UNIVERSIDAD PERUANA DE LAS AMERICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACION

LOS DELITOS INFORMÁTICOS Y LOS DATOS EN SISTEMAS INFORMÁTICOS

PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

AUTOR:

PERALTA CASTRO RICARDO GOODIER
CODIGO ORCID: 0000-0002-1238-4254

ASESOR: Med. Abg.

CASTRO EGUAVIL JOSÉ CARLOS
CODIGO ORCID: 0000-0002-6548-0100

LINEA DE INVESTIGACION: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERU

MARZO, 2022

Resumen

Este trabajo plantea respecto a los delitos informáticos y los datos en sistemas informáticos; lo vulnerable que hoy en día resulta para la penetración por la ciberdelincuencia en un mundo globalizado transnacional, atentando pluriofensivamente los derechos fundamentales de las personas y la seguridad jurídica del propio Estado, como en el mundo, es necesario destacar que hoy en día toda actividad humana aplica el conocimiento al uso y empleo de las tecnologías de la información (TIC), como elemento importante en cada modernización del Estado, para ello el Perú no es la excepción, ya que dentro de sus políticas públicas de desarrollo, el Estado pone en práctica la modernidad de ello, facilitando en todas las entidades públicas su uso; y para ello desde luego que aparecen los llamados "ciberdelincuentes" que no son otra cosa de aquellos que cometen los delitos penetrando de muchas formas los sistemas informáticos, para sustraer así los datos contenidos en ellos, ya sea también en las diversas empresas privadas, bancos, empresas comerciales, etc.; defraudando desde muchos sitios del mundo ello, obteniendo ingentes cantidades de dinero, en perjuicio de la sociedad. Ante ello las autoridades en su condición de operadores de justicia en la búsqueda de la recolección de evidencias o pruebas tienen que estar a la vanguardia respecto los delitos informáticos, a fin de que no falle en sus procesos judiciales.

Palabras Clave: Delitos, datos, ataques cibernéticos, sistemas informáticos.

Abstract

This work raises regarding computer crimes and data in computer systems; how vulnerable it is today for the penetration by cybercrime in a transnational globalized world, multi-offensively attacking the fundamental rights of people and the legal security of the Peruvian State itself as in the world; and for this it is necessary to highlight that today during all human activity knowledge is applied to the use and employment of information technologies (ICT), as an important element in each modernization of the State, for this Peru is not the exception, since that within its public development policies, the State puts its modernity into practice, facilitating its use in all public entities; and for this, of course, the so-called "cybercriminals" appear, who are none other than those who commit crimes by penetrating computer systems in many ways, in order to steal the data contained in them, whether it is also in the various private companies, banks , trading companies, etc; defrauding from many places in the world, obtaining huge amounts of money, to the detriment of society. Given this, the authorities in their capacity as operators of justice in the search for the collection of evidence or evidence must be at the forefront regarding computer crimes, so that they do not fail in their judicial processes.

Keywords: Crimes, data, cyberattacks, computer systems.

Tabla de Contenidos

I. Introducción

Con el inicio del siglo XX, la globalización significó la revolución de la era digital, que viene cambiando la vida del ser humano, experimentan a diario cualquier interacción con dispositivos de alta gama, capaces de romper las barreras de tiempo espacio en todo aspecto (económico, tecnológico, político, social, cultural, etc.), generando la alta demanda de acceso de la sociedad al uso de las Tecnologías de la Información, lo que permite conocer de manera ágil el conocimiento y diversidad de información almacenada en internet, algunas con un alto grado de credibilidad y en beneficio del desarrollo de los Estados y otras que generan conflictos ante ciertos intereses muchas veces de connotación delictiva; en dicho sentido la criminalidad organizada para la comisión de sus delitos informáticos transnacionales viene utilizando los llamados ataques cibernéticos o ciberataque es una actividad maliciosa que se lleva a cabo por parte de un atacante informático afectando a una o múltiples víctimas, utilizando como medio la red (internet) pudiendo también atacar a nivel de red local para conseguir el control de la plataforma de sus víctimas o conseguir vulnerar de modo tal que pueda sacar un provecho de ella, principalmente económico aunque en algunos casos son de otro tipo (Alfaro, 2017).

