FACULTAD DE DERECHO

UNIDAD DE POSGRADO

LAS FISCALÍAS ESPECIALIZADAS EN DELITOS INFORMÁTICOS COMO MECANISMO PARA LA LUCHA CONTRA EL CIBERCRIMEN

PRESENTADA POR

MEDELYN CARBAJAL CAMONES

ASESOR

HUGO HERCULANO PRINCIPE TRUJILLO

TESIS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRA EN DERECHO EN CIENCIAS PENALES

LIMA – PERÚ
2022

UNIDAD DE POSGRADO

LAS FISCALÍAS ESPECIALIZADAS EN DELITOS INFORMÁTICOS COMO MECANISMO PARA LA LUCHA CONTRA EL CIBERCRIMEN

Tesis para Optar el Grado Académico de Maestra en Derecho en Ciencias Penales

Presentado por:

MEDELYN CARBAJAL CAMONES

Asesor:

Mg. Hugo Herculano Principe Trujillo

LIMA, PERÚ
2022

DEDICATORIA

Dedicado a la memoria de mi madre Elizabeth a quien le agradezco su amor y su fe puestos en mí, a mis queridos hijos Michell y Gael fuente de mi inspiración y fortaleza, y a mí por la perseverancia dedicada a esta investigación que hoy concluyo.

INDICE

RESUMEN

El presente estudio analiza cómo la denominada revolución digital que ha facilitado nuestra comunicación y se ha convertido en una herramienta fundamental para el desarrollo laboral y profesional de toda persona, amenaza a su vez el desarrollo social y a la estabilidad de la ley, debido a que la ciberdelincuencia ha mermado la capacidad del Estado de proteger a las personas, dando un enfoque principal a como la creación de fiscalías especializadas en delitos informáticos contrarresta los factores que dificultan la investigación y enjuiciamiento del delito de fraude informático, dentro de los cuales identificamos al anonimato del sujeto activo, la falta de colaboración del denunciante en esclarecer los hechos, la falta de peritos en materia de delitos informáticos, así como la necesidad de contar con fiscales capacitados en investigación criminal de delitos informáticos, entre otros factores, ello en el marco de una situación de emergencia vivida por la pandemia del Covid – 19, la cual generó un incremento exponenecial de operaciones bancarias por internet debido al aislamiento social implementado como medida de contención de la emfermedad.

Asimismo, haremos un breve desarrollo de los delitos informáticos y los aspectos que lo diferencian de los delitos comunes, para posteriormente identificar a la sociedad de riesgo, el perfil criminológico del delincuente cibernético, así como las iniciativas legislativas que nuestro país ha tomado para afrontar la lucha contra el cibercrimen.

Palabras clave: Fiscalías especializadas, factores, dificultades, investigación, fraude informático, Covid – 19.

ABSTRACT

This study analyzes how the so-called digital revolution that has facilitated our communication and has become a fundamental tool for the work and professional development of every person, threatens in turn social development and the stability of the law, due to the fact that the Cybercrime has undermined the State's ability to protect people, focusing primarily on how the creation of specialized prosecutors for computer crimes counteracts the factors that hinder the investigation and prosecution of the crime of computer fraud, among which we identify the anonymity of the active subject, the lack of collaboration of the complainant in clarifying the facts, the lack of experts in the field of computer crimes, as well as the need to have prosecutors trained in criminal investigation of computer crimes, among other factors, within the framework of a emergency situation experienced by the Covid-19 pandemic, the qua l generated an exponential increase in internet banking operations due to the social isolation implemented as a measure to contain the disease.

Likewise, we will make a brief development of computer crimes and the aspects that differentiate them from common crimes, to later identify the risk society, the criminological profile of the cyber criminal, as well as the legislative initiatives that our country has taken to face the fight against cybercrime.

Keywords: Specialized prosecutors, factors, difficulties, investigation, computer fraud, Covid - 19.

NOMBRE DEL TRABAJO

TESIS MEDELYN CARBAJAL CAMONES . docx

AUTOR

MEDELYN CARBAJAL CAMONES

RECUENTO DE PALABRAS

32074 Words

RECUENTO DE CARACTERES

179134 Characters

RECUENTO DE PÁGINAS

146 Pages

TAMAÑO DEL ARCHIVO

3.0MB

FECHA DE ENTREGA

Jan 24, 2022 11:57 AM GMT-5

FECHA DEL INFORME

Jan 24, 2022 12:10 PM GMT-5

20% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 19% Base de datos de Internet
- Base de datos de Crossref
- 8% Base de datos de trabajos entregados
- 3% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 9 palabras)

INTRODUCCIÓN

Respecto a los avances tecnológicos podemos indicar que éstos no sólo han facilitado nuestra comunicación a nivel global, también estos constituyen una herramienta fundamental para el desarrollo educativo, laboral y social; sin embargo, el desarrollo social y la estabilidad de la ley se ven amenazados debido a que la ciberdelincuencia ha mermado la capacidad del Estado de proteger a las personas, ya que pese a los denodados esfuerzos de los distintos operadores de justicia encargados de cumplir con la labor de investigar, denunciar y combatir el cibercrimen, las estadísticas reportan un incremento progresivo en su comisión, siendo que los delitos denunciados que registran mayor incidencia delictiva son el delito de fraude informático, así como las operaciones y transferencia electrónicas y/o de fondos no autorizados.

Recientemente y a consecuencia de la pandemia que se vive por el Covid – 19, el tránsito abrupto al mundo cibernético ha normalizado que a la fecha podamos hablar de trabajo remoto, de clases virtuales y de transacciones masivas las cuales se vienen ejecutando a través de plataformas virtuales, este proceso de adaptación ha puesto a disposición de los delincuentes cibernéticos un volumen de datos sin precedentes, datos de la grande y pequeña empresa, de entes públicos y privados, incluida la información del ciudadano como individuo. Es así que la presente investigación abordará como la creación de fiscalías especializadas en delitos informáticos contrarresta los factores que dificultan la investigación y enjuiciamiento del delito de fraude informático, analizada en el contexto que se vive por la

pandemia por el covid – 19; el presente trabajo de investigación estará compuesto por cuatro capítulos, en el Capítulo I denominado Marco Teórico se abordan las diferentes definiciones que sobre el concepto de delincuencia informática han escritos los autores, se detallan los aspectos positivos y negativos de la aparición de la informática en nuestro desarrollo social, los aspectos diferenciales entre los cibercrímenes y los delitos comunes, lo cual a su vez justifica un tratamiento especial debido a la frecuencia en la comisión de delitos informáticos y al desarrollo de las tecnologías y las herramientas digitales, lo cual demanda a su vez la evolución del orden punitivo, a fin de hacer frente a los nuevos riesgos que aparecen y que amenazan el desarrollo social. Se realiza un desarrollo del marco legal nacional e internacional, dándole un principal enfoque al Convenio de Budapest suscrito por nuestro país, el cual establece una serie de medidas a ser implementados por los países suscribientes, esto es, una serie de reformas legislativas tendientes a garantizar los derechos de los ciudadanos y personas en general en el entorno digital, con la finalidad de garantizar la confianza de las personas durante su interacción con los servicios digitales prestados por entidades públicas o privadas en el territorio nacional. Finalmente se aborda también el despliegue de funciones y objetivos planteados por la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú – DIVINDAT, de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público y del despliegue de actividades desempeñadas por el Centro Nacional de Seguridad Digital.

En el Capítulo II denominado Metodología de la Investigadora, explica el diseño metodológico de su investigación y los aspectos éticos, precisando que se trata de una investigación cualitativa, de forma tal que la investigadora identificará y analizará las dificultades que afronta la investigación y enjuiciamiento del delito de fraude informático.

En el Capítulo III denominado Resultados se ha analizado la entrevista realizada al SO 1 PNP Miguel Antonio Moreno – Agente DIVINDAT, a fin de obtener su opinión respecto a cuáles considera constituyen los factores que dificultan la investigación de los delitos informáticos, haciendo incidencia en el fraude informático. Así también, la investigadora pudo participar del curso Equipo de Respuestas ante incidentes de seguridad digital, certificado por el Centro Nacional de Seguridad Digital, lo cual le ha permitido conocer mejor cual es la perspectiva del Estado frente a las iniciativas de prevención en materia de comisión de delitos informáticos. En el Capítulo IV denominado Discusión la investigadora analiza los resultados de la investigación, señalando por ejemplo que, la creación de una red de fiscalías especializadas en ciberdelincuencia a nivel nacional demanda también la necesidad fortalecer la unidad de peritos en esta materia, los cuales estén provistos de equipos informáticos y softwares forenses necesarios.

El abordaje de los temas antes señalados, me permitirá establecer como es que la creación de fiscalías especializadas en delitos informáticos contrarresta los factores que dificultan la investigación y enjuiciamiento del delito de fraude informático.

CAPÍTULOI

MARCO TEÓRICO

1.1 Antecedentes de la Investigación

Respecto a la temática abordada, debe indicarse que la presente investigación identificará las dificultades que afronta la lucha contra el fraude informático, esto es, los factores que determinan su impunidad y dificultan su persecución.

1.- Antecedentes nacionales:

Montoya Guillén (2018) en su investigación realizada sobre la Regulación expresa del delito informático de clonación de tarjetas - Sede DIVINDAT, 2017, señala que delito de fraude informático tipificado en el artículo 8 de la Ley N° 30096 no es clara, lo cual genera deficiencias al momento de su aplicación por los operadores de justicia, lo cual se debe a que nuestra legislación se ha basado en los estándares del Convenio de Budapest, sin adecuarla a nuestra realidad, y es que en nuestro país no se tiene previsto el delito de clonación de tarjetas de manera expresa.

Agrega que, en nuestra legislación penal para que una conducta pueda ser sancionada debe encontrarse plenamente prevista dentro de nuestro cuerpo normativo, no siendo posible realizar una aplicación por analogía, lo cual implica aplicar consecuencias de una norma establecida para sancionar una conducta prevista por el legislador a otro caso no contemplado en ella, debido a que es semejante a la prevista.

Es así que Montoya Guillén (2018) considera que en referencia al artículo 8 de la Ley N° 30096, existe una regulación general, en la que es posible encajar en múltiples conductas, lo cual vulnera el tipo penal que constituye garantía hacia las personas que pueden verse acusadas por delitos que previamente debe estar tipificados, razón por la cual se hace necesario que en nuestro país se prevea el delito de clonación de tarjetas de manera expresa, detallando la tipificación clara sobre todas las formas que se contemplan con relación a las tarjetas de crédito y débito.

En tanto, Mengoa Valdivia (2021), en su investigación realizada sobre la Punibilidad del comportamiento del *phisher-mule* en referencia al delito de fraude informático en el Perú, señala que la forma general en la que ha sido redactada conforme el artículo 8 de la Ley N° 30096, no permite sancionar el comportamiento del phisher-mule, quien es la persona que brinda su o sus números de cuentas bancarias ya sean nacionales o internacionales, a fin de efectuar las transferencias bancarias que posibilitan el movimiento del dinero sustraído, a cambio de recibir un porcentaje del monto total sustraído; en ese entender, el comportamiento del *phisher-mule* debe ser concebido como aquel brinda ayuda a su cómplice con la receptación del monto sustraído de manera ilícita, quedándose con un pequeño porcentaje de lo sustraído.

Mengoa Valdivia (2021) plantea que la conducta del *phisher-mule* no se logra establecer ni individualizar, por lo que recomienda que esta conducta sea incluida de forma expresa en la legislación sobre los delitos informáticos contra el patrimonio, estableciéndose la diferenciación entre las modalidades de estafa, fraude, sabotaje o hurto informático.

De las tesis antes citadas se advierte que el tipo penal de fraude informático presentan deficiencias en su regulación, por lo cual resulta necesario perfeccionar su redacción y su marco punitivo.

2.- Antecedentes internacionales:

- La tecnología no solo facilita la perpetración de nuevas conductas dañosas, sino que también facilita el ocultamiento de los rastros de las mismas, lo cual aunado al vacío legal relacionado con algunos aspectos de la red, así como el gran desconocimiento en el mundo judicial de la mayoría de aspectos relacionados con las nuevas tecnologías de la información y las comunicaciones, acarrean su impunidad, por lo que surge la necesidad de formación de todos los intervinientes. Así también, se hace necesario que se provea de los recursos suficientes para la investigación de este tipo de conductas, tanto humanos (policiales e institucionales) con la correspondiente cualificación profesional, como técnicos (software y herramientas informáticas), (Rayón Ballesteros & Gómez Hernández, 2014).

- Las posibilidades de ganar dinero en la red, han sido aprovechadas por las mafias de la delincuencia organizada, quienes se han visto favorecidas por este nuevo escenario, el cual ostenta deficiencias legislativas que los benefician y han posibilitado su expansión, para lo cual, comprendido entre sus filas a los hackers, naciendo así un maridaje el maridaje entre la delincuencia organizada y el cibercrimen (Clotet, s.f.).

- Una de las principales características que definen a los delitos informáticos, es la dificultad para ser descubiertos o perseguidos, ya que los sujetos activos actúan premunidos de anonimato y de herramientas capaces de borrar todo rastro de intrusión o la consumación del delito (Acurio del Pino, s.f.).

1.2 Bases Teóricas

1.2.1 Aspectos positivos y negativos de la informática

A) Aspectos positivos. -

La informática en la actualidad constituye una herramienta indispensable en todos los ámbitos de la actividad humana, ya que ha posibilitado la organización y almacenamiento de la información, constituyendo una herramienta fundamental en la administración de empresas privadas y públicas, así como ha hecho posible la realización de investigaciones científicas, de producción e incluso de ocio (Jiménez Herrera, 2017).

Otro aspecto positivo que brinda la informática es que, ha permitido almacenar gran información que se hallaba contenida por años en papeles, logrando con ello liberar gran espacio físico ocupada por esta (Jiménez Herrera, 2017).

La informática no solo ha liberado espacio y ha permitido el almacenamiento de la información, esta herramienta ha posibilitado una interconexión que

rompe el tiempo y el espacio, permitiendo que sea posible ahora realizar trabajo remoto, clases virtuales, recibir atenciones médicas en línea, realizar compras por internet, así como transacciones bancarias, entre otras actividades, sin la necesidad de que su ejecución demande nuestra presencia y es que vamos rumbo hacia la virtualidad, por lo cual surge la necesidad de brindar protección a los usuarios mientras interactúan en el ciberespacio, ya que este nuevo escenario provisto de vacíos legales, se ha convertido en el escenario perfecto para los delincuentes informáticos.

