositivos. Asimismo, se habla de Gusanos o virus autor replicante, que no afecta a archivos locales, sino que se propagan a otros sistemas y agota los recursos. El Banco Vizcaya Argentaria S.A (BBVA:2023:1) los define como "programas maliciosos que tienen la capacidad de reproducirse, realizando copias de sí mismos en los dispositivos de las víctimas e infectando otros equipos".

Dentro de estos *Software* se cuentan los Troyanos: se llaman así rememorando la estrategia militar griega, en la que los soldados aqueos usaron un caballo de madera (el Caballo de Troya), para poder entrar a la ciudad de Troya sin ser

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

detectados. El *malware* se hace pasar por un programa inofensivo, pero se ejecuta en segundo plano, robándose los datos y permitiendo el control remoto del sistema, o esperando una orden por parte del atacante para desplegar una carga útil, entre otros. La compañía de ciberseguridad *es et Progresss.Protected*, lo define como un tipo de *software* malicioso que se *"disfraza"* para ocultar sus verdaderas intenciones.

De igual manera se encuentran los *Spyware*: Fortinet (2023:1), lo define como un *software* malicioso "que ingresa a la computadora de un usuario, recopila datos del dispositivo y del usuario y los envía a terceros sin su consentimiento. Lo define como cadena de *malware* diseñada para acceder y dañar un dispositivo sin el consentimiento del usuario. Al igual que los *Malware* (Software Malicioso), los *Spyware*, también tiene algunos tipos como los que sigue:

En cuanto al *Adware*: se ubica en un dispositivo y monitorea la actividad de los usuarios, para luego vender sus datos a anunciantes y actores maliciosos o publicita anuncios maliciosos.

-Registradores de teclas: Registran las pulsaciones de teclas que un usuario realiza en su dispositivo infectado guardando los datos en un archivo de registro cifrado. Este método de *spyware* recaba toda la información que el usuario escribe en sus dispositivos, como datos de correo electrónico, contraseñas, mensajes de texto y nombres de usuario.

-Monitores del sistema: rastrean la actividad del usuario en su computadora, capturando información como correos electrónicos enviados, redes sociales y otros sitios visitados y pulsaciones de teclas.

En cuanto los *Cookies* de seguimiento: estos se colocan en un dispositivo mediante un sitio web y luego se utilizan para seguir la actividad en línea del usuario. Los *Keyloggers*: según Proofpoint, (2025:1)

> Son programas que se ejecutan como un proceso en segundo plano en un ordenador u otro dispositivo y registran las pulsaciones de teclas que realiza un usuario sobre su teclado. Pueden tener propósitos tanto legítimos como malintencionados, dependiendo de los objetivos que persiga aquel que los instala. Los keyloggers son conocidos por su intención perversa de recopilar las credenciales del usuario objetivo, así

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

como otros datos importantes, pero también se pueden usar para control parental y proteger la seguridad de menores de edad.

De acuerdo con esta empresa experta en ciberseguridad, “una instalación en Windows podría ejecutarse sin necesidad de recibir instrucciones por parte del propietario del ordenador y comenzar inmediatamente a registrar pulsaciones de teclas sin que el rendimiento del dispositivo presente cambios detectables”. Se necesita ser diestro para investigar e identificar el proceso malintencionado, sin embargo, gran parte de los usuarios no son capaces de distinguir entre los ejecutables necesarios de Windows y el contenido malintencionado.

Los ciberataques que atacan la integridad de la información o sistema

Entre ellos está *el Ransomware:* este tipo de *malware se* propaga por email (el cual lleva insertado un virus malicioso) y secuestra toda la información, cifrando los archivos, para pedir un rescate económico a cambio de los datos. Según Kosinski (2024:1) “retiene los datos o el dispositivo confidenciales de una víctima, amenazando con mantenerlos bloqueados, o peor, a menos que la víctima pague un rescate al atacante. “

Defacement Web: también conocido como desfiguración web. Este ataque cibernético modifica la apariencia de un sitio web sin autorización. Según Grozeva (2013:1) “se refiere a cualquier cambio no autorizado realizado en la apariencia de una sola página web o de un sitio completo”. Los atacantes, se conocen como *defacers*, alteran con frecuencia el contenido, imágenes o enlaces para mostrar mensajes políticos, publicidad o para realizar vandalismo. Este tipo de ataque a menudo ocasionan graves consecuencias, incluyendo daños a la reputación, pérdidas financieras y riesgos de violación de datos. Algunos delincuentes utilizan técnicas de fuerza bruta; pueden acceder a puntos vulnerables dentro de los sitios web y ejecutar técnicas como inyección SQL, o secuencias de comandos entre sitios (XSS), enviando malware a los administradores del sitio web.