En nuestro país la penetración a los sistemas de seguridad a los datos informáticos a través de los ataques cibernéticos o ciberataques por la delincuencia organizada, ya constituyen una amenaza constante en las plataformas digitales que almacena diversidad de datos de información y que, si son vulnerados a sus sistemas de seguridad, estos atentan los derechos fundamentales en la intimidad, libertad de información etc.

La importancia del tema radica en la necesidad de dimensionar la realidad de la vulnerabilidad de los datos informáticos pese a su seguridad, en que se infringe los Delitos informáticos conforme a la legislación peruana, ciberataques que ya vienen ocasionando grave daños a la seguridad informática de personas naturales y jurídicas.

Este trabajo se justifica por cuanto debemos asumir medidas de ciberseguridad que nos permitan contrarrestar este tipo de ataques, conocer debidamente las técnicas especiales de su investigación para la reunión de pruebas por los operadores de justicia durante la prosecución de un proceso penal; más aún en la actualidad, cuando por la pandemia del COVID19 el uso de los sistemas digitales e informáticos se ha incrementado.

Según información estadística registrada por la División de Investigación de Delitos de Alta Tecnología (DIVINDAT PNP), las denuncias en delitos informáticos al año 2016 registra 880, y al año 2018 con 3031, 2019 con 7814, 2020 con 9,787, y 2021 con 16,232 ante la aparición pandémica del Covid19, lo que hace indicar que dicha unidad especializada sufre falencias de escases de personal policial especializado a nivel nacional, resulta una de las investigaciones muy complejas y desconocidas por los operadores de justicia peruana.

A ello se tiene que, a la mayoría de ciudadanos al habérseles restringido su libertad de tránsito al no salir de sus viviendas, utilizaron los sistemas informáticos y tecnológicos con cierto desconocimiento, facilitaron por engaño brindar sus datos a los ciberdelincuentes quienes vaciaron en minutos sus cuentas bancarias, ante la creencia de estar seguros en el sistema financiero. La (DIVINDAT PNP), tiene la importante tarea investigatoria especializada en sus pesquisas cuando delincuentes comunes u organizaciones criminales

cometen los delitos a través de las TICS, realizando para ello análisis informático, forense y acciones de geolocalización; apoyando y asesorando a las distintas unidades de la PNP a nivel nacional a fin de reunir los elementos probatorios de acuerdo a la ley de Delitos informáticos Nº 30096, modificada en la Nº 30171 del 10MAR2014.

II. Antecedentes

La llegada de la tecnología se remonta en la segunda parte del S. XX. En la cual este tuvo 5 generaciones: pero nos vamos a situar en la última (1981 – hasta la actualidad) en la cual se empieza a usarse la inteligencia artificial.

Por otro lado, con la llegada de esta tecnología, se buscaba garantizar la unificación de las personas. Pero como todo va evolucionando, la delincuencia a la par con ello y de esta curiosidad por transgredir a la norma sea peruana o internacional, nace lo que hoy conocemos como la “ciberdelincuencia”.

2.1 Antecedentes nacionales

Huamán (2020) explica que los delitos informáticos en el Perú, de manera progresiva tiene su inicio en 1991 en concordancia con el Código Penal, es así que específicamente el año 2013 se promulga la Ley 30096 y su modificatoria Nº30171, hasta suscribirse del Convenio de Budapest, conllevando a contar con una legislación equiparable a la legislación comparada de los delitos informáticos.

La problemática de este delito, radica en el acceso a través diversos instrumentos tecnológicos por parte de los ciberdelincuentes, hechos que dificultan su apropiada ubicación e identificación.

Vilca (2018) concluye que, el desconocimiento de los límites de la tecnología informática por falta de información, resulta un factor crítico que llega a impactar como delitos informáticos; por ello, es requerible contar con mayores conocimientos tecnológicos para un adecuado manejo de situaciones.

Ante el hecho de aquellos que incurren en la comisión de delitos informáticos, deviene el problema que afecta a la sociedad mundial, donde la edad y género son vulnerables a la red de algún delito o crimen cibernético, por eso, es necesario la capacidad profesional de un investigador o perito en la escena de crimen y un correcto procedimiento de la misma.

Por otro lado, este tipo de delitos informáticos son por lo general, de aquella ignorancia de la sociedad en base a este tema, por el hecho de que, con la existencia de estas normas, se especifica de los actos o hechos que se consideran “hackers”.