B) Aspectos negativos. -

La delincuencia pronto encontró en la informática un espacio libre de regulación legal, lo cual ha posibilitado la comisión de nuevos delitos a través de su empleo, siendo un rasgo significativo la dificultad para identificar al autor (Jiménez Herrera, 2017).

1.2.1.1 La ciberseguridad en la era de la hiperconectividad y las pandemias

El Banco Interamericano de Desarrollo (2020) expone que la pandemia mundial del COVID-19 ha evidenciado nuestra dependencia de la infraestructura digital, poniendo al descubierto deficiencias estructurales de nuestra sociedad en diferentes sectores como salud, economía, empleo y educación. Iniciada la cuarentena experimentamos una aceleración de la transformación digital, la cual afecto nuestra vida profesional y personal, situación que ha sido aprovechada por la delincuencia. Según el Informe de

Riesgos Globales 2020 del Foro Económico Mundial, el fraude o robo de datos ostenta el mayor índice delictivo.

Debo precisarse que, del universo de delitos informáticos previstos en la Ley N° 30096, modificada por la Ley N° 30171, el fraude informático es el de mayor incidencia delictiva, así se evidencia de la información provista por la División de Investigación de delitos de Alta Tecnología – DIVINDAT, la cual consigna el incremento progresivo de denuncias interpuestas entre el 2013 y el 2020, evidenciándose un crecimiento del 86% a la fecha, siendo la clonación de tarjetas, las compras fraudulentas por internet, las transferencias de fondos no autorizados y los retiros no autorizados, los más recurrentes. La modalidad más usada es el *phishing*, la cual consiste en engañar a los usuarios con páginas falsas como si se tratase de páginas oficiales de bancos o entidades financieras, a fin de que estos registren sus datos personales y, con esa información, las organizaciones criminales realicen transferencias no autorizadas, siendo también posible que sean clonadas páginas de reconocidas tiendas en línea cuyas ofertas tentadoras hacen que los usuarios realicen compras en páginas clonadas, o como aquellos casos en los se ofertan productos a muy bajos precios en Facebook y WhatsApp, para que luego de realizado el pago, los perfiles de los vendedores sean desactivados.

Cabe precisar que, debido a pandemia vivida por el COVID-2019, nos hemos visto forzados a dar un paso abrupto al mundo informático, normalizando una serie de acciones que antes de este suceso nos rehusábamos a desempeñar, como las clases virtuales, el trabajo remoto y las transacciones

bancarias a través de plataformas virtuales, por lo cual, ante este nuevo escenario se necesita brindar mayor seguridad a los usuarios mientras interactúan por el ciberespacio, ya que ello posibilitará su crecimiento personal, profesional y laboral, lo cual significa un crecimiento económico para nuestro país, por lo cual se requiere de iniciativas legislativas tendientes a tipificar las nuevas conductas delictivas que se cometen a través del uso del sistema informático.

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	**14**	**3**	**6**	**4**	**5**	**1**	**2**	**19**	**54**	**0.4%**
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6%**
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4%**
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2%**
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						**3**	**2**	**8**	**13**	**0.1%**
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

Adaptado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.

Fuente de imagen: Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público

Del presente cuadro podemos advertir además cuales son las principales modalidades de comisión del delito de fraude informático.

1.2.1.2 El imperativo estratégico de ciberseguridad empresarial

El Banco Interamericano de Desarrollo (2020) resalta la importancia de comprender que la ciberseguridad constituye parte integral de todo producto tecnológico, se trata pues de encontrar un equilibrio que minimice las pérdidas generadas por el uso de las tecnologías digitales, de la misma forma resulta de gran importancia lograr que todo usuario que haga uso de una plataforma digital y en especial de aquellos líderes empresariales que ofrecen plataformas virtuales a sus usuarios, comprendan acerca de los riesgos cibernéticos existentes y la importancia de contar con productos adecuados que garanticen su seguridad. Cabe señalar, que esta cultura de ciberseguridad también debe generar más conciencia en las pequeñas y grandes empresas, ya que se evidencia un incremento en los ataques dirigidos a éstas.

En este punto debo mencionar que en nuestro país conforme al artículo 9 del Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone como obligaciones de todo Proveedor de servicios digitales el notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, así como implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones o como el gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información; todas estas acciones están destinadas a que los líderes empresariales que ofrecen plataformas virtuales a sus usuarios, comprendan acerca de los

riesgos cibernéticos existentes y la importancia de contar con productos adecuados que garanticen su seguridad.

1.2.2 Definición de delitos informáticos

Como cita Pérez López (2019), la lucha contra la delincuencia informática constituye una tarea difícil debido a su mutabilidad en el tiempo y al surgimiento de nuevas tecnologías, por la cual el autor se sirve de instrumentos informáticos para su comisión.

En nuestro ordenamiento interno también podemos encontrar una definición de delitos informáticos si recurrimos a la Ley 30096 - Ley de delitos informáticos, la cual en su artículo primero los define como las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación.

Para el catedrático Acurio del Pino (s.f.), la definición de delito informático exige que la conducta ilícita consista en operar sobre la base de las funciones del computador, como la utilización de programas para alterar, socavar, destruir, o manipular, cualquier sistema informático, con el fin de causar una lesión o poner en peligro un bien jurídico cualquiera.

Finalmente, Di Piero (2013) concibe al delito informático como todas aquellas conductas en las que las tecnologías de la información y la comunicación

son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos.

Cabe señalar, que de todas las definiciones antes expuestas, esta última es con la que concuerdo, ya que se aproxima a la definición otorgada por la Ley N° 30096, Ley de delitos informáticos, y es que indistintamente se trate de delitos contra datos y sistemas informáticos, contra la indemnidad y libertad sexual, contra la intimidada y el secreto de las comunicaciones, contra el patrimonio o contra la fe pública, la característica principal de este tipo de delitos es que estas son realizadas mediante el uso de tecnologías de la información y la comunicación, con el objetivo de dañar los sistemas y datos informáticos.

1.2.3 La delincuencia informática

1.2.3.1 Sujeto activo

Jiménez Herrera (2017), expone que las personas que cometen delitos informáticos son aquellas que poseen habilidades para el manejo de los sistemas informáticos o aquellas que por su situación laboral se encuentran en lugares estratégicos donde pueden fácilmente acceder a información de carácter sensible. Al respecto, podría mencionarse al trabajador de una entidad financiera la cual almacena información sensible de sus usuarios.

Si bien en un principio se creía que la delincuencia informática estaba vinculada a la idea de un autor eminentemente especializado en materia informática, esa idea ha sido desplazada para poder comprender a cualquier

persona que acceda al uso del medio informático, no siendo exigible que el autor posea un conocimiento especial (Pérez López ,2019). Con el transcurso del tiempo, se ha hecho evidente que las nuevas generaciones tienen una mejor comprensión y dominio de las herramientas tecnológicas y sistemas informáticos, la exigencia de un conocimiento especial del autor implicaría que el delito no pueda ser realizado por cualquier persona que no posea este conocimiento especializado, y no es este el caso de los delitos informáticos, ya que como lo hemos mencionado antes, también es posible que el autor cometa el delito haciendo uso de la información a la que puede acceder por su situación laboral. Así también lo ha entendido Posada Maya (2017), para quien el sujeto activo es aquel sujeto que se conecta virtualmente a los sistemas informáticos para ejecutar actos delictivos dolosos a través del tratamiento de información o servicios a los que puede acceder en la red, precisando que cuando se habla de un sujeto idóneo o capaz para la realización de cibercrímenes, se hace referencia a que éste sea capaz de dominar lógicamente el tratamiento de la información con fines ilícitos.

Asimismo, Acurio del Pino (s.f.) agrega que la calificación del sujeto activo no exige que este tenga una condición especial o conocimientos especializados en informática.

Considero de gran importancia mencionar en este estadio en el que definimos al sujeto activo de los delitos informáticos que, su característica principal es el anonimato, para Posada Maya (2017) esta característica se

hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes y son capaces de borrar todos sus rastros.

1.2.3.2. Sujeto pasivo

Puede recaer en una persona física, en una persona jurídica, el Estado, o incluso una pluralidad de personas, debe precisarse que uno de los factores determinantes en la comisión de delitos informáticos, es la falta de conocimientos en la utilización de la tecnología de los sujetos pasivos, ya que, al no poseer conocimientos básicos en informática se convierten en blanco fácil para ser víctimas de estos delitos (Jiménez Herrera, 2017). A lo expuesto por el autor debo agregar que, no sólo es el escaso conocimiento en las tecnologías de la información por parte de la víctima lo que potencializa su comisión, sino que también lo es la falta de concientización acerca de la ciberseguridad, esto es, de la protección de sistemas, datos, software y hardware que están conectados a Internet, haciendo uso por ejemplo de antivirus originales cuya adquisición se realiza comprando una licencia y no haciendo uso de aquellos descargados del internet de forma gratuita.

En tanto, Acurio del Pino (s.f.) define al sujeto pasivo como el titular del bien jurídico protegido sobre la cual recae la actividad típica del sujeto activo; el autor agrega que a través del sujeto pasivo es posible conocer los diferentes ilícitos que cometen los delincuentes informáticos, información que es utilizada en la prevención de estas acciones.

En este punto, corresponde señalar que, en efecto la víctima constituye una fuente de información valiosa sobre todo en este tipo de delitos mutables en el tiempo, debido al surgimiento de nuevas tecnologías, haciendo posible identificar las distintas modalidades en su comisión, así como los bienes jurídicos afectados, lo cual ha de servir para construir políticas orientadas en la prevención de este tipo de delitos.

Di Piero (2013), respecto al rol protagónico que posee la víctima en el ciberespacio, señala que su accionar no implica que la sociedad deba cargar con los costos de asumir comportamientos imprudentes o inclusos dolosos de la víctima, y que debe ser esta quien asuma la obligación de adoptar medidas de protección eficaces y efectivas, debiendo limitarse la intervención del Derecho penal sólo a supuestos en que no es posible la autoprotección.

En este punto y respecto al rol de la víctima de fraude informático, debo precisar que la entrevista realizada al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, me permite concluir que el escaso conocimiento en el uso de los sistemas informáticos de las víctimas no está asociado necesariamente a sus escasos recursos económicos, sino más bien se trata de la falta de una cultura que en general nos afecta a todos los ciudadanos con mayor y menor intensidad, sobre el uso adecuado de los sistemas informáticos, ya que en nuestro país no existen oportunidades para acceder a una educación en ciberseguridad y el uso responsable de la

tecnología, ya sea en universidades públicas o privadas. Asimismo, debe resaltarse que una de las dificultades de la investigación en este tipo de delitos, es generada por la falta de colaboración de la víctima por esclarecer los hechos, a su vez, el Estado no se ha preocupado por promover una cultura de ciberseguridad en el uso seguro de dispositivos conectados a Internet, tampoco se está priorizando la formación de un capital humano que haga frente a la delincuencia informática, situación que debe tenerse presente en las futuras políticas adoptadas por el gobierno entrante.

1.2.3.3 Bien jurídico protegido en los delitos informáticos

Pérez López (2019), afirma que los delitos informáticos tienen naturaleza pluriofensiva, esto es, afectan diferentes bienes jurídicos de manera conjunta o concatenada; siendo posible que se afecte la información concebida de manera general, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos, así como a otros bienes jurídicos tales como, la indemnidad sexual, la intimidad, el patrimonio, la intimidad, la confidencialidad de los datos seguridad o fiabilidad del tráfico jurídico, etc.

En tanto, para Posada Maya (2017) lo fundamental a resaltar en cuanto al bien jurídico de protección en este tipo de delitos, es que estos son dinámicos, ello en alusión a su mutabilidad en el tiempo y al surgimiento de nuevas tecnologías, por lo cual su protección exige cambios en las estructuras formales y materiales de tipicidad.

Para Acurio del Pino (s.f.) el bien jurídico protegido en este tipo de delitos es en general la información, la cual puede ser considerada como un valor económico, que atañe a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

En mi posición personal, considero que el bien jurídico protegido en los delitos informáticos es pluriofensivo ya que se afecta tanto los sistemas y datos informáticos, así como otros bienes jurídicos de relevancia penal como lo son la indemnidad sexual, la intimidad, el patrimonio, la intimidad, la confidencialidad de los datos seguridad o fiabilidad del tráfico jurídico, etc.

1.2.4. Aspectos diferenciales entre los cibercrímenes y los delitos comunes

Rayón Ballesteros y Gómez Hernández (2014), afirma que el cibercrimen constituye una conducta delictiva que no puede ser subsumida en otra conducta punible, como el hurto o la estafa, ya que en los delitos informáticos no media el engaño directo a una persona, ni existe un apoderamiento de bienes físicos a través del engaño a la víctima, y es que en su configuración existe una manipulación del sistema informático, lo cual define las características propias de estos delitos. Es así que podemos identificar cuatro aspectos diferenciales entre los cibercrímenes y los delitos comunes, que son los siguientes:

1. El bien jurídico

A diferencia de los delitos comunes, los delitos informáticos tienen por objeto la protección los sistemas y datos informáticos, siendo que de modo

secundario protegen otra clase de bienes jurídicos como la indemnidad sexual, la intimidad, el patrimonio, la intimidad, la confidencialidad de los datos seguridad o fiabilidad del tráfico jurídico, etc.

2. La acción o el nacimiento de la “ciberacción”

Mientras en los delitos comunes se valoran jurídicamente conductas humanas realizadas en el plano físico, en los delitos informáticos las acciones valoradas son realizadas en el ciberespacio por sistemas dominados por hombres, cuyos resultados no trascienden al mundo físico (Posada Maya, s.f.).

3. Los sujetos activos del cibercrimen

Posada Maya (s.f.) señala que en los delitos tradicionales existe una relación entre el sujeto activo y el sujeto pasivo, determinada por una acción u omisión que genera el delito, en tanto, en los delitos informáticos se requiere además que el autor desarrolle la conducta típica en calidad de usuario de un sistema informático, esto es, mediante una conexión virtual.

4. El resultado

Mientras los delitos comunes expresan un resultado en el mundo exterior o físico, en los ciberdelitos los resultados tales como la destrucción, borrado, alteración y supresión de datos informáticos o de sistemas de tratamiento de información, expresan un resultado inmaterial en el ciberespacio.