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

Se hace necesario la detección y monitorización para identificar y prevenir el ataque. Según Avast Academy (2020:2) “es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos”

Manipulación de Datos: es la alteración o modificación no autorizada de datos dentro de un sistema informático con fines maliciosos. Este tipo de ataque busca, entre otro, robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital. La Computing-Tabulating-Recording Company (IBM:1911), sostiene que “los ataques de manipulación de datos pueden ser sutiles, haciendo que sean difíciles de detectar, y pueden tener consecuencias graves para las organizaciones”.

Los ciberataques que atacan la disponibilidad de los servicios

Denegación de Servicio *(DoS),* de acuerdo con Manota, **(**2022:5)

> La abreviatura DDoS significa Distributed Denial Of Service. Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a los recursos de red, como la infraestructura sobre la que se basa el sitio web de una empresa. El ataque DDoS enviará gran cantidad de solicitudes al recurso web atacado con el fin de superar la capacidad del sitio web para gestionar tantas solicitudes y evitar así que este funcione correctamente.

Se deduce de lo citado que, la denegación de servicio (DDoS) es un ataque que busca atacar ciertos sectores distrayéndolos con menudencias o cortinas de humo para distraerlos, mientras preparan ataques más complejos. Es muy común en los sectores, médicos, educativos, financieros y gubernamentales.

Los ciberataques que atacan la autenticación, autorización

*Cracking de Contraseñas***:** tiene que ver con el descifrado de contraseñas a menudo con fines maliciosos. Esta puede pertenecer a un usuario o a un

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

administrador. El ciberdelincuente puede usar la contraseña de un usuario autorizado para robar sus credenciales bancarias e incluso su dinero. Awati y Gillis (2025) este descifrado "consiste en usar una aplicación para identificar una contraseña desconocida u olvidada que permite el acceso a un equipo o recurso de red." Es decir, puede facilitar a los usuarios recuperar contraseñas olvidadas y a los administradores si las contraseñas son débiles.

*Spoofing (Suplantación), s*e conoce como suplantación de identidad. De acuerdo con Urrutia y Julca (2024:1)

> Este tipo de ataques de spoofing, tiene como principal objetivo perjudicar la privacidad de usuarios que se encuentre dentro de una red, ya sea doméstica o empresarial, puesto que es un problema que estaría provocando pérdidas financieras, por lo que estaría afectando la integridad de las personas, debido a que la información es leída o modificada, cuando el atacante logra interceptar el flujo de datos, afectando la confidencialidad de las posibles víctimas.

Esta técnica se usa en ciberseguridad por un atacante que se hace pasar por una fuente legítima para engañar a la víctima y obtener información confidencial, realizar fraudes o propagar *malware*. En esencia, el *spoofing* busca disfrazar la verdadera identidad del atacante para que la víctima confíe en la comunicación o la acción.

En cuanto a la aplicabilidad del derecho penal venezolano, debe decirse que la Ley Especial Contra los Delitos Informáticos (LECDI: 2001), clasifica los delitos informáticos en categorías protegiendo diversos bienes jurídicos. El objeto de esta Ley lo contiene su artículo 1, indicando la protección integral de los sistemas que usan tecnologías de información. También garantiza la prevención y sanciona los delitos cometidos contra tales sistemas o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos contemplados en esta Ley. De esta manera el artículo 2, de la Ley, señala los términos clave relacionados con las tecnologías de la información, sistemas, datos, información, documento, computador*, hardware,*

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

firmware, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña *(password),* y mensaje de datos

Ahora bien, el Título II, Capítulo I de la Ley en comento, contempla los delitos contra los sistemas que utilizan tecnologías de información, señalando en su art. 6 el acceso indebido; en el art.7, sabotaje o daño a sistemas; art. 8, favorecimiento culposo del sabotaje o daño; en su art.9, acceso indebido o sabotaje a sistemas protegidos; el art. 10 posesión de equipos o prestación de servicios de sabotaje; espionaje informático en el art. 11, y la falsificación de documentos (art.12). En su Capítulo II, contempla, los Delitos contra la Propiedad tales como**:** hurto (art. 13); fraude (art.14); obtención indebida de bienes o servicios (art.15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (art.17).