Es por ello, que, mediante una buena instrucción de los agentes de investigación en crímenes informáticos, estos tendrán bajo control jurídico los elementos o indicios necesarios a ser considerados como evidencia y prueba durante el proceso penal.

2.2 Antecedentes internacionales

Ruiz (2016) manifiesta que actualmente, la necesidad de que las personas se comuniquen, conlleva a que haya un avance en las tecnologías de la información (TICS), permitiendo una aceleración en los delitos informáticos. Es por ello que, para legislar en la tipicidad a sancionar respecto a la sustracción ilícita de la información privada de las personas a través de las redes, se debe considerar precautelar la integridad y la intimidad de personas; es decir, de los ecuatorianos.

En muchas ocasiones, este delito no solo transgrede la privacidad de las personas, sino que este afecta de forma global.

Echevarría (2015) concluye que, cuando la tecnología avanza, aparecen nuevas formas y métodos para delinquir, utilizando medios tecnológicos que, por tener un libre

acceso, las personas se confías y terminan agregando información en donde no deberían hacerlo.

A ello se tiene que los más propensos a la divulgación de su información sin su consentimiento, se da en aquellas personas que carecen de conocimientos informáticos básicos y por ende resultan vulnerables a ser víctimas de un delito informático.

III. Base teórica

3.1 Definiciones

3.1.1 Delitos Informáticos

El derecho y la sociedad siempre han estado en constante cambio, por lo que el derecho siempre se está adecuando a las necesidades que se necesita.

Para el derecho penal, aún no existe abundancia doctrinaria respecto a los delitos informáticos, debido a que la actividad criminal dentro su desarrollo comprende una variedad de acciones, difícil de establecer en una sola definición**.**

Como menciona Camacho citado en el libro del Dr. Santiago Acurio del Pino; en todas las fases de la actividad humana existe todo tipo de engaños, manipulaciones, codicia, fraude, venganza, etc. Por ello, con el desarrollo de la tecnología, nace el fraude, robo, espionaje, sabotaje e incluso hasta asesinato. (Acuario del Pino, S/F, p. 7)

Mediante las palabras de los autores Fernández Villegas, Vivanco Quinto & Vara Morocco citados por Juan Blossiers;

> "(…) cabe mencionar que existen principales cambios, como progreso o la actualización de la tecnología, en relación a la informática.

Por eso, existen comportamientos ilícitos en las cuales se denominan como delitos informáticos, el cual existe un sujeto activo que mediante sus acciones van a provocar una afectación al sujeto pasivo, causo así un daño y

vulnerando su privacidad, intimidad e incluso su patrimonio. Así mismo, en referencia a la informática, este es un proceso automático de información en base al uso de dispositivos electrónicos y computacionales o sistemas informáticos, cumpliendo tres tareas básicas: captar la información, procesamiento de la información y la transmisión de estos resultados; a este conjunto se le conoce como “algoritmo” (Blossiers, 2018, p. 20)

Villavicencio citado en su trabajo de Elías Chávez; la define como aquella conducta que busca burlar y vulnerar los sistemas en los equipos informáticos, rompiendo y penetrando en su seguridad, llámese, computadoras, laptops, sistema de datas. (Chávez, 2018, p. 43)

El Dr. Acurio del Pino citado en el mismo trabajo, define a la delincuencia informática a toda aquella conducta ilícita e ilegal, en otras buscando destruir, manipular cualquier equipo tecnológico, poniendo en peligro cualquier bien jurídico protegido en ello. (Chávez, 2018, p. 43)

Por otro lado, el Convenio de Ciberdelincuencia del Consejo de Europa menciona que son aquellos actos en la cual van en contra de la confidencialidad, disponibilidad e integridad de los sistemas informáticos; así como, datos y redes informáticos. (Haarscher, 2012, p. 12)

Finalmente, la INTERPOL citado en la tesis de Carlos Reyes, señala que se categoriza en variedades como: ataques contra los sistemas informáticos, usurparse la identidad, difundirse imágenes sexuales en agravio de menores

de edad, irrupción en servicios financieros, estafas por internet, propagación de virus, phishing y botnets (Reyes, 2020, p. 23)

3.1.2 Tipos de delitos informáticos: estos son algunos tipos que se encuentran dentro de los delitos informáticos.

3.1.2.1 Los fraudes:

Para la Ley N°30096 citado en la tesis de Carlos Reyes; el fraude se da utilizando las TICS o las tecnologías de información, realizando para sí o un tercero, el beneficio ilícito con claro perjuicio del individuo a través de la manipulación en el funcionamiento del sistema informático.(Reyes, 2020, p. 27).