1.2.5 Perfil criminológico del delincuente informático

> Son aquellas personas que hacen uso de su inteligencia superior para desarrollar comportamientos ilegales, son poco sociables, actúan preferentemente en la noche, desarrollan sus actividades en ciudades grandes, odian las burocracias, son desaliñados, intensos, abstraídos, son curiosos y tienen una facilidad para las abstracciones intelectuales, les gusta la novedad y son atraídos por lo intelectual, son a veces egocéntricos y casi nunca están conformes con lo que hacen, difícilmente logran satisfacerse con lo que saben, siempre tratan de encontrar algo novedoso y no les importa el tiempo que puedan pasar navegando en la internet (Ramírez Luna, s.f.).

1.2.6 Sociedad del riesgo e intervención penal

1.2.6.1 Definición de Sociedad del Riesgo

> Jiménez Diaz (2014) señala que la sociedad del riesgo surge como consecuencia de los riesgos generados en la economía empresarial, caracterizada por su complejidad y transnacionalidad, agrega que los avances científicos y la globalización favorecen la aparición de nuevos peligros. El citado autor afirma que el orden punitivo, debe evolucionar y hacer frente, a los nuevos riesgos que vayan apareciendo, sin llegar a un intervencionismo desmedido del derecho penal.

En atención a lo expuesto, debe precisarse que el sector empresarial casi en su totalidad ofrece plataformas virtuales a sus usuarios, lo cual se masificó debido a la pandemia vivida por el Covid-19 y ello significa que existe una gran cantidad de información en las redes que puede ser sujeto de una afectación, ya en otros países como los Estados Unidos de Norteamérica se han

presentado otras formas de afectación patrimonial como el denominado *ransomware*, el cual constituye un programa malicioso que bloquea los archivos o dispositivos del usuario, a fin de solicitar un denominado pago por rescate de información, lo cual restaurar el acceso a la información. Todo esto, constituye una alarma tanto para nuestras autoridades como para todo proveedor de un servicio digital, respecto de los riesgos cibernéticos existentes y la importancia de advertir los vacíos legales, así como de contar con productos adecuados que garanticen su seguridad.

1.2.6.2 Características

Jiménez Diaz (2014) expone que, los aspectos que definen a la sociedad del riesgo son: “a) El incremento de los peligros actuales en relación con los de otros períodos y los problemas de imputación y atribución de responsabilidad a los autores; b) La complejidad organizativa de las relaciones de responsabilidad. c) El tercero y último, es la creciente sensación de inseguridad subjetiva ante los nuevos peligros, que existe incluso cuando dichos peligros no sean reales”.

1.2.6.3 Fenómeno socio jurídico de la delincuencia

Ramos Suyo, Juan A. (2014) expone que, para la criminología, la delincuencia es un fenómeno de la vida social, porque se produce en su seno y porque se compone de actos ilícitos que los individuos cometen contra otros miembros de la sociedad.

1.2.6.4 La llamada delincuencia latente

Ramos Suyo (2014) manifiesta su preocupación respecto del poco estudio que hay sobre la delincuencia latente, ya que ésta siempre es superior a la descubierta, en la que se incrementan las infracciones cometidas por los menores de edad, en este tipo de delitos, así como la inmersión de la criminalidad organizada la que se ha beneficiado de los avances tecnológicos y la libertad de los mercados (Ramos Suyo, 2014).

En este extremo debo mencionar que los datos estadísticos con los cuales cuentan la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, así como la División de Investigación de Alta Tecnología, respecto de las denuncias por delito de fraude informático realizados entre el 2013 y el 2020, estos representarían sólo un 30% de la cifra real, ya que existe una alta cifra oculta que no es de conocimiento de los operadores de justicia, debido a que los agraviados no denuncian estos hechos, muchas veces promovidos por la postura que asumen las entidades del sistema financiero, las cuales al tomar conocimiento del reclamo formulado por sus clientes los cuales han sido víctimas de fraude informático, en sus diversas modalidades, analizado el reclamo devuelven las sumas sustraídas, a fin de no dañar su imagen de transacciones seguras, lo cual genera una cifra oculta; otra de las razones del surgimiento de la denominada cifra oculta es la propia actitud de la víctima, la cual denunciado los hechos no colabora con la investigación, pero principalmente ello se debe a la dificultad que existe para identificar al autor delictivo.

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

Fuente de imagen: Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público

1.2.7 La política criminal en la globalización

Ramos Suyo (2014) expone que el Derecho constituye una disciplina a fin al desarrollo de la idea global, por lo que derecho penal no puede relegarse al funcionamiento de tribunales especiales, sino que se debe buscar salidas globales a algunos de estos problemas que conlleven a una política criminal también global y por ende a la globalización del Derecho Penal.

Al respecto, Acurio del Pino (s.f.) señala que las acciones esenciales para la implementación de una política criminal global requieren: a) Armonización de leyes penales sustantivas; b) Estandarización de procesos penales; y c) Cooperación internacional.

Ramos Suyo (2014) señal que la existencia de una política criminal se encuentra orientada a las siguientes situaciones: Una de persecución y otra de protección o tutela, la cual tiene por objetivo proteger a la víctima, y no utilizarla.

1.2.8 Análisis del Convenio sobre la Ciberdelincuencia, Budapest – 2001

1. Sobre la implementación

Guerrero Argote (2018) el autor señala que el Convenio de Budapest, firmado el 23 de noviembre de 2001, y cuya entrada en vigor se produjo el 1 de julio de 2004, tiene tres objetivos declarados: La creación de un marco común de derecho penal sustantivo, la estandarización de procesos penales y la cooperación internacional.

Cabe agregar que, en nuestro país mediante Resolución Legislativa N.º 30913, el Congreso de la República aprobó la adhesión del Perú al Convenio sobre Ciberseguridad, también conocido como Convenio de Budapest, el 13 de febrero de 2019.

2. Marco común de Derecho Penal sustantivo

Acurio del Pino(s.f.) afirma la necesidad de contar una herramienta común para procesar los delitos informáticos, la cual posibilite la aplicación de una ley común de carácter supranacional, que permita el intercambio de información y pruebas, de cooperación internacional de los países miembros, haciendo frente a la delincuencia informática organizada.

En ese sentido, Guerrero Argote (2018) expone que el Convenio de Budapest incorpora en su primer capítulo una serie de artículos destinados a crear un marco común de derecho penal sustantivo, armonizando la legislación relativa al cibercrimen y estableciendo un régimen de cooperación y asistencia internacional en materias como la extradición o el

establecimiento de un equipo experto en redes que funcione las 24 horas. El Convenio de Budapest propone principalmente cuatro categorías: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, delitos informáticos, delitos relacionados con el contenido y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Debe precisarse también que el Convenio de Budapest ha sido ratificado por 60 Estados, entre los cuales se hallan Estados miembros de la Unión Europea, así como por países no europeos, entre ellos Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina, Colombia.

En el Perú, el producto final de dichas discusiones ha sido la Ley N° 30096 publicada en 2013, en la cual no se había cuidado la redacción y se castigaba acciones inofensivas, errores que fueron subsanados con las modificaciones introducidas por la Ley N° 30171 publicada en 2014 que mejoró la redacción, eliminando disposiciones problemáticas (Guerrero Argote, 2018).

El siguiente cuadro elaborado nos permite comparar las definiciones del Convenio de Budapest principalmente con los delitos creados por la Ley N° 30096 y sus posteriores modificaciones:

Ley N° 30096	Ley N° 30171	Convenio de Budapest
Art. 8 LDI.- El que, a través de las	Art. 8 LDI.- El que deliberada e	Art. 8.- Las Partes adoptarán las medidas

tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.	ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.	legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Cuadro elaborado por Elías Puelles (2014).

3. Estandarización de procesos penales

Guerrero Argote (2018) expone que por el Convenio de Budapest se establecen una serie de disposiciones comunes destinadas a hacer posible

la persecución penal, las cuales están referidas a adaptar la legislación en materia de extradición; así también propone un modelo de cooperación internacional; en nuestro país por ejemplo, contamos con la División de Investigaciones de Delitos de Alta Tecnología y la Interpol Perú, para coadyuvar en la red de persecución internacional conformada por estados miembros adscritos al Convenio de Budapest.

4. Acciones esenciales para una implementación exitosa

Guerrero Argote (2018) resalta la importancia de contar con reformas legislativas, que consideren la participación de actores no estatales que viabilicen estas propuestas. En tanto Acurio del Pino (s.f.) señala que las acciones esenciales para una implementación exitosa son: a) Armonización de leyes penales sustantivas; b) Estandarización de procesos penales; y c) Cooperación internacional.

5. Apoyo en organismos multilaterales

Guerrero Argote (2018) señala que en los procesos de reformas legislativa tendientes a adecuar la legislación interna de los países a las disposiciones del Convenio de Budapest, pueden hacerse recibiendo asesoría externa de la Oficina del Programa de Cibercriminalidad del 19 Consejo de Europa y de la Gerencia de Programa de Seguridad Cibernética de la Organización de Estados Americanos.

6. Creación de un plan de ciberseguridad

Guerrero Argote (2018) expone que en nuestro país aún no cuenta con un Plan Nacional de Ciberseguridad, y resalta la necesidad de que en su implementación se cuente con la participación del Estado, así como la del sector privado, la sociedad civil organizada y la ciudadanía, a fin de erradicar los delitos informáticos. Agrega que la ratificación del Convenio de Budapest por un Estado parte, conlleva una reforma legislativa en esta materia y el fortalecimiento de la cooperación internacional.

7. Actores y Roles

Guerrero Argote (2018) expone que, al alinearse el Perú con las prácticas establecidas en el Convenio de Budapest, éste experimentará un crecimiento en el mercado interno de la seguridad informática, así como en la oferta educativa relacionada a las Tecnologías de Información y Comunicación.

8. La Convención de Budapest como iniciativa internacional

Asociación por los derechos civiles (2018), señala que la iniciativa de regulación por parte de organismos internacionales, surge como consecuencia de advertirse el carácter transnacional de los delitos informáticos, esto es, los autores del delito operan en diferentes países, o porque las víctimas están en un país distinto, e incluso porque la prueba está alojada en servidores ubicados en países distintos al país en el que se sigue la investigación, por lo cual y a fin de viabilizar la recolección de evidencia que haga posible la sanción en este tipo de delitos, surgió la iniciativa de regulación por parte de organismos internacionales, siendo la más

importante el "Convenio de Budapest", el cual entró en vigor en 2004 en Europa y a la cual nuestro país se adhirió el 13 de febrero de 2019.

9. Cooperación internacional

En el Tercer Capítulo, el Convenio de Budapest establece disposiciones comunes para hacer viable la cooperación entre sus miembros, las cuales están referidos a la adaptación de la legislación en materia de extradición, a efectos de que esta sea viable siempre que se cometa un delito informático y los países implicados lo hayan tipificado en su norma penal, en el NCPP peruano la legislación referente a la extradición se encuentra plasmada en los artículos 513 al 527; la asistencia mutua, a efectos de ampliar la eficacia de la persecución penal, a través de actos de cooperación basados en la designación de puntos de contacto para atender solicitudes de emergencia, en el NCPP peruano la legislación referente a la asistencia mutua judicial, se encuentra regulada en los artículos del 508 al 512 y 528 al 539; y la creación de un aparato de respuesta a emergencias, la cual comprende la construcción de una red compuesta por los miembros del Convenio. Una de ellas es el contacto de Interpol en donde está incluida la Policía Nacional (Guerrero Argote 2018).

1.2.9 La respuesta del Estado peruano frente a los delitos informáticos

1.2.9.1 La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú – DIVINDAT

Elías Puelles (2014) indica que en un inicio la lucha contra los delitos informáticos tipificados en el Código Penal, estaban a cargo de las divisiones

policiales encargadas de la investigación de otros delitos, y es en despliegue de las actividades de investigación que consideran necesario contar con una División capacitada en la investigación de delitos informáticos, razón por la cual el 08 de agosto de 2005 se creó la División de Investigación de Delitos de Alta Tecnología – DIVINDAT, la cual según la opinión del autor carece de un personal debidamente capacitado, el cual además no ostenta una la logística que les permita realizar patrullajes a través del internet las 24 horas, por la cual se requiere de una reforma integral en la Unidad Especializada que tiene como labor la investigación de estos ilícitos.

Cabe señalar, que como parte del proceso de investigación que me llevó a identificar los obstáculos que enfrenta la lucha contra el fraude informático, en mi visita a la División de Investigación de Alta Tecnología y de la entrevista al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, pude conocer que los cursos de capacitación en materia de delitos informáticos que reciben los agentes DIVINDAT son posibles debidos a los convenios internacionales de los cuales nuestro país es parte, pero que principalmente estos son organizados por la Asociación de Bancos del Perú, siendo una de las limitaciones, el reducido número de agentes que podían participar de estos, siendo un máximo de tres o cuatro agentes, los cuales a fin de compartir los conocimientos adquiridos, organizaban cursos que ellos mismos dictaban al interior de su institución a otros agentes que formaban parte de esta división de investigación. A la opinión del SO1 PNP Miguel Antonio Torres Moreno, la capacitación en la investigación de delitos informáticos no es una causa principal que dificulte la investigación de los

delitos de fraude informático, pues para él la principal razón, es la dificultad que se tiene para identificar al autor delictivo, quien se encuentra premunido de un anonimato, lo cual a su entender podría remediarse con mecanismos de cooperación con las entidades del sistema financiero, las cuales podrían proveer información necesaria para identificar al autor delictivo, y es que justamente la gran dificultad en su trabajo de investigación se presenta por la falta de colaboración de las entidades financieras involucradas, las cuales al no proveer de la información de manera inmediata, los casos denunciados se archivan.

1.2.9.2 Unidad Fiscal Especializada en ciberdelincuencia del Ministerio Público.

La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, fue creada el 30 de diciembre de 2020, a través de la Resolución de la Fiscalía de la Nación N°1503-2020- MP-FN. Su creación se dio como respuesta al incremento de la ciberdelincuencia en el país. Esta Unidad Fiscal Especializada, tiene entre sus principales funciones el acompañamiento técnico a los fiscales en la realización de la investigación en los delitos de la Ley N°30096, Ley de delitos informáticos, así como establecer lineamientos que orienten las investigaciones y la unificación de criterios en procedimientos y métodos de investigación en materia de ciberdelincuencia. Se encarga también de promover la capacitación permanente con la Escuela del Ministerio Público para todos los fiscales y peritos de la especialidad.