Posesión de equipo para falsificaciones. (art 19). El Capítulo III, de la mencionada Ley contempla los delitos contra la privacidad de las personas y de las comunicaciones: el art. 20, contiene la violación de la privacidad de la data o información de carácter personal; violación de la privacidad de las comunicaciones (art.21); revelación indebida de data o información de carácter personal (art.22). El Capítulo IV refiere a los delitos contra niños, niñas y adolescentes: así el art. 23, se refiere a la difusión o exhibición de material pornográfico; el (art. 24); exhibición pornográfica de niños o adolescentes. El Capítulo V refiere a los delitos contra el orden económico, destacando en su art. 25, la apropiación de propiedad intelectual. La oferta engañosa en su art. 26.

En resumen, Venezuela cuenta con un marco legal específico para los ciberataques a través de la Ley Especial contra los Delitos Informáticos, que ha permitido sancionar diversas conductas ilícitas en el ámbito digital; sin embargo, la constante evolución tecnológica y la sofisticación de los ciberdelincuentes exigen una revisión y adaptación continua de la normativa y de las capacidades de los organismos encargados de su aplicación. Por cuanto es un tema que amerita estar revisándolo a menudo, habida cuenta que involucra diversos sectores del mundo

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

informático, no debe dejarse a un lado; sobre todo, quienes están ávidos de hallar nuevas fórmulas de solución para este tipo de amenazas.

Conclusión

En esta era digital que vivimos, la interconexión global y la dependencia de la tecnología han traído no solo avances y comodidades para casi todas las facetas de la vida cotidiana, sino también nuevas amenazas. Los ciberataques, entendidos como acciones deliberadas para comprometer la integridad, confidencialidad o disponibilidad de sistemas informáticos, redes o datos, se han convertido en una preocupación creciente a nivel mundial. La aplicabilidad del Derecho Penal venezolano a los ciberataques, se basa fundamentalmente en la Ley Especial Contra los Delitos Informáticos (2001).

Esta normativa ha permitido perseguir y sancionar diversas conductas ilícitas en el ámbito digital. Sin embargo, para enfrentar eficazmente la creciente amenaza de los ciberataques, es fundamental continuar fortaleciendo las capacidades investigativas, así como promover la cooperación internacional sobre la ciberdelincuencia; no solo a través de la Convención de las Naciones Unidas suscrito por Venezuela en el año 2025, sino a través de otros convenios como el Convenio N° 185 del Consejo de Europa sobre la Ciberdelincuencia o Convenio de Budapest, para combatir el crimen organizado y así evaluar la necesidad de actualizar el marco jurídico para que responda de manera más ágil a las nuevas modalidades delictivas que nacen o se derivan en el ciberespacio. Solo a través de un enfoque integral, sólido y adaptable, se podrá garantizar que los organismos de seguridad estatales, resguarden la seguridad digital y la protección de los bienes jurídicos en la sociedad venezolana.

Referencias

Awati, R., y Gillis, A., (2025). *¿Qué es el descifrado de contraseñas? Red Tech Target. Seguridad.* URL. tttps://www.techtarget.com/searchsecurity/definition/password-cracker

Almario, P., (2022). *Análisis de las amenazas y riesgos cibernéticos que afrontan*

los usuarios y las organizaciones en la consulta y/o adquisición de servicios turísticos a través de medios electrónicos. [Proyecto de Grado] Monografía presentado para optar por el título de Especialista en Seguridad Informática Universidad Nacional Abierta y a Distancia–UNADESCUELA de Ciencias Básicas, Tecnología e Ingeniería -ECBTI Especialización en seguridad Informática. 2022. https://repository.unad.edu.co/handle/10596/53985

Avast Adademy (2020). *¿Qué es la inyección de SQL y cómo funciona?* (Blogs.) https://www.avast.com/es-es/c- sql-injection

Banco Vizcaya Argentaria BBVA.S. A (1988). *¿Qué es un gusano informático y en qué se diferencia de un virus?* .URL https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques- informaticos/que-es-un-gusano informatico.html.