Los fraudes se dividen en:

Datos falsos o engaños, manipulación de programas o los famosos “caballos de troya”, la técnica del salami, falsificaciones informáticas, manipulación de los datos de salida y pishing. (Acuario del Pino, S/F, pps. 23-25)

3.1.2.2 Sabotaje informático:

Para Azaola citado en la tesis de Carlos Yupanqui; menciona que este se da al borrarse, modificarse, o altera sin autorización alguna las funciones y datos de una computadora con la finalidad de dificultar los funcionamientos normales de los sistemas con virus informáticos. (Yupanqui, 2015, p. 21)

Por otro lado, Morant citado en la misma tesis, menciona que este sabotaje informático es dirigido al utilizarse los sistemas informáticos, y dañándose a los programas. (Yupanqui, 2015, p. 21)

El sabotaje se divide en:

Bombas lógicas, virus informático, gusanos y malware, ciberterrorismo y ataques de denegación de servicio. (Acuario del Pino, S/F, p. 27)

3.1.3 Cibercriminalidad:

Fernando Miró Linares citado en su artículo por Julio García y Daniel Peña; menciona que el cibercrimen o criminalidad se refiere al vocablo anglosajón cybercrime, es decir, sirve para englobar a todo tipo de delincuencia relacionada con el uso de las Tecnologías de Información y Comunicación (TICS). (García & Peña, S/A, p. 9)

Según Walt citado en la tesis de Miriam Chilcon menciona que el cibercrimen es utilizado hoy en día para describir los delitos o daños en la cual resulten creadas por las tecnologías en red. (Chilcon, 2019, p. 26)

Cabe considerar que el autor Kuehl citado en el mismo trabajo de investigación; menciona que,

“es un conjunto entorno a la información, tiene carácter único y distintito por el hecho que se usa el espectro electromagnético, la electrónica, para crear, almacenar, modificar, intercambiar y explotar aquella información mediante

> las redes interconectadas e interdependientes, de esta forma se usarían las tecnologías de información y comunicación de forma informal al no estar autorizado". (Chilcon, 2019, p. 26)
>
> Por otro lado, este término engloba a un conjunto de actividades ilícitas realizadas en el ciberespacio, teniendo como objeto los sistemas informáticos, siempre que para su desarrollo y ejecución se usen las herramientas tecnológicas; es por ello que en función de la naturaleza del hecho punible nace el ciberterrorismo, ciberdelito o hacktivismo. (Ministerio del Interior, 2019, p. 5)

Casos de ataques cibernéticos:

a. Caso BCP. Hackers accedieron a datos de sus clientes

El Banco de Crédito revelo que en el 2018 sufrió un ataque informático que permitió a terceros acceder a datos de identificación personal, cuentas, números de tarjetas y saldos de un grupo de sus clientes, sin embargo, aseguran que no se sustrajo ni claves ni dinero, pero la interrogante que quedó es ¿A dónde fue toda esa información que se filtró? Los datos, exactamente alguien los subió a la Deep web, lo cual es de alto riesgo, pues al estar libremente expuestos los datos se genera mayor riesgo, pues no se sabe con qué fines los cibercriminales pueden estar consultando esta información. Al producirse esta filtración de datos muchas personas quedan expuestas: nombre, el teléfono celular, dirección, ocupación, esto es, datos que podrían ser utilizados para la extorsión, suplantación de identidad. La repercusión

negativa es que va a aumentar el número de estafas, ciber crimen. El BCP informo que, mediante el reforzamiento de sus sistemas de seguridad, la brecha de intrusión ya fue cerrada. (S/A, 2019).