En este extremo debe precisarse que la Escuela del Ministerio Público, ha organizado 05 actividades académicas, sobre temas relacionados a la

ciberdelincuencia y los delitos informáticos, conforme se desprende del siguiente cuadro, provisto por la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, según se observa:

Tabla 15. Actividades académicas desarrolladas por el Ministerio Público. 2018–2020

AÑO	ACTIVIDAD ACADÉMICA	MODALIDAD	DURACIÓN	CO-ORGANIZADOR
2018	Taller: Delitos informáticos	Presencial (Lima)	10 horas académicas	Escuela MP
2018	Curso: Delitos Informáticos	Virtual	120 horas académicas	Escuela MP
2020	Taller de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos - Cybercrimen	Presencial (Lima)	50 horas académicas	American Bar Association Rule of Law Initiative ABA ROLI PERÚ
2020	Curso de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos - Cybercrime	Virtual	Del 30.03 al 27.05 de 2020	American Bar Association Rule of Law Initiative ABA ROLI PERÚ
2020	Ciberdelincuencia, Delitos Tecnológicos	Virtual	36 horas académicas	Unión Europea

Fuente de imagen: Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público

Cabe señalar que, la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público también desarrolla herramientas de gestión que permiten orientar a los fiscales en su labor. Tiene a su vez, potestad de articular con organismos estatales y privados de Perú y a nivel internacional de manera que pueda acceder a información y a colaboración para el desarrollo de las investigaciones, con el fin de dar una respuesta eficaz y oportuna a este tipo de delitos que suponen un desafío para el Sistema de Justicia por su uso intensivo de tecnologías de la información y las comunicaciones.

1.2.9.3 Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional – PECERT

El PECERT (s.f) se desempeña como el Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional de la Administración Pública Peruana, creado por RM 360-2009-PCM el 19 de agosto del 2009, es el encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los desafíos informáticos y coordinar la defensa ante los Ciberataques, con el fin de proveer a la Nación de una postura segura en el Ámbito de la Seguridad Informática, realiza un trabajo conjunto con diversas entidades públicas como el Ministerio de Defensa, Marina de Guerra, Fuerza Aérea, Ministerio del Interior, la PNP con la DIVINDAT, Interpol Perú, Migraciones, Poder Judicial, RENIEC, OEA, empresas de telecomunicaciones, empresas proveedoras de TI.

El Banco Interamericano de Desarrollo (2020) precisa que el PECERT es miembro de la red del Equipo de Respuesta ante Incidentes de Seguridad de la Información-CSIRT Américas, el cual tiene por objetivo coordinar la prevención, el tratamiento y la respuesta a incidentes de seguridad cibernética de instituciones del sector público, asimismo se encuentra a cargo de la elaboración de estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad de la información del Estado.

La Organización de los Estados Americanos (2018) señala que debe entenderse por incidente de seguridad digital al total de ataques exitosos que sufrió la institución durante el mismo periodo de tiempo, con la finalidad de

analizar los resultados y gestionar respuestas ante incidentes de seguridad digital.

1.2.9.3.1 Objetivos

Conforme se desprende de la página institucional de la Presidencia del Consejo de Ministros, el PECERT tiene por objetivos (PECERT, s.f):

- Promover la coordinación entre las entidades del sector público y privado en materia de prevención, detección, detención, manejo y recopilación de información.
- Desarrolla soluciones para incidentes de seguridad.
- Propone normas destinadas a incrementar los niveles de seguridad en las Tecnologías Informáticas.
- Brindar asesoría técnica ante incidentes de seguridad informática, tanto para el sector público como el privado.
- Centralizar los reportes sobre incidentes de seguridad ocurridos en redes del sector público y privado, facilitando el intercambio de la información para afrontarlos, difundiendo información útil para incrementar los niveles de seguridad de las redes del Perú.

1.2.9.3.2 Alerta Integrada de seguridad digital del PECERT

En cuanto al desempeño desplegado por el PECERT respecto a la emisión de alertas integradas de seguridad, debe entenderse que estas corresponden a un análisis técnico y periódico que concluye con una serie de recomendaciones y que es realizado por el Comando Conjunto de las

Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, con el objetivo de informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población (PECERT, s.f).

1.2.9.4 Ley N° 30618. Ley que modifica el Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, a fin de regular la seguridad digital

Del contenido de la presente ley debemos destacar que nos otorga una definición del Sistema de Inteligencia Nacional - SINA, definiéndola como un conjunto de principios, normas, procedimientos, técnicas, instrumentos, organismos y órganos del Estado, funcionalmente vinculados, que bajo la dirección y coordinación de la Dirección Nacional de Inteligencia - DINI como ente rector de Inteligencia Militar e Inteligencia Policial, realiza actividades de inteligencia en las áreas de su responsabilidad, como lo es producir un conocimiento útil y realizar una serie de actividades destinadas a alcanzar la seguridad digital en materia de seguridad nacional.

1.2.9.5 Decreto Legislativo N° 1412. Decreto Legislativo que aprueba la Ley de gobierno digital

Concibe al gobierno digital como aquel que comprende el uso estratégico de las tecnologías digitales y datos en la Administración Pública, cuyo objetivo es el de asegurar el respeto de los derechos de los ciudadanos y personas en general en el entorno digital, a través de la colaboración entre las entidades de la Administración Pública y la promoción de investigación y desarrollo en la implementación de tecnologías digitales.

1.2.9.6 Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento

En el camino a generar confianza digital, el presente decreto establece una serie de medidas tendientes a garantizar la confianza de las personas durante su interacción con los servicios digitales prestados por entidades públicas o privadas en el territorio nacional, para lo cual se dispuso la creación del Centro Nacional de Seguridad Digital, a cargo de la Presidencia del Consejo de Ministros, la cual tienen por objetivo el realizar coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza**;** asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos. Asu vez, se crea el Registro Nacional de Incidentes de Seguridad Digital el cual tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de

servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

Resulta importante resaltar que esta norma, en su artículo noveno detalla cuales serían las obligaciones de todo proveedor de servicios digitales, esto es, cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional.

Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:

a) Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.

b) Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.

c) Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de

riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.

e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.

f) Mantener una infraestructura segura, escalable e interoperable.

Morachimo (2020) advierte que las entidades públicas no están preparadas para recibir reportes de ciberseguridad, ya que lo toman como críticas directas a su trabajo y tampoco reconocen cuando se equivocan, lo cual los condena a seguir repitiendo los mismos errores en perjuicio de todos los ciudadanos.

De la lectura de los objetivos desplegados por Centro Nacional de Seguridad Digital podría surgir la interrogante de si su creación conlleva al desplazamiento del PECERT en sus funciones, pero esto no es así, ya que el CNDS está conformado por sub áreas dentro de las cuales se encuentran: Gestión de Alertas Digitales, Gestión de incidentes, Gestión de Seguridad de la información, Gestión de riesgos digitales, Observatorio Nacional de Seguridad Digital, Equipo de respuestas ante incidentes de seguridad digital, Análisis forense digital, Gestión de seguridad de comunicaciones y Gestión de infraestructura, debiendo precisarse que el Equipo de respuestas ante incidentes de seguridad digital ahora asume el rol del antes denominado PECERT pero con el adicional de que ahora se ha formado una red nacional, internacional y sectorial de CSIRT dentro de la cual están comprendidos otros países como Chile, Colombia, México, entre otros, como países

miembros de la Alianza del Pacífico, parte del marco de acuerdo del pacifico, pero también integrado por otros países de la OEA

1.2.9.7 Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

En el capítulo tercero referido al Equipo de Respuestas ante incidentes de seguridad digital, establece en su artículo 105 lo siguiente:

> Artículo 105. Obligaciones de las entidades en Seguridad Digital
>
> Las entidades públicas tienen, como mínimo, las siguientes obligaciones:
>
> a) Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
>
> b) Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital.
>
> c) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
>
> d) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad y red de confianza.
>
> e) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
>
> f) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.

g) Requerir a sus proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.

Asimismo, precisa en el artículo 107, que la comunicación de un incidente de seguridad digital se realiza en un plazo máximo de 48 horas, a partir de la toma de conocimiento de la brecha de seguridad.

1.2.9.8 Legislación Nacional y análisis de los tipos penales contenidos en la Ley de Delitos Informáticos en el Perú – (Leyes 30096-30171)

D) El fraude informático como delito contra el patrimonio (art. 8 de la Ley N° 30096)

El artículo 8 de la Ley de Delitos Informáticos - Ley N° 30096, señala lo siguiente:

> "El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

a) Bien jurídico protegido

Pérez López (2019) expone que el bien jurídico protegido es el patrimonio, ello debido al derecho de propiedad que tiene el sujeto pasivo respecto a su base de datos informáticos y al adecuado funcionamiento de un sistema informático.

En tanto, Jiménez Herrera (2017) señala que el provecho ilícito para sí o para otro, hace referencia a un acto voluntario que causa perjuicio patrimonial a otra persona, a través de la introducción, alteración o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático. A ello agrega que la rúbrica de la ley delitos informáticos se deprende: “Delitos contra el Patrimonio”, por lo cual el bien jurídico protegido sería el patrimonio.

b) Tipicidad objetiva

Pérez López (2019) señala que consiste en la afectación del funcionamiento del sistema informático o de transmisión de datos, ya sea introduciendo datos falsos o suprimiendo datos verdaderos con fines fraudulentos, a fin de obtener una ventaja económica. Cabe señalar que, se diferencia de la estafa tradicional porque no exige que la defraudación vaya precedida de un desplazamiento patrimonial provocado por un error humano, y es que, si bien el fraude informático constituye una modalidad de engaño a través de la red, esta no está sujeta a los requisitos básicos exigidos para la estafa, ya que el

apoderamiento de un bien se produce como consecuencia de la manipulación informática que genera la transferencia patrimonial.

Las nuevas tecnologías han propiciado el nacimiento de una nueva modalidad de delito de estafa en el que no resulta necesaria la colaboración de la víctima, sino que basta con alterar o manipular los sistemas informáticos para conseguir el mismo resultado. A modo de conclusión, debe precisarse que el tipo penal exige la necesaria manipulación de un sistema informático con el propósito de obtener un ilegítimo beneficio económico (Pérez López, 2019).

En tanto, Jiménez Herrera (2017) expone que a través de la manipulación de datos se produce una doble afectación, la económica y otra referida al funcionamiento de los sistemas informáticos.

c) Tipicidad subjetiva

Son de comisión dolosa, no siendo posible su comisión culposa o imprudente.

d) Grados de desarrollo del delito

Pérez López, Jorge (2019) expone que el delito de fraude informático se consuma con la afectación de datos informáticos o el funcionamiento de un sistema informático de tercero, motivado por el ánimo de lucro.

1.2.10 Principales modalidades de Fraude informático

A continuación, se detalla el cuadro estadístico provisto por la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, del cual se evidencian las modalidades de fraude informático más recurrentes. Debe precisarse que las modalidades mencionadas a continuación, aunque no se encuentran tipificadas con los nombres de “Clonación de tarjetas”, “Compras fraudulentas por internet” y Operaciones y transferencia electrónicas y/o de fondos no autorizados” en la Ley N° 30096 Ley de delitos informáticos, estos han podido ser identificados como consecuencia de las actividades identificadas a través de las denuncias impuestas por los agraviados.

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

Fuente de imagen: Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público

1.2.10.1 Clonación de tarjeta

El *skimming* es la técnica por la cual los delincuentes colocan una lectora en los cajeros automáticos, a efectos de obtener información de los clientes bancarios que realicen acciones en los mencionados cajeros automáticos, estos dispositivos son imperceptibles debido a su sofisticación, la información recopilada es transferida a un ordenador PC para introducirlo en

una tarjeta en blanco y así poder ser usadas como medios de pagos en diversos servicios y realizar compras con el dinero de la víctima.

1.2.10.2 Compras fraudulentas por internet

Esta modalidad inicia con la publicación de una oferta de determinado producto en un sitio web o en redes sociales, ya sea Facebook y WhatsApp, para que, con posterioridad a la realización del pago en línea o transferencia a cuentas personales, los perfiles de los delincuentes son desactivados.

1.2.10.3 Operaciones y transferencias electrónicas y/o de fondos no autorizados

Jiménez Herrera (2017) señala al respecto que, consiste en la apropiación de una suma de dinero, a través de la introducción de instrucciones a un programa para que haga efectiva la remisión para apropiarse de sumas de dinero.

Esta modalidad inicia con la técnica denominada *phishing*, por la cual los ciberdelincuentes engañan a los usuarios con páginas falsas que simulan ser los sitios web de entidades financieras, siendo que al registrar las víctimas sus datos personales y datos bancarios, con esta información las organizaciones criminales realizan operaciones y depósitos sin autorización.

De lo expuesto se concluye que, el phishing constituye un ataque por el cual se envían una serie de correos electrónicos, mensajes a redes sociales, SMS/MMS, llamadas telefónicas o se produce una infección de malware, este último debe ser entendido como un programa malicioso que puede

robar, cifrar, borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin el consentimiento o incluso sin el conocimiento del receptor, para que este revele información comprometedora como sus datos personales, información financiera y credenciales de acceso.

El tipo de información que roban son: Direcciones de correo, número de documento de identidad, datos de localización y contacto, número de tarjeta de crédito, números de cuentas, redes sociales o cuentas de correo. Los principales medios de propagación son: correos electrónicos, redes sociales, SMS/MMS, llamadas telefónicas o infección de malware, por ello es recomendable evitar enlaces sospechosos, además una forma sencilla de advertir que una dirección electrónica no es segura, puede identificarse a través de la descripción de la URL, la cual debe iniciar con http:// o https://, así también, se podrá visualizar la imagen de un candado al lado izquierdo de la URL, otras recomendaciones son: jamás hacer clic en un link sospechoso, no facilitar datos por correo electrónico ya que los Bancos jamás solicitan datos por dicho medio, no hacer clic en enlaces, uno mismo debe escribir la dirección, revisar tu estado de cuenta de forma frecuente, mantener actualizado tu software y usar antivirus.