Computing-Tabulating-Recording Company (IBM:1911). https://www.ibm.com/history/ctr- and-ibm

Convenio de las Naciones Unidas (2025). Convenio sobre la Ciberdelincuencia, N° 185.Budapest, 23. XI. 2021 URL https://www.oas.org/uridico/english/cyb_pry_convenio.pdf

Es et Progresss.Protected (2025). *Plataforma de gestión de seguridad unificada que brinda una visibilidad superior de la red*. URL. https://www.eset.com/es/caracteristicas/malware-troyano/?srsltid=AfmBOoo-RiB79BxfdD_YNt-bV8ElUZd4vv0sAqyn7WZw7RVlnqWk7MpY

Federal Bureau of Investigation (1896). *Suplantación de identidad y phishing.* Sitio Web Oficial del gobierno de los Estados Unidos. https://www.fbi.gov/how-we-can-help- you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing

Fortinet (2023*. Definición de spyware*. Informe Global Sobre el Panorama de amenazas de 2H de 2023. https://www.fortinet.com/lat/resources/cyberglossary/spyware

Glosario de Términos de la *Tecnología de la Información y Comunicación* (2014). URL https://www.alfafar.es/wp-content/uploads/2014/11/Glosario_TIC_Alfafar.pdf.

Grozeva, L., (2013). *¿Qué es la desfiguración de un sitio web?* WebSitePulse Blog. 5 de marzo de 2013. https://www.websitepulse.com/blog/what-is-website-defacement#

Kosinski, (2024). *¿Qué es el ransomware?* IBM (International Business Machines Corporation). https://www.ibm.com/mx-es/think/topics/ransomware.

Ley *Especial contra Delitos Informáticos* (2021). Caracas, Gaceta Oficial de la República Bolivariana de Venezuela N° 37. 313.octubre 30,2001

Manota, (2022). *Ataques de denegación de servicio distribuido, Cómo evitarlos y cómo enfrentarlos.* Universidad Piloto de Colombia – Especialización En seguridad informática Bogotá D.C., Colombia. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12271/Articulo%20Mauricio%20Pacheco.pdf?sequence=1

Depósito Legal: pp200202AR286 ISSN: 1690-0685 ISSN: 2791-3589 (en línea)

Natalucci,F.,Quereshi, M.,y Suntheim, F.,(2024*). Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera*. IMF Blog. https://meetings.imf.org/es/IMF/Home/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Organización de Estados Americanos, (2020). *Ciberseguridad: Riesgos, Avances y el camino a seguir en América Latina y el Caribe*. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=AVI-095/20

Plaza, González, (2021). *Análisis de un ataque Ransomware Desarrollo del ransomware Gengar.* Facultat de Matemàtiques i Informàtica Universitat de Barcelona. [Trabajo de grado] Departament de Matemàtiques i Informàtica. https://diposit.ub.edu/dspace/bitstream/2445/182628/3/tfg_marcos_plaza_gonzalez.pdf

Proofpoint, (2025). *¿Qué s el Smishing?* Empresa de Ciberseguridad. https://www.proofpoint.com/es/threat-reference/smishing.

Política para su Talavera, Miranda, P, (2018). *¿Son los ciberataques un peligro inminente del siglo XXI? La pertinencia de la Comunicación estudio*.
https://www.academia.edu/38425156/Ciberataques_La_pertinencia_de_la_Comunicaci%C3%B3n_Pol%C3%ADtica_para_su_estudio_pdf

Universidad de Monroe (1933). *Historia de la ciberseguridad: piratería y vulneracio vulneraciones de datos.* https://www-monroeu-edu.translate.goog/news/cybersecurity-history-hacking-data-breaches?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Urrutia Vásquez M., y Julca Rojas, A., (2024). *Desarrollo de un método de identificación automática de ataques spoofing de envenenamiento Arp en la suplantación de identidad en redes lan*. Universidad Señor de Sipán. Chiclayo, Perú.https://repositorio.uss.edu.pe/handle/20.500.12802/13206