IV. Legislación

a. Perú

La razón de ser de la Ley N°30096 Ley de delitos informáticos (LDI) busca prevenir y desde luego sancionar todas las conductas delictivas que vulneran o afectan los sistemas y datos informáticos, u otro bien jurídico de relevancia penal, ya sea cometida utilizando las tecnologías de la información o de la comunicación, garantizando la lucha eficaz contra la ciberdelincuencia. (Yupanqui, 2015, pág. 15)

Por otro lado, a través de la Resolución Ministerial N°622-96-MT-15-17 el Ministerio de transportes, comunicaciones, vivienda y construcción aprueba los procedimientos de inspección de requerimiento de información en relación al secreto de las telecomunicaciones y protección de datos. Lo que quiere decir que se busca establecer procedimientos adoptando medidas para las empresas operadoras de servicios públicos de telecomunicaciones para proteger el secreto de las telecomunicaciones y protección de estos datos; así se busca que se mantenga la confidencialidad de la información personal. (Resolución Ministerial Nº 622-96-MTC-15.17, 1996)

b. En Chile

La legislación chilena en su Ley N°19.223, esta ley fue publicada en el año 1993 específicamente el 7 de junio de ese año y promulgada el 28 de mayo de ese mismo año; en esa ley se busca la idoneidad de la información, su calidad, su tratamiento, sobre el contenido del sistema sistematizado, ya que la doctrina chilena

en describe a que los delitos informáticos resultan pluriofensivos, pudiendo atentar diversos bienes jurídicos. Así mismo, haciendo mención al art. 3 de dicha ley, menciona que “el que destruye o dañe los datos contenidos en su sistema de tratamiento de información”, con este artículo se busca proteger a aquellos programas que tienen la información tanto de los ciudadanos chilenos e información confidencial que involucren bancos o telefonías. (Ley 19.233, 1993)

c. En Colombia

La Ley 1273 del 2009, denomina “la protección de la información y de los datos”. A través de la modificación de estos artículos se busca sancionar a aquella vulneración en base a la protección de los datos informáticos, a todo sistema tecnológico o ya sea este de comunicaciones, salvaguardando la estricta confidencialidad de la información; lo que conllevo a que se legislara una serie de conductas delictivas conforme a su legislación. Lo que a comparación con la legislación peruana sería similar. (Ley 1273, 2009)

V. Jurisprudencia

a. Pleno Sentencia. 1100/2020

Mediante esta sentencia, el pleno del TC declarada infundada la demanda de hábeas corpus, que condenó a Marcos Morales Vargas por los delitos de fraude informático y falsificación de firma en documento privado, alegándose que los hechos se cometieron el julio del 2013, por lo que la ley 30096 por delitos informáticos aun entraba en vigencia el 22 de octubre del 2013. El aporte de la sentencia radica en que desde ya ni bien entró en vigencia dicha ley, la corte superior de justicia de Lima, aplicó sus agravantes, considerando el periodo del desarrollo del delito con la manipulación del password sobre las cuentas a plazo fijo, hasta su materialización de la sustracción del dinero en agravio de los ahorristas de la caja municipal de ahorro y crédito de Trujillo el 24marzo del 2014. (**Exp. N° 01189-2019-PHC/TC**).

VI. Tratados

6.1. Convenio sobre la Ciberdelincuencia. Budapest. 23. XI. 2001.

Este convenio es el primer tratado internacional, pone el especial énfasis de la lucha contra la ciberdelincuencia a nivel nacional e internacional, buscando la mayor cooperación e en la lucha eficaz con la finalidad de cooperar, proteger la puesta en peligro de determinadas informaciones confidenciales, el abuso de las redes y sistemas informáticos, a través de la vulneración ilícita de la base de datos personal o de entidades privadas o públicas de cualquier Estado, socavando los derechos fundamentales de las personas así como de la seguridad jurídica, pudiéndose así de dicha forma facilitar la tipificación de los autores inmersos en esta clase de delitos, así como busca eliminar algún obstáculo jurisdiccional, mejorando las técnicas de la investigación.

6.2 Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Pruebas en materia de Delitos Cibernéticos.

Mediante este convenio, se busca mantener la lucha del delito informático, a través de la cooperación que brinden los distintos países conformantes, que coadyuve a la recopilación de las pruebas durante los procesos penales, la conservación de estas en los distintos casos de delitos cibernéticos.