1.2.10.4 Tesis Nacionales en referencia al fraude informático.

Montoya Guillén (2018) en su investigación realizada sobre la Regulación expresa del delito informático de clonación de tarjetas - Sede DIVINDAT, 2017, señala que delito de fraude informático tipificado en el artículo 8 de la Ley N° 30096 no es clara, lo cual genera deficiencias al momento de su

aplicación por los operadores de justicia, lo cual se debe a que nuestra legislación se ha basado en los estándares del Convenio de Budapest, sin adecuarla a nuestra realidad, y es que en nuestro país no se tiene previsto el delito de clonación de tarjetas de manera expresa.

Agrega que, en nuestra legislación penal para que una conducta pueda ser sancionada debe encontrarse plenamente prevista dentro de nuestro cuerpo normativo, no siendo posible realizar una aplicación por analogía, lo cual implica aplicar consecuencias de una norma establecida para sancionar una conducta prevista por el legislador a otro caso no contemplado en ella, debido a que es semejante a la prevista.

Es así que Montoya Guillén (2018) considera que en referencia al artículo 8 de la Ley N° 30096, existe una regulación general, en la que es posible encajar en múltiples conductas, lo cual vulnera el tipo penal que constituye garantía hacia las personas que pueden verse acusadas por delitos que previamente debe estar tipificados, razón por la cual se hace necesario que en nuestro país se prevea el delito de clonación de tarjetas de manera expresa, detallando la tipificación clara sobre todas las formas que se contemplan con relación a las tarjetas de crédito y débito.

En tanto, Mengoa Valdivia (2021), en su investigación realizada sobre la Punibilidad del comportamiento del *phisher-mule* en referencia al delito de fraude informático en el Perú, señala que la forma general en la que ha sido redactada conforme el artículo 8 de la Ley N° 30096, no permite sancionar el comportamiento del phisher-mule, quien es la persona que brinda su o sus números de cuentas bancarias ya sean nacionales o internacionales, a fin

de efectuar las transferencias bancarias que posibilitan el movimiento del dinero sustraído, a cambio de recibir un porcentaje del monto total sustraído; en ese entender, el comportamiento del *phisher-mule* debe ser concebido como aquel brinda ayuda a su cómplice con la receptación del monto sustraído de manera ilícita, quedándose con un pequeño porcentaje de lo sustraído.

Mengoa Valdivia (2021) plantea que la conducta del *phisher-mule* no se logra establecer ni individualizar, por lo que recomienda que esta conducta sea incluida de forma expresa en la legislación sobre los delitos informáticos contra el patrimonio, estableciéndose la diferenciación entre las modalidades de estafa, fraude, sabotaje o hurto informático.

De las tesis antes citadas se advierte que el tipo penal de fraude informático presentan deficiencias en su regulación, por lo cual resulta necesario perfeccionar su redacción y su marco punitivo.

1.2.11 Factores que dificultan la investigación y enjuiciamiento del fraude informático

1.2.11.1 Anonimato del sujeto activo

Como cita Posada Maya (2017), una característica principal de los sujetos activos en el cibercrimen es su anonimato, lo cual se hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes, es así que la identificación del autor en este tipo de delitos

se establecerá al determinarse la relación entre la IP del equipo informático, la cual identifica una red o dispositivo en internet y el ciberdelincuente.

Una de las principales dificultades que presenta la investigación y enjuiciamiento del delito de fraude informático y que de forma general afecta a todos los delitos informáticos es que existe poca información que permita identificar al autor, lo cual se hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes, lo cual aunado acarrea el archivamiento o sobreseimiento de las investigaciones, ya que la formalización de una denuncia o investigación preparatoria que permita el ejercicio de la acción penal, exige como requisito la individualización de la persona imputada, lo cual implica identificarlo con sus nombres y apellidos.

Cabe mencionar que el Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público, referido a la ciberdelincuencia, advierte un alto porcentaje de denuncias archivadas, siendo que la principal causa atribuible al resultado es la poca información y dificultades para identificar al autor, ya que los jueces en base al Art. 230 del NCPP (no identificación el autor), deniegan el levantamiento del secreto de las comunicaciones, sustentada en que el requerimiento debe dirigirse contra una persona determinada, esto es, debe conocerse el nombre del afectado con la medida.

Tabla 6 . Denuncias por delitos informáticos 2013-2020, según estado procesal

ESTADO	CANTIDAD	%
Archivadas	12608	58%
En proceso	8842	41%
Sobreseimiento	125	1%
Sentencia	108	0%
Terminación anticipada	4	0%
TOTAL	**21 687**	

Fuente de imagen: Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público

A ello debe añadirse la falta de mecanismos de cooperación con las entidades del sistema financiero, a fin de que estos provean datos relevantes que posibiliten la identificación de las partes intervinientes, sin precisar ningún detalle que ponga en peligro el secreto bancario. En este extremo debo precisar que de la entrevista realizada al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, éste me manifestó que muchas veces en el desarrollo de los actos de investigación, ante la negativa de las entidades del sistema financiero de proveer los nombres de los titulares de las cuentas a las cuales habían sido transferidos fondos no autorizados, ellos se veían en la necesidad de realizar depósitos de pequeñas sumas de dinero en esas cuentas identificadas, a fin de conocer el nombre de los titulares de las cuentas, y así poder continuar con la investigación, situación que podría evitarse a su entender si esta información fuera provista por las entidades financieras como consecuencia de un acto de cooperación normado.

Finalmente cabe señalar que la falta de equipos sofisticados, como técnicos (software y herramientas informáticas), dificulta aún más el accionar de los agentes de la DIVINDAT. Para Rayón Ballesteros y Gómez Hernández (2014) la lucha contra la ciberdelincuencia requiere de estrategias que involucren sofisticación y trabajo de inteligencia por parte de los operadores encargados de la investigación y persecución, pero es igual de importante la adquisición y conservación de la prueba, de forma tal que estas no pierdan su eficacia, ya que son estas pruebas las que serán sometidas a un profundo análisis por parte de la autoridad judicial, ya que han de evidenciar la comisión del delito.

Es menester precisar en referencia a la investigación que el Inciso 1 del Artículo 334 señala que el Fiscal al calificar la denuncia o después de haber realizado o dispuesto realizar diligencias preliminares, considera que el hecho denunciado no constituye delito, no es justiciable penalmente, o se presentan causas de extinción previstas en la ley, declarará que no procede formalizar y continuar con la investigación preparatoria, así como ordenará el archivo de lo actuado. Finalmente, el Inciso 1 del Artículo 336 señala que si de la denuncia, del Informe Policial o de las Diligencias Preliminares que realizó, aparecen indicios reveladores de la existencia de un delito, que la acción penal no ha prescrito, que se ha individualizado al imputado y que, si fuera el caso, se han satisfecho los requisitos de procedibilidad, el Fiscal dispondrá la formalización y la continuación de la Investigación Preparatoria. Estando a lo antes expuesto, debe indicarse que el Nuevo Proceso Penal se encuentra dividido en tres etapas, Investigación Preparatoria, Etapa

Intermedia y Juzgamiento, la primera de esta se divide a la vez en dos sub etapas: La Investigación Preliminar y la Investigación Preparatoria propiamente dicha, cada una de las cuales con su propia naturaleza, objetivos y características. En la investigación preliminar se han de realizar todas las diligencias urgentes e inaplazables destinadas a determinar si se ha cometido un hecho delictuoso, así como asegurar los elementos materiales de su comisión, individualizar a las personas involucradas en su comisión, incluyendo a los agraviados, a fin de que concluidas dichas diligencias si se advierte la presencia de indicios reveladores de la existencia de un delito, que la acción penal no haya prescrito y que se haya individualizado al imputado, se deberá formalizar la investigación preparatoria.

1.2.11.2 El denunciante no colabora en esclarecer los hechos y posee escasa cultura en seguridad digital

En este punto, corresponde señalar que, en efecto la víctima constituye una fuente de información valiosa sobre todo en este tipo de delitos mutables en el tiempo, debido al surgimiento de nuevas tecnologías, haciendo posible identificar las distintas modalidades en su comisión, así como los bienes jurídicos afectados, lo cual ha de servir para construir políticas orientadas en la prevención y sanción de este tipo de conductas. No solo ello, sino que además la información provista por los agraviados en sus denuncias, así como de aquella que se obtiene a raíz de una investigación, con el uso de la tecnología también puede ser usada contra el crimen, ya que es posible que, a través del uso de inteligencia artificial, puedan agruparse cientos de

denuncias, a fin de encontrar en cuestión de minutos, patrones y asociaciones criminales que antes eran imposibles de identificar. Cabe señalar que las principales razones por las que los denunciantes no colaboran en esclarecer los hechos, es la frustración que en ellos genera la dificultad de identificar al autor, ese sentimiento de injusticia los lleva a desistirse de continuar colaborando con la investigación. Aunado a ello, y como ya lo he mencionado antes, una de las razones advertidas por los agentes de la DIVINDAT, quienes son los encargados de recibir las denuncias y realizar los actos de investigación en los delitos de fraude informático, así como de otros delitos informáticos, como es el caso del SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, quien considera que las entidades del sistema financiero terminan por desempeñar un rol importante en el esclarecimiento de los hechos, no solo porque estos podrían proporcionar datos importantes como los nombres de titulares de cuentas, lo cual coadyuvaría en la identificación del sujeto activo del delito de fraude informático, sino también porque las empresas del sistema financiero, a fin de mantener una imagen de seguridad en el uso de sus plataformas virtuales o de los cajeros automáticos, luego de tomar conocimiento de los reclamos formulados por sus clientes quienes desconocen operaciones no efectuadas por ellos o denuncian la sustracción de su dinero de las cuentas de los bancos en los que son clientes, éstos devuelven los montos sustraídos de las cuentas de sus clientes, razón por la cual los agraviados desisten de continuar con las investigaciones, incluso cuando los hechos hayan sido denunciados.

Debe mencionarse que incluso los bancos ofrecen a sus clientes seguros de protección de tarjeta, justamente para que cubran casos como la clonación de tarjetas, la de transferencias no autorizadas de fondos, en caso de pérdida o robo de tarjeta, o incluso cuando sus clientes han sido víctimas del *phishing*.

Otra de las principales razones por las que los denunciantes no colaboran en esclarecer los hechos, es la percepción de injusticia que estos advierten, por el tiempo que demanda estar involucrado en una investigación y posterior enjuiciamiento, lo cual genera en la víctima un estrés que algunos prefieren no asumir.

Esta situación genera un grave problema en la investigación y enjuiciamiento de la ciberdelincuencia, ya que no se logra identificar y sancionar al autor delictivo, además de no permitir que se conozcan las cifras reales de comisión del delito de fraude informático, ni tampoco conocer las nuevas modalidades delictivas usadas para afectar el patrimonio de las víctimas en el delito de fraude informático.

Finalmente, otra característica que define al usuario víctima del delito de fraude informático según la Organización de los Estados Americanos (2018), es que los usuarios no se informan de las nuevas amenazas de ciberseguridad, existe una falta de conciencia sobre las amenazas a la seguridad, y aunque cada vez más existe información disponible sobre las nuevas formas de ataques y amenazas de seguridad, estas no son muy difundidas en los medios de comunicación tradicionales como los periódicos, la TV y radios locales.

1.2.11.3 Falta de peritos en la materia

A efectos de desarrollar la problemática que surge en cuanto a la falta de peritos en materia de delitos informáticos, debo mencionar que para Rayón Ballesteros y Gómez Hernández (2014) la volatilidad de la prueba electrónica hace necesaria la actuación de protocolos que garanticen su inalterabilidad o daño como consecuencia de una actuación inadecuada, como encender o apagar un ordenador, es por ello que el autor concluye que resulta necesaria la formación adecuada de todos los profesionales del derecho en materia de prueba electrónica, lo cual garantizará su admisibilidad en el proceso (Rayón Ballesteros y Gómez Hernández, 2014).

En cuanto a la evidencia digital Presman (s.f.) expone, que esta está compuesta por los registros que fueron procesados en un dispositivo informático y se encuentran almacenados o fueron transmitidos a través de un medio de comunicaciones informático. La evidencia digital permite almacenar grandes volúmenes de información en contenedores de dimensiones reducidas como es un disco rígido, resalta además la importancia de identificar correctamente la evidencia logrando capturar una foto que retrata un instante ya que al instante siguiente el contenido de la misma habrá variado (Presman, s.f.).

Ahora bien, el perito informático cumple un rol importante en la fase de investigación del delito de fraude informático, a fin de identificar la dirección IP de dispositivos informáticos, que permita identificar al autor delictivo, para

lo cual el perito actúa conforme a los lineamientos y procedimientos establecidos en la Guía de Análisis Digital Forense, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG del 11 de agosto de 2020, la cual estandariza la labor pericial durante el manejo de las evidencias digitales involucradas en investigaciones fiscales, en sus diferentes etapas: identificación, adquisición, aseguramiento, análisis, presentación de informe, hasta su disposición final; analizándolas en busca de indicios que colaboren a llevar adelante una causa judicial, utilizando Software y hardware debidamente reconocidos y licenciados.

Cabe precisar que en el Perú mediante Resolución Ministerial N° 848-2019-IN de fecha 12 de junio del 2019, se resolvió aprobar el Manual para el Recojo de Evidencia Digital, el cual ha sido elaborado con el fin de unificar los criterios empleados por la Policía Nacional del Perú para el adecuado recojo de dispositivos informáticos como celulares, laptops, USB, entre otros, que pueden encontrarse en una escena del crimen, con el objetivo de preservar su contenido como evidencia a ser empleada durante el proceso de investigación.

De lo expuesto, se advierte que la creación de un red de fiscalías especializadas en ciberdelincuencia a nivel nacional, demanda también la necesidad fortalecer la unidad de peritos en esta materia, los cuales estén provistos de equipos informáticos y softwares forenses necesarios, ya que actualmente la demora en la investigación de delos delitos de fraude informático se genera por el retraso en obtener la información solicitada,

como es el caso de la dirección de IP, lo cual permitirá vincular a una determinada persona con los hechos imputados, ya que al no existir Unidades de Alta Tecnología de la Policía Nacional a nivel nacional, se terminan por remitir las pruebas requeridas de todos los delitos informáticos a la ciudad de Lima, surgiendo así una alta demanda de requerimientos, lo cual además acarrea el desvanecimiento de la posibilidad de vincular a alguna persona con los hechos investigados.