VII.Conclusiones

Conforme al mundo globalizado y a través de la modernidad se vienen empleando a nivel mundial el almacenamiento de datos personales, así como en las diversas entidades públicas o privadas, bajo el apoyo de cierta seguridad indispensable como soporte de garantías a sus actividades, las cuales no son obstáculo para ciertas organizaciones criminales o los llamados ciberdelincuentes quienes a través de técnicas o procedimientos tecnológicos sofisticados, acceden bajo diversas modalidades de engaño o fraude a los accesos bancarios de sus potenciales víctimas, vaciando sus cuentas financieras o suponiendo actividades comerciales.

Los ataques cibernéticos se orientan a dañar los sistemas informáticos de las víctimas, además de ocasionar daño patrimonial. Se trata de ciberataques que dejan expuestos sus datos. Los ciberdelincuentes que realizan estos ataques no siempre tienen su foco en atacar directamente las fuentes de financiación de las empresas; robar, secuestrar o modificar información confidencial también son sus objetivos.

Los casos de ciberataques señalados rebelan que este tipo de criminalidad puede impactar profundamente en los sistemas informáticos y digitales. En el Perú los ataques cibernéticos se producen desde países lejanos como Rusia y Moldavia, pudiendo atacar a grandes corporaciones, bancos y personas naturales. Cabe señalar que los sistemas informáticos de diferentes entidades públicas del Estado han sufrido ataques cibernéticos, exponiendo públicamente toda la información que guardaban. Esto demuestra la enorme vulnerabilidad de la información digital en nuestro país.

VIII. Aporte de la Investigación

En suma, el presente trabajo, tiene por objeto difundir para conocimiento público, sobre los alcances que implican el uso de los sistemas informáticos en que se almacenan los datos propios de cada uno o de empresas públicas o privadas muchas veces como fuente abierta a través de OSINT (Open Source Intelligence) es una disciplina en pleno crecimiento y maduración que tiene un potencial prometedor en las investigaciones policiales realizadas por el personal de la Policía Nacional del Perú, para poder contrarrestar a los ciberdelincuentes en sus diversas modalidades de penetración en los delitos informáticos.

Esto se debe a la creciente participación en internet, redes sociales y plataformas tecnológicas de la población en general, así también resaltar el crecimiento del uso de dispositivos móviles (laptops, tabletas, celulares), creación de sitios web, plataformas tecnológicas y aplicaciones de los que se puede obtener información. Siendo Internet el recurso más valioso existente en la actualidad, ya que proporciona ingentes cantidades de información sobre diversos tipos de temas y entre los contribuyentes a esta enorme reserva de información tenemos las redes sociales, los blogs, sitios web y plataformas de comunicación (del gobierno, sector empresarial, organismos públicos, entre otros). Las redes sociales a su vez son mucho más que el concepto de conectar con otras personas o compartir fotos, su propósito más importante es el de que la información que maneja es pública, esto posiciona a las plataformas de redes sociales como uno de los mayores y más importantes recursos para la difusión.

Asimismo, debemos señalar que en el Perú, desde el punto de vista del ciberespacio y la ciberseguridad somos vulnerables a las ciber amenazas mundiales dada la debilidad de

nuestros entornos y medios digitales. Ello ha quedado evidenciado con los ataques de hackers así como activistas informáticos (Anonymous), además de la ciberdelincuencia internacional que puede sabotear y robar información de los sistemas digitales nacionales (tanto públicos como privados), los que articuladamente deberían mejorar coordinadamente entre si evitando que se socave la seguridad jurídica del Estado, los derechos fundamentales de los ciudadanos, y que a través del presente trabajo se pone a conocimiento el grave daño que vienen causando.

IX. Recomendaciones

Que, ante el incesante crecimiento estadístico de denuncias en que la ciudadanía peruana viene sufriendo, resulta importante que la Policía Nacional del Perú y las fiscalías especializadas, establezcan a nivel nacional o regional sedes de alta tecnología para la operabilidad procesal en el ámbito de la justicia.

Se debe diseñar un plan de estudios para difundir dentro de las políticas públicas de educación en todos los niveles por parte del Estado, así como a través de los medios de audiencia, que la ciudadanía conozca sobre fortalecimiento de la ciberseguridad digital cuando se tenga acceso a las TICS el conocimiento de los beneficios y riesgos que conlleva el trabajar en el ciberespacio.

Ante la aparición de tecnologías emergentes, los operadores de justicia deben capacitarse constantemente respecto a los avances de las vulnerabilidades de los sistemas informáticos por ser un delito mundial, de fácil operabilidad por los ciberdelincuentes, más aún de encontrarnos ante investigaciones sumamente complejas, sabiendo usar los procedimientos y herramientas en la recolección de la prueba informática.

Referencias Bibliográficas

Acurio del Pino, S. (S/F) *Delitos informáticos: generalidades*. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Budapest (2001) Convenio sobre la ciberdelincuencia. Serie de Tratados Europeos, S/V (23) pp.

Blossiers, J. (2018) *"El delito informático y su incidencia en la empresa bancaria".* (Tesis de maestría) Universidad Nacional Federico Villareal, Lima. https://www.congreso.gob.pe/Docs/comisiones2020/CE-Tribunal-Constitucional/files/postulantes/exp037/tesis.pdf

Chávez, E. (2018) *El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017*. (Tesis de doctorado) Universidad Federico Villareal, Lima. https://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y

Chilcon, M. (2019) *El cibercrimen en el Perú y su incidencia en la seguridad nacional*. (Tesis de doctorado) Centro de altos estudios nacionales, Caen. https://renati.sunedu.gob.pe/bitstream/sunedu/393223/1/CHILCON%20TESIS%20DOCTORADO%202019.pdf

Echevarría, G. (2015) *Los delitos informáticos y el derecho constitucional a la seguridad pública*. (Tesis de pregrado) Universidad Técnica de Ambato, Ecuador. https://repositorio.uta.edu.ec/bitstream/123456789/10034/1/FJCS-DE-802.pdf

García, J. y Peña, D. (S/F) Cibercriminalidad & postmodernidad: La cibercrimonología como respuesta al escenario contemporáneo. *S/R, S/V* (S/N) pp. 1-22 https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20170408_03.pdf

Gestión (03 de diciembre de 2019) BCP reconoce que se filtró información de clientes en un ataque cibernético de 2018. *Gestión.* https://gestion.pe/tu-dinero/bcp-reconoce-que-se-filtro-informacion-de-clientes-en-un-ataque-cibernetico-de-2018-nndc-noticia/

Haarscher, A. (2012) *Delitos informáticos*. (Trabajo final de graduación) Universidad empresarial, siglo 21. https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/10620/Delitos_Informaticos.pdf?sequence=2&isAllowed=y

Huamán, M. (2020) *Los delitos informáticos en Perú y la suscripción del Convenio de Budapest*. (Tesis de pregrado) Universidad Andina de Cusco, Perú. https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Ley 19.223 (1993) *Tipifica figuras penales relativas a la informática*. https://www.bcn.cl/leychile/navegar?idNorma=30590

Ley 1273 (2009) *Modificación de los artículos del Código Penal.* https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ministerio del Interior (2019) *Estudio sobre la cibercriminalidad en España*. http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b

Resolución Ministerial N°622-96-MTC-15.17. (1996) Aprueban procedimientos de inspección y de requerimiento de información relacionados al secreto de las telecomunicaciones y protección de datos. http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_130.pdf

Reyes, C. (2020) *Los delitos informáticos y su influencia en la Integridad personal, distrito de Chorrillos, Lima Metropolitana, 2019*. (Tesis de bachiller) Universidad Peruana de las Américas, Lima. http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/937/T.%20INVESTIGACION-REYES%20VALDIVIA.pdf?sequence=1&isAllowed=y

Ruiz, C. (2016) *"Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos"*. (Tesis de pregrado) Universidad Nacional de Loja, Ecuador.

https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf

STC. (2019) EXP. N° 01189-2019-PHC/TC https://tc.gob.pe/jurisprudencia/2020/01189-2019-HC.pd

Vilca, G. (2018) *Los hackers: "Delito informático frente al código penal peruano"* (Tesis de pregrado) Universidad Nacional "Santiago Antúnez de Mayolo", Huaraz-Ancash. http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2496/T033_47272593_T.pdf?sequence=1&isAllowed=y

Yupanqui, C. (2015) *"Impacto del Decreto Legislativo N° 1182 en el contenido esencial de los derechos a la información y libertad de expresión"* (Tesis de pregrado) Universidad Autónoma del Perú, Lima. https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/462/Carlos%20Yupanqui.pdf?sequence=1&isAllowed=y