1.2.11.4 Necesidad de contar con fiscales capacitados en investigación criminal de delitos informáticos y peritaje forense

Otro problema que genera dilación en la atención de requerimientos formulados a los peritos informáticos, es el desconocimiento de los fiscales respecto de las diligencias a seguir en casos de investigación por delitos de fraude informático, como lo son la identificación del IP, las solicitudes de información de cuentas de correos electrónicos, determinar la ubicación de una página web, identificar al propietario de una página web, la ubicación física de un servidor web, la información de una página web, la recuperación de archivos eliminados o borrados, entre otros.

Así también, resulta necesario que los fiscales conozcan acerca de los procedimientos de informática forense, lo cual posibilitaría que puedan formular un requerimiento adecuado a los peritos informáticos, esto es, que conozcan que información se puede recuperar y cual no, acerca del manejo de la evidencia digital en la investigación, los requerimientos a proveedores

de servicios informáticos extranjeros, a proveedores de redes sociales y correos electrónicos, lo cual permitirá centrar su análisis (Oficina de Análisis Estratégico contra la Criminalidad, 2021).

Cabe señalar que, que esta necesidad de contar con fiscales capacitados en investigación criminal de delitos informáticos y peritaje forense surge debido a que son los representantes del Ministerio Público quienes conducen la investigación realizada por la Policía Nacional y son quienes se encuentran presentes en el allanamiento y registro domiciliario e incautación de bienes en la búsqueda de bienes delictivos cosas o efectos relevantes para la investigación, por lo cual se hace necesario que conozcan el manejo de la evidencia digital en la investigación.

1.2.11.5 Falta de mecanismos de cooperación con las entidades financieras y sobre los reportes de incidentes de seguridad digital que deben efectuar las empresas del sistema financiero

Como ya lo habíamos mencionado con anterioridad las entidades del sistema financiero terminan por desempeñar un rol importante durante el proceso de identificación del autor delictivo de fraude informático, ya que poseen la información identificatoria de los titulares con cuentas en su entidad, información que actualmente debe ser requerida por los fiscales a los jueces penales, conforme a lo establecido en el artículo 235 del Código Procesal Penal, y la Resolución de la Fiscalía de la Nación 4933-2014-MP-FN, la cual aprueba cuatro “Protocolos de Actuación Conjunta” de las medidas limitativas de derechos, de allanamiento, impedimento de salida,

intervención de las comunicaciones telefónicas, y levantamiento del secreto bancario, reserva tributaria y bursátil, señalando que frente a operaciones financieras anómalas vinculadas a la presunta comisión del delito, el fiscal solicitará al juez penal competente el levantamiento del secreto bancario, debiendo precisar en su requerimiento la identidad del sujeto sobre el cual incidirá la medida, entre otras, información que deberá ser proporcionada por la entidad en un máximo de treinta días, tiempo que resulta excesivo teniendo presente la dificultad de los cortos plazos de investigación. En este punto debo precisar que de la entrevista realizada al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, éste me pudo explicar que en este punto de la investigación ellos optan primero por identificar a los *phisher-mule* con la colaboración de los denunciantes, solicitándoles el reporte de sus últimos movimientos bancarios, a fin de obtener los números de cuenta de las personas a quienes se han transferido sumas de dinero, para posteriormente acercarse a algún agente y realizar depósitos por mínimas sumas de dinero y así poder conocer el nombre del titular de la cuenta, y es que se ven en la necesidad de realizar este tipo de prácticas, con la finalidad de acelerar la investigación y debido a que no cuentan con cantidad suficiente de softwares y personal especializado que permita la obtención oportuna de la información requerida, debiendo precisarse que este accionar que sólo es posible con la colaboración del denunciante.

A lo expuesto, debe agregarse que de conformidad con el Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital, todos los proveedores de servicios digitales del sector financiero, deben notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital; al

respecto, debe mencionarse que desde la creación del PECERT y la actual creación del Centro Nacional de Seguridad Digital, siempre existió la disposición de promover la coordinación entre las entidades del sector público y privado en materia de prevención, detección, detención, manejo y recopilación de información, para lo cual se hacía necesario contar con un Equipo de Respuesta ante Incidentes de Seguridad Digital; sin embargo, es a partir de la publicación del Decreto de Urgencia N° 007-2020 que se le agregó el carácter obligatorio, aunque la norma no precisa cual es la sanción a imponer a las entidades del sistema financiero que no cumplan con dicha disposición, por lo cual considero que sería de utilidad que sean los propios clientes afectados los que puedan reportar los incidentes de seguridad digital de los que son víctima.

Lo mencionado encuentra respaldo en lo señalado por la Organización de los Estados Americanos (2018) la cual ha identificado en alusión a los reportes de incidentes de seguridad digital, que existe la necesidad de que las entidades del sistema financiero cuenten con mecanismos de reporte interno, a fin de que sus usuarios internos (empleados y contratistas) reporten ataques exitosos de seguridad digital sufridos, pero también hacer posible que sean los propios clientes de servicios financieros quienes reporten a la entidad incidentes de seguridad digital sufridos, cabe precisar que estos incidentes en su gran mayoría están vinculados al fraude de phishing.

1.2.11.6 Falta de recursos humanos con formación académica en ciberseguridad

La Organización de los Estados Americanos (2018), considera que se hace necesario realizar seminarios web y talleres y mesas redondas, sesiones de capacitación y entrenamientos, a fin de crear conciencia, competencia y transferir habilidades sobre incidentes de seguridad digital.

Debemos recordar que, conforme al artículo 9 del Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone como obligaciones del Proveedor de servicios digitales el notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, así como implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones o como el gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información, todas estas acciones requieren contar por lo menos con un área responsable de la seguridad digital en la entidad bancaria, dependiendo del tamaño de la organización, lo cual implica una necesidad de contar con capital humano suficiente para cubrir la demanda, cabe resaltar que conforme se desprende de la norma antes acotada esta obligación debe ser cumplida por toda empresa proveedora de servicios digitales, esto es, no solo empresas del sistema financiero sino todo proveedor de servicios digitales, ya sean de servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, por lo cual se hace necesario contar con profesionales formados en ciberseguridad; en países como Brasil, Chile y Argentina existen muchas

oportunidades para que la población acceda a una educación en ciberseguridad, tanto en universidades públicas como privadas, así como posgrados y diplomados de especialización relacionados con la ciberseguridad, iniciativas que debemos copiar a efectos de darle lucha a la ciberdelincuencia.

La Organización de los Estados Americanos (2018), resalta la importancia de destinar y mantener un recurso humano adecuado, a fin de llevar a cabo actividades relacionadas con la gestión de riesgos de seguridad, ya que nos actualmente nos encontramos frente a problemas tales como la falta habilidades en ciberseguridad que puedan ser integraos a sus organizaciones.

Además, considero necesaria no solo la preparación de personal humano para que se inserten laboralmente, sino que constituye de vital importancia capacitar a la población, lo cual podría evitar que estos sean víctimas del fraude electrónico, como sucede en el caso del *phishing*, a efectos de que puedan identificar cuando una página a la que acceden es oficial, lo cual puede descubrirse de forma sencilla cuando advertimos que en la barra direcciones aparece un candadito, lo cual significa que la página es segura y, en algunos casos, hasta incluso advertir quién es el propietario.

1.2.11.7 Inmersión de la criminalidad organizada en los delitos informáticos

1.2.11.7.1 Definición de la criminalidad organizada

Sánchez García de Paz (2005) en referencia a la expresión “grupo criminal organizado”, la define como un grupo estructurado de tres o más personas, el cual debe existir durante cierto tiempo y actuar concertadamente con el

propósito de cometer uno o más delitos graves o delitos tipificados en la referida Convención con el fin de obtener un beneficio económico o material. El autor concluye que las características distintivas de la organización criminal frente a la asociación criminal, están referidos a la gravedad de los delitos, la estructura del grupo, la permanencia en sus actividades y el fin económico que persiguen.

En nuestro país podemos obtener un concepto de crimen organizado, a través de la definición establecida en el artículo 2 de la Ley N° 30077, Ley contra el crimen organizado, de la cual se desprende:

> “1. Para efectos de la presente Ley, se considera organización criminal a cualquier agrupación de tres o más personas que se reparten diversas tareas o funciones, cualquiera sea su estructura y ámbito de acción, que, con carácter estable o por tiempo indefinido, se crea, existe o funciona, inequívoca y directamente, de manera concertada y coordinada, con la finalidad de cometer uno o más delitos graves señalados en el artículo 3° de la presente Ley”.

Prado Saldarriaga (2019) define al crimen organizado como un fenómeno delictivo con una estructura organizada y capacidad operativa internacional, la cual desarrolla actividades ligadas, las cuales evidencian abuso de poder,

cuyo accionar delictivo se ha beneficiado del avance tecnológico y la globalización de los mercados.

En tanto, Sánchez García de Paz (2005) señala que la expansión de los grupos criminales organizados en el ámbito internacional constituye uno de sus rasgos más importantes, la cual se ha visto favorecida por la globalización de la economía, la creación de zonas de libre comercio y en principio la red global de transmisión de datos informáticos que conocemos como Internet, la cual posibilita la operación a distancia, lo que dificulta la persecución penal y requiere de la cooperación policial y judicial internacional.

Para Peña Cabrera Freyre (2020) la ciencia y la tecnología han sido utilizados con propósitos ilícitos, ya que a través de la generación de mecanismos sofisticados se ha facilitado la realización de actos delictivos, ya sea facilitando su comunicación o usándola como medio para la comisión de actuar criminal.

La globalización de la economía constituye el factor más importante de expansión de la criminalidad a nivel mundial, la cual ha logrado desestabilizar la seguridad pública y ha generado la impunidad de determinadas conductas, debido a actuales regulaciones deficientes de los países y sus instituciones débiles. El carácter transnacional de la criminalidad organizada requiere de un tratamiento del Derecho comparado, ya que este tipo de organizaciones se encuentra en la búsqueda de

legislaciones benignas, con operadores jurídicos carentes de formación o corruptos, que favorecen su accionar delictivo (Peña Cabrera Freyre, 2020).

Prado Saldarriaga (2019) refiere que el paradigma del Derecho Penal en la actualidad es la globalización del delito económico, denominada también macro criminalidad, la cual aún carece de garantías adecuadas de protección por su alta peligrosidad.

Jimenes Herrera (2017) afirma que la forma adecuada de combatir la criminalidad organizada es a través de la cooperación de todos los Estados, para lo cual antes deberán superarse las diferencias políticas, culturales y sociales, es por ello que deberán fomentarse los convenios bilaterales y multilaterales entre Estados.

1.2.11.7.3 La especial peligrosidad del crimen organizado en los delitos informáticos

Es evidente que existe mayor peligrosidad cuando los delitos son cometidos por una organización criminal, que cuando son cometidos de forma individual, ya que la organización facilita la comisión de delitos y el encubrimiento de sus miembros para evitar la persecución penal, asimismo la participación de profesionales entre sus miembros favorece su carácter duradero y racional (Sánchez García de Paz ,2005).

Los delincuentes informáticos han sido captados por organizaciones

criminales, a fin de fortalecer y facilitar sus actos delictivos resguardando la identidad de sus miembros, pues el ciberespacio brinda ventajas que favorecen sus actos delictivos, ya que otorga anonimato a los miembros, facilita su comunicación incluso a nivel internacional, ha facilitado la perpetración de nuevas conductas dañosas, les permite ocultar más fácilmente sus rastros y es que la complejidad de estos ilícitos y el escaso conocimiento que sobre el mundo tecnológico tienen los encargados de su persecución y castigo, así como el vacío legal producido por aspectos propios del uso de la red dificultan su persecución generando impunidad. Del siguiente cuadro se advierte cómo más del 50% de denuncias de delitos informáticos son archivadas.

Tabla 6 . Denuncias por delitos informáticos 2013-2020, según estado procesal

ESTADO	CANTIDAD	%
Archivadas	12608	58%
En proceso	8842	41%
Sobreseimiento	125	1%
Sentencia	108	0%
Terminación anticipada	4	0%
TOTAL	**21 687**	

Fuente de imagen: Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público

La División de Investigaciones de Alta Tecnología de la Policía Nacional del Perú, bajo un trabajo de inteligencia en los últimos años ha logrado desarticular organizaciones criminales cuyos miembros operaban desde distintos países, los cuales cometían principalmente actos de fraude informático clonando tarjetas de otros países, o mediante el *phishing*, para posteriormente realizar transacciones en línea y transferirlos vía internet a

cuentas bancarias de terceros quienes reciben comisiones por un monto el cual oscila entre 50 a 100 soles por la creación de una cuenta bancaria, entrega de la tarjeta y clave para el retiro del dinero, debe precisarse que estos terceros no conocen la identidad de las personas que les ofrecen dinero, por lo que su identificación debe lograrse empleando herramientas digitales o solicitando información a través de la asistencia mutua en materia penal a otros países.

1.2.11.7.4 Cooperación entre sistemas de Justicia

La complejidad con la que opera la delincuencia organizada, hace que este fenómeno delictivo, demande en la ejecución de actos de investigación y enjuiciamiento del esfuerzo de todos los operadores de justicia, pero también de leyes claras y de herramientas telemáticas de cooperación judicial internacional, así como de equipos conjuntos de investigación, lo cual en conjunto favorecerá el resultado en la lucha contra el crimen organizado (El PAcCTO, s.f.).

Sánchez García de Paz (2005) expone que la Convención de Naciones Unidas contra la delincuencia organizada internacional brinda a los estados miembros de ONU de un marco jurídico para combatir la delincuencia organizada con instrumentos tales como: Extradición y asistencia jurídica en materia penal; nuevos métodos y técnicas de investigaciones especiales; aseguramiento y posterior decomiso de bienes o productos del delito; compromiso de los estados para realización de investigaciones conjuntas; protección de víctimas y testigos y asistencia técnica y capacitación de personal.

En tanto, respecto a los actos de cooperación entre sistemas de Justicia, debemos mencionar que en atención a la Convención Interamericana sobre asistencia mutua en materia penal, ratificada por nuestro país el 04 de marzo de 1995, la cual tiene como principal propósito que los Estados americanos se comprometan a brindarse asistencia mutua en materia penal, esto es, en investigaciones, juicios y actuaciones en materia penal referentes a delitos cuyo conocimiento sea de competencia del Estado requirente al momento de solicitarse la asistencia.

Asimismo, cabe señalar que el Perú cuenta con otro mecanismo de cooperación policial internacional que tiene por objetivo lograr un intercambio fluido de información entre los países miembros, lo cual facilita la investigación y hace posibles operaciones conjuntas, y este es El PAcCTO (Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado), el cual constituye un programa de cooperación internacional entre la Unión Europea y América Latina que tiene por objetivo principal, mejorar la cooperación internacional entre autoridades policiales, así como judiciales y fiscales; el cual da tratamiento a cinco temas principalmente. el cibercrimen, la corrupción, los derechos humanos, el género y el lavado de activos; la asistencia técnica se enfoca en reforzar las capacidades de investigación y cooperación en la lucha contra el crimen organizado transnacional, resaltando la importancia de la participación activa de los países miembros; cabe señalar que este programa se encuentra intrínsecamente vinculado con otros dos proyectos como: AMERIPOL e INTERPOL (El PACCTO, s.f.).

1.2.11.7.7 Jurisdicción y competencia de los tribunales

> Nuestro país se rige bajo el principio de territorialidad (art. 1 CP), según el cual, la ley penal peruana se aplicaría a todo aquel que cometa un hecho punible en el territorio de la República. De lo anterior, se desprende que la ley peruana se aplicaría a todas las personas que estén en territorio peruano, sin importar si son peruanas o extranjeras.
>
> Jiménez Herrera (2017) señala que, en el caso de delitos informáticos, al tratarse de delitos transnacionales, existe jurisdicción múltiple, esto es, los efectos pueden producirse en múltiples países, ya que el internet otorga un espacio sin frontera, lo cual hace compleja su investigación. Por las razones expuestas, los delitos informáticos constituyen una excepción al principio de territorialidad, razón por la cual la competencia es atribuida a tribunales que se encuentren en mejores condiciones de celebrar el juicio.

Cabe señalar que el Convenio sobre la ciberdelincuencia, al respecto señala en la Sección 3 referida a la Jurisdicción, lo siguiente:

> Artículo 22 – Jurisdicción 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:
>
> a. En su territorio; o

b. a bordo de un buque que enarbole su pabellón; o

c. a bordo de una aeronave matriculada según sus leyes; o

d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo. (……).

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.

Estando a lo expuesto, la competencia en materia de delitos informáticos puede ser atribuida al tribunal que se encuentren en mejores condiciones de celebrar el juicio.

1.2.12 Tratamiento internacional de los delitos informáticos

1.2.12.1 México

En el 2017, México presentó una estrategia nacional de seguridad cibernética que permitió a la población y las organizaciones públicas y privadas el uso de las tecnologías de la información y comunicación de manera responsable, con lo cual se fomentaría el desarrollo sostenible del Estado mexicano, para ello cuenta con el CERT-MX, para prevenir y mitigar las amenazas cibernéticas, la cual se encuentra supervisada por la Policía

Federal y forma parte de la red CSIRT (Equipo de respuesta ante incidentes informáticos) Américas. Otra propuesta del Estado mexicano ha sido asegurar suficientes oportunidades a los mexicanos, a fin de que estos realicen estudios tanto de grado como de posgrado centrados en la seguridad cibernética. También se han promovido foros sobre ciberseguridad, con énfasis en el sector financiero o el curso básico de ciberseguridad para funcionarios públicos ofrecido por la Policía Federal. Si bien México no cuenta con una ley dedicada al delito cibernético, el artículo 211 del Código Penal prevé el delito informático, por lo cual las lagunas existentes en materia legal dificultan la lucha contra el cibercrimen (Banco Interamericano de Desarrollo, 2020).

1.2.12.2 Costa Rica

Costa Rica cuenta desde el 2017 con un Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) el cual tiene por objetivo diseñar un marco para orientar las acciones que el país puede tomar respecto al uso seguro de las tecnologías de la información y comunicación, promoviendo medidas de educación, prevención y mitigación del riesgo de utilizar las mismas. En el 2012 se creó un CSIRT (Equipo de respuesta ante incidentes informáticos), el cual es miembro de la red CSIRT (Equipo de respuesta ante incidentes informáticos) Américas, encargado de coordinar entre los diferentes interesados todo lo relacionado con la información y seguridad cibernética, y que además conforma un equipo de expertos en seguridad en tecnologías de la información y comunicación destinado a prevenir y responder a los incidentes cibernéticos contra las instituciones gubernamentales. Se propugna la generación de políticas conformadas por

miembros de entidades públicas y privadas. También se realizan eventos de capacitación para funcionarios (Banco Interamericano de Desarrollo, 2020).

1.2.12.3 Ecuador

Si bien Ecuador aún no cuenta con una estrategia de seguridad cibernética, sí cuenta con EcuCERT, el equipo de respuesta ante incidentes cibernéticos del país, la cual depende de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). El EcuCERT es miembro de CSIRT (Equipo de respuesta ante incidentes informáticos) Américas, por lo que se beneficia de la red de colaboración, intercambio, estímulo y participación en proyectos técnicos entre los CSIRT nacionales, de defensa, policiales y gubernamentales de los países miembros que proporciona la organización. Además, las universidades públicas y privadas ofrecen algunos cursos de capacitación enfocados en seguridad cibernética para hacer frente al déficit en profesionales de seguridad cibernética. (Banco Interamericano de Desarrollo, 2020).

1.2.12.4 Argentina

En 2017, se promulgó el Decreto 577/2017, por él cual se creó el “Comité de Ciberseguridad” dependiente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros y con representantes del Ministerio de Defensa y el Ministerio de Seguridad, cuyo objetivo principal es el de desarrollar una estrategia nacional de seguridad cibernética. También tiene en trámite un proyecto de creación de unidades fiscales especializadas en cibercrimen a nivel nacional, además, para fortalecer los lazos internacionales y sus políticas de seguridad cibernética,

Argentina se asoció con Estados Unidos para mejorar la cooperación en materia de seguridad cibernética y también ha firmado acuerdos con España y Chile, además se encuentran bajo análisis memorandos de entendimiento con China, República de Corea y Rusia. Cuenta también con el ICIC-CERT, el cual, si bien no es miembro de CSIRT (Equipo de respuesta ante incidentes informáticos) Américas, se beneficia de la red. Existen muchas oportunidades para que los argentinos continúen su educación en seguridad cibernética, tanto en universidades públicas como privadas, y también ofrecidos por la sociedad civil (Banco Interamericano de Desarrollo, 2020).

1.2.12.5 Chile

Chile como parte de su estrategia nacional de seguridad cibernética cuentan con la Unidad de Coordinación de Ciberseguridad la cual está encargada de promover una serie de medidas relacionadas con la seguridad cibernética, siendo una de estas medidas el fortalecer el CSIRT (Equipo de respuesta ante incidentes informáticos) de Gobierno, el cual depende del Ministerio del Interior y Seguridad Pública, de conformidad con la Política Nacional de Ciberseguridad. El Banco Interamericano de Desarrollo apoya al gobierno de Chile con asesoría técnica en la evaluación de los niveles de preparación y respuesta en materia de ciberseguridad en el país con el objetivo de identificar, planificar y diseñar mejoras. El CSIRT de Gobierno es miembro de CSIRT Américas, lo cual facilita el intercambio dinámico de información con los países miembros. Chile también cuenta con la Alianza Chilena de Ciberseguridad, la cual reúne a organizaciones públicas y privadas, así como a instituciones académicas, con el fin de promover la educación y el uso responsable de la tecnología, y generar canales de comunicación entre el

sector privado y el gobierno, entre otras cosas. Finalmente, se han impulsado varios programas de educación continua y posgrado en materia de ciberseguridad, tanto desde la perspectiva técnica como legal, con el fin de formar recursos humanos capacitados en estas áreas, en las universidades tanto públicas como privadas hay carreras de grado, así como posgrados y diplomados de especialización relacionados con la ciberseguridad (Banco Interamericano de Desarrollo, 2020).

1.2.12.6 Bolivia

Bolivia cuenta con el Decreto Supremo N.º 2.514 desde el septiembre de 2015 el cual establece la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), con el objetivo de liderar la transformación de la gestión pública y la construcción de la soberanía científica y tecnológica. Asimismo, mediante Decreto Supremo Nº 2.514 se creó el Centro de Gestión de Incidentes Informáticos (CGII), cuya misión es proteger la información crítica del Estado y promover la conciencia de la seguridad para prevenir y responder a los incidentes de seguridad, la cual forma parte de la plataforma CSIRT Américas (Equipos de Respuesta a Incidentes de Seguridad Cibernética). En la Constitución de 2009 se incluyó un apartado sobre la protección de la privacidad. En Bolivia existen cursos de titulación en temas relacionados a la ciberseguridad, así como la existencia de oportunidades en el sector público y privado para capacitación en gobierno digital y seguridad cibernética (Banco Interamericano de Desarrollo, 2020).

1.2.12.7 Brasil

El 5 de febrero de 2020, Brasil publicó el Decreto Federal N° 10.222 102 por el cual aprobó la Estrategia Nacional de Ciberseguridad, la cual busca guiar a Brasil en la seguridad cibernética e incluye acciones para aumentar su resistencia frente a amenazas cibernéticas y fortalecer su desempeño a nivel internacional. En Brasil se advierte que el sector financiero está más avanzado en ciberseguridad, debido a que son objetivos frecuentes, por lo que están invirtiendo más en ciberseguridad. Sin embargo, los usuarios aún no son conscientes de los riesgos de seguridad cibernética, pero a menudo no actúan en consecuencia en sus prácticas cotidianas, por lo que el gobierno ha identificado la necesidad de mejorar la educación en ciberseguridad en escuelas y universidades. Los profesionales del sector público asisten a las cualificaciones profesionales de las TI en el extranjero y reciben certificados de TIC registrados por instituciones internacionales como el Certificado de Seguridad de Sistemas de Información Profesional o el de Gerente de Seguridad de Información Certificado (Banco Interamericano de Desarrollo, 2020).

1.2.13.8 Colombia

Colombia adoptó como estrategia política nacional destinada a fortalecer las capacidades de todas las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. Una de los principales aportes de la nueva política, se creó el Comité de Seguridad Digital, liderado por el Coordinador Nacional de Seguridad Digital. Colombia cuenta con un Ministerio de Tecnología y las Comunicaciones (MinTIC) el cual apoya la gestión e implementación de buenas prácticas y estándares para proteger

los activos críticos de información, infraestructura tecnológica, y sistemas de información y comunicaciones, fomentando la mejora continua. Colombia además cuenta con el ColCERT, un equipo nacional de respuestas a incidentes de seguridad digital, que actualmente depende del Ministerio de Defensa Nacional, y es el encargado de atender en primer término los incidentes cibernéticos y proteger la infraestructura crítica cibernética nacional. Los colombianos tienen amplias oportunidades de continuar con estudios en seguridad cibernética tanto a nivel de grado como de posgrado. Colombia es miembro tanto de Interpol como de Europol y ha priorizado su participación en escenarios internacionales (Banco Interamericano de Desarrollo, 2020).

1.2.12.9 Venezuela

Venezuela actualmente no tiene una estrategia nacional de seguridad cibernética, pero cuenta con SUSCERTE también es sede del CSIRT nacional de Venezuela, VenCERT, cuyo principal objetivo es prevenir, detectar y gestionar incidentes en los sistemas de información de la administración pública nacional y las entidades públicas a cargo de la gestión de infraestructura crítica. No existen oportunidades para que los venezolanos continúen una educación en seguridad cibernética. Venezuela cuenta con la Ley Especial contra los Delitos Informáticos (Banco Interamericano de Desarrollo, 2020).

1.2.12.10 Estados Unidos

Estados Unidos afronta el desafío de la ciberseguridad con un conjunto de normas, instituciones, políticas, campañas de espionaje económico y

financieros, una de estas políticas se expresa en la creación de la figura de un Coordinador Nacional para la Seguridad encargado de trabajar con las administraciones estatales y locales, así como con el sector privado para ofrecer una respuesta unificada a futuros incidentes cibernéticos; asimismo cuenta con un Centro de Análisis e Intercambio de Información.

Estados Unidos tiene una de las culturas cibernéticas más dinámicas del mundo, se creó la Comisión Federal de Comercio (FTC), la cual proporciona a las empresas informes sobre la seguridad de los datos, en tanto, el Sistema Nacional de Concienciación Cibernética constituye el Equipo de Respuesta ante Emergencias Cibernéticas, el cual supervisa el entorno de las amenazas y emite alertas oportunas.

En Estados Unidos existe el Mes de la Concienciación sobre la Ciberseguridad Nacional, creado en 2004 el cual tiene por objetivo el promover una cultura de ciberseguridad en el trabajo y el uso seguro de dispositivos conectados a Internet, así inspirar a los estudiantes a optar por una carrera en el ámbito de la ciberseguridad en estos centros de educación tecnológica, para lo cual facilita el acceso a programas de seguridad informática en los centros universitarios, lo cual a su vez solventa la escasez de personal con conocimientos de ciberseguridad.

Las leyes en este país exigen al sector financiero, las entidades privadas o gubernamentales el informar a las personas sobre violaciones a la seguridad de la información personal de la que hayan sido sujeto.

El equipo de respuestas ante emergencias informática ICS-CERT opera a través de alianzas público-privadas con empresas de infraestructura crítica,

ofreciendo monitoreo, servicios analíticos y asistencia de respuesta para infraestructuras críticas y organizaciones de recursos clave.

El FBI es el organismo líder en la investigación de los delitos informáticos, la cual suma esfuerzos con la Agencia Nacional de Seguridad en la misión de cuidar de la ciberseguridad nacional. Estados Unidos es un país líder en tecnología y ciberseguridad de la información. La ciberseguridad se ha convertido en una prioridad de inversión tanto para el gobierno como para el sector privado (Banco Interamericano de Desarrollo, 2020).

1.2 Definición de términos básicos

- Ciberespacio:

  Se entenderá como una realidad virtual desarrollada mediante herramientas informáticas.

- Cibercrimen:

  Se trata de delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo (Rayón Ballesteros & Gómez Hernández, 2014).

- Ciberseguridad

  Capacidad tecnológica de asegurar el adecuado funcionamiento de las redes y sistemas informáticos, protegiéndolos ante amenazas y vulnerabilidades existentes en el entorno digital (Rayón Ballesteros & Gómez Hernández, 2014).

- Datos informáticos:

Se entenderá toda representación de información o conceptos expresados a través del tratamiento informático (Elías Puelles, (2014).

- *Hacker*:

  Un *hacker* es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información (Jiménez Herrera, 2017).

- Incidente de seguridad digital

  Evento o serie de eventos que comprometen la confianza, la prosperidad económica, la protección de las personas, su información y sus datos personales, a través del uso de tecnologías digitales (Banco Interamericano de Desarrollo, 2020).

- Sistema informático:

  Se entenderá como el conjunto de dispositivos relacionados entre sí, cuya función es el tratamiento automatizado de datos en ejecución de un programa (Elías Puelles, (2014).

- Software:

  Programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático (Rayón Ballesteros & Gómez Hernández, 2014).

- Proveedor de servicios digitales

  Comprende a cualquier entidad pública u organización del sector privado, responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional (Rayón Ballesteros & Gómez Hernández, 2014).

- TIC:

  Las Tecnologías de la Información y las Comunicaciones (en adelante TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que hacen posible el procesamiento, almacenamiento y transmisión de información como (Jiménez Herrera, 2017).

- Usuario:

  Es aquel sujeto funcional que utiliza su identidad digital y la de sus dispositivos, a través de una conexión virtual a los sistemas informáticos, para interactuar en el ciberespacio (Rayón Ballesteros & Gómez Hernández, 2014).

CAPÍTULO II

METODOLOGÍA

2.1 Diseño metodológico

La investigadora desarrollará una investigación cualitativa, de forma tal que identificará y analizará las dificultades que afronta la investigación y enjuiciamiento del delito de fraude informático, se trata pues de una investigación descriptiva de aquellos factores identificados, para lo cual la investigadora ha recurrido a información estadística proporcionada por la División de Investigación de Alta Tecnología, así como reportes estadísticos y entrevistas realizadas por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público a fiscales a cargo de la investigación en este tipo de delitos, así también la investigadora ha podido participar de cursos dictados por la Presidencia del Consejo de Ministros en materia seguridad digital y Equipo de respuesta frente a incidentes de seguridad digital, obteniendo a través de ello respuestas a cuestiones planteadas frente a la ejecución de las medidas legislativas tomadas por el gobierno en el camino a lograr la ansiada confianza digital, todo ello enfocándose en el fraude informático, ya que constituye el delito informático de mayor incidencia delictiva, además analiza las bases teóricas que al respecto se pronuncian, así como el análisis situacional comparativo con la legislación internacional.

2.2 Aspectos éticos

La investigadora declara que respetará los derechos de autor y todos los aspectos éticos necesarios para desarrollar la investigación. La investigadora declara que no ha manipulado la declaración de la entrevista realizada al agente DIVINDAT SO1 PNP Miguel Antonio Torres Moreno, en tanto, respecto a las declaraciones vertidas por el responsable del Centro Nacional de Seguridad Digital, debo precisar que las mismas son de conocimiento público y se hallan contenidas en la página de la Presidencia del Consejo de Ministros, a través de los cursos virtuales publicitados.

CAPÍTULO III

RESULTADOS

1. Entrevista al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT

¿Como realiza sus labores de investigación?

La Unidad de División de Alta Tecnología, rige su accionar sobre la Ley de Delitos Informáticos - Ley 30096 y su modificatoria por la Ley 30171, la cual se desglosa en tres bloques grandes, el acceso ilícito, el fraude informático y la suplantación de identidad; nuestro trabajo en base a estos tres bloques se desarrolla a través de la denuncia por parte del agraviado quien nos provee de las pruebas que se generan en la ejecución del acto delictivo y la intervención del representante del Ministerio Público quien califica el hecho delictivo y conduce la investigación. Además, de las labores propias de investigación que se desarrollan como parte de una investigación, la DIVINDAT cuenta con un área dedicada al desarrollo de patrullajes virtuales, a las cuales denominamos actividades de inteligencias, las cuales permiten detectar los intentos de ataques de los *hackers* a páginas institucionales del sector público, pero también permiten detectar otros ataques cibernéticos, así como identificar a redes de pornografía.

Análisis personal:

La constante evolución que presenta el mundo tecnológico ha facilitado la consumación de nuevos tipos delictivos, lo que hace exigible que los operadores jurídicos encargados de conducir la investigación, como es el caso de los representantes del Ministerio Público, así como del personal que coadyuva en la investigación como lo son los miembros de la Policía Nacional, deban estar

debidamente capacitados en la investigación criminal de delitos informáticos y peritaje forense. Si bien los miembros de la DIVINDAT vienen recibiendo capacitaciones, cursos de especialización tanto a nivel nacional como internacional, a los que pueden acceder gracias a los convenios internacionales suscritos, así como por apoyo del sector financiero y de empresas dedicadas a la tecnología de la información; sin embargo, son pocos los efectivos policiales los que se ven beneficiados con estas capacitaciones, y aquel personal capacitado es el encargado de transmitir sus conocimientos a otros compañeros de la División de Investigación de Alta Tecnología - DIVINDAT, lo cual resulta insuficiente ya que como suele suceder en los distintos centros laborales, el personal es susceptible de ser rotado lo cual demanda una capacitación constante del personal que ingresa, ello además considerando que antes de ingresar a esta área los efectivos policiales no contaban con preparación alguna en materia de ciberseguridad ni el uso de las tecnologías de la información y comunicación, aunado a ello deben enfrentarse además a la carencia de equipos sofisticados, como técnicos (software y herramientas informáticas), para investigar dichos hechos delictivos.

¿Cuáles son los delitos con mayor índice delictivo producidos como consecuencia de la pandemia por el COVID -19?

De acuerdo a los reportes estadísticos los delitos con mayor índice delictivo son el fraude informático, en sus diversas modalidades, y la suplantación de identidad, los cuales se han incrementado de forma exponencial a razón de la pandemia por el COVID -19, esto a razón del incremento de las transacciones a través de la banca por internet por parte de los usuarios, ello en el caso del fraude electrónico; en el caso de la suplantación de identidad, la modalidad más recurrente se ejecuta a

través de la creación de perfiles falsos en páginas de internet, por las cuales haciendo uso de la identidad de la persona suplantada se solicitan donativos económicos para apoyar a un familiar enfermo de COVID-19.

Análisis personal:

Conforme a la tabla de denuncias de delitos informáticos investigados entre el 2013 al 2020, elaborada por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público referida a la ciberdelincuencia, el delito de fraude informático es el de mayor incidencia delictiva, representando casi el 80 % de las denuncias recibidas en matera de delitos informáticos e investigadas por la DIVINDAT, alcanzando en el año 2020 las 2615 denuncias.

Ahora bien, del reporte estadístico recabado de la DIVINDAT se advierte que en el año 2020 la modalidad de fraude informático que mayor denuncia registra son las operaciones y transferencias electrónicas y/o de fondos no autorizados, las cuales a lo largo del 2020 registraron 2350 denuncias.

¿Conoce acerca de las labores desarrolladas por el PECERT, puede precisar cómo se desarrollan las actividades de intercambio de información con la referida institución y Policía Nacional del Perú?

Como parte del Gobierno digital, el PECERT realiza labores de emisión de alertas frente a ataques contra la estabilidad gubernamental, instituciones públicas, a fin de centralizar información, pero como apreciación personal considero que la labor desempeñada por la referida institución aún es deficiente.

Análisis personal:

Cabe precisar que, esta entrevista fue realizada el 19 de abril del presente año y pese a que incluso ya se había publicado el Decreto de Urgencia N° 007-2020 el 09 de enero del 2020 que aprueba el marco de confianza digital y dispone como obligaciones del Proveedor de servicios digitales el notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, este desconocía de su existencia y tampoco supo precisar si en la DIVINDAT existía un área encargada de recibir las alertas de seguridad remitidas por el PECERT, así como la de comunicar los incidentes de seguridad digital, lo cual reafirma la tesis de Morachimo (2020) por el cual refiere que las entidades públicas no están preparadas para recibir reportes de ciberseguridad, agrega que, estas toman como críticas directas a su trabajo y tampoco reconocen cuando se equivocan, lo cual los condena a seguir repitiendo los mismos errores en perjuicio de todos los ciudadanos.

¿Cuál considera usted constituye un mayor obstáculo para el correcto desarrollo en la investigación de los delitos informáticos, y su consecuente persecución y sanción a los autores delictivos?

Actualmente no existe una adecuada coordinación con el sector privado, con el sistema financiero por ejemplo, sería interesante que se promueva una política tendiente a sancionar a las entidades financieras que no comuniquen los actos ataques reiterativos de *hackers* de los que son víctimas sus clientes, ya que esta cifra es alta y no llega a ser de conocimiento por parte de las autoridades competentes y que afecta al patrimonio de los ciudadanos peruanos, ello debido a que las empresas del sistema financiero buscan brindar una imagen de transacciones seguras, ya que de lo contrario podrían dañar su imagen lo cual les acarrea un perjuicio. Los bancos poseen gran información respecto de quienes son las personas que realizan de forma recurrente actos ilícitos y a fin de no aniquilar

promueven impunidad, ya que esta información delictiva oculta no es registrada en las estadísticas que realiza la PNP. El banco devuelve el dinero al ciudadano afectado y este desiste de continuar con la investigación, lo cual da pie a que no se identifique a los autores delictivos, por ello resulta fundamental que exista una coordinación con el sector privado, con los bancos principalmente, los cuales deben contar con un grupo especial que monitoree los delitos informáticos que se cometen en agravio de sus usuarios y que además se facilite la información a la que se necesita acceder para que no prolifere la impunidad. Por lo expuesto, sugiero que deben implementarse políticas destinadas a que se facilite el intercambio de información con las empresas del sistema financiero.

Análisis personal:

En este punto debo precisar que de la entrevista realizada al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, éste me pudo explicar que en este punto de la investigación ellos optan primero por identificar a los *phisher-mule* con la colaboración de los denunciantes, solicitándoles el reporte de sus últimos movimientos bancarios, a fin de obtener los números de cuenta de las personas a quienes se han transferido sumas de dinero, para posteriormente acercarse a algún agente y realizar depósitos por mínimas sumas de dinero y así poder conocer el nombre del titular de la cuenta, y es que se ven en la necesidad de realizar este tipo de prácticas con la finalidad de acelerar la investigación y debido a que no cuentan con cantidad suficiente de softwares y personal especializado que permita la obtención oportuna de la información requerida, debiendo precisarse que este accionar sólo es posible con la colaboración del denunciante.

¿Los efectivos policiales que laboran en la DIVINDAT reciben una capacitación adecuada a efectos de afrontar a los delitos informáticos, teniendo en cuenta su constante evolución? ¿Considera necesaria la capacitación de los operadores jurídicos para afrontar los delitos informáticos?

Los agentes policiales que pertenecemos a esta área recibimos capacitaciones promovidas por entidades financieras, por empresas dedicadas a la tecnología de la información, así como aquellos promovidos por convenios internacionales.

Los delitos informáticos no son delitos comunes y por ende resulta complicado determinar cuándo nos encontramos frente a una flagrancia delictiva, ya que los actos delictivos inician con un acceso ilícito, en la que aún no se ha dispuesto del dinero, pero posteriormente se produce la disposición del dinero, denominado fraude, por ello se necita de fiscales capaces de tipificar adecuadamente los delitos e identificar correctamente cuando nos encontramos frente a flagrancia, lo cual acarrearía una mejor investigación.

Análisis personal:

La constante evolución que presenta el mundo tecnológico ha facilitado la consumación de nuevos tipos delictivos, lo que hace exigible que los operadores jurídicos encargados de conducir la investigación como es el caso de los representantes del Ministerio Público, así como del personal que coadyuva en la investigación como lo son los miembros de la Policía Nacional deban estar debidamente capacitados en la investigación criminal de delitos informáticos y peritaje forense.

¿Considera que una población con mayores conocimientos del uso de redes y con conocimiento de las medidas de prevención mínimos, conllevaría a una reducción de estos tipos delictivos?

La desinformación es determinante en el uso de la tecnología, ya que ésta avanza y esto promueve el incremento delictivo. Por ello la PNP brinda charlas de orientación a la comunidad en los diferentes distritos de la ciudad de Lima. Por las cuales se les explica como realizamos nuestra investigación, la importancia del uso correcto de una tarjeta bancaria, les advertimos de los peligros que conlleva el descargarse aplicaciones sin tener mayor información de las mismas, sobre todo cuando se ventila información personal.

Análisis personal:

En este extremo debo agregar que, otra característica que define al usuario víctima del delito de fraude informático según la Organización de los Estados Americanos (2018), es que los usuarios no se informan de las nuevas amenazas de ciberseguridad, existe una falta de conciencia sobre las amenazas a la seguridad, y aunque cada vez más existe información disponible sobre las nuevas formas de ataques y amenazas de seguridad, estas no son muy difundidas en los medios de comunicación tradicionales como los periódicos, la TV y radios locales. Finalmente, otro aspecto que resulta de vital importancia al momento de estudiar los delitos informáticos, es la actuación del sujeto pasivo, y es que autores como Jiménez Herrera, Acurio del Pino y Di Piero, señalan que constituye un factor determinante en la comisión de delitos informáticos la falta de conocimientos de los sujetos pasivos de la tecnología, lo cual los convierte en blanco fácil para ser víctimas de estos delitos recayendo en ellos la obligación de adoptar medidas de protección

eficaces y efectivas, limitando la intervención del Derecho penal sólo a supuestos en que no es posible la autoprotección.

¿Qué actos de prevención podemos ejecutar a efectos de no ser víctimas del Fraude informático y la suplantación de identidad, ante su potencial incremento delictivo?

Para evitar ser víctima de fraude se debe verificar la procedencia de la página a la cual se intenta acceder, y de una forma sencilla como realizar la búsqueda del enlace en Google, la cual detallará el origen de la misma, ante ello si uno advierte que el origen de la página se ubica en país distinto al de la empresa a la cual se pretende acceder, pues no debería acceder a la misma por el alto riesgo que ello conllevaría, otra forma de verificar la seguridad de la página a la que se accede es advertir la presencia del símbolo del candado te indica que esta página es monitoreada, lo cual no sucede en el caso de páginas creadas; otras sugerencias van desde tener las tarjetas a la vista, ver al operador que manipula nuestra tarjeta, ocultar los dígitos de seguridad que registran las tarjetas al reverso, y principalmente exhortar a la población no hacer pública información personal a través de las redes sociales.

Aporte personal:

En la comisión del delito de fraude informático la información que generalmente roban es: Direcciones de correo, número de documento de identidad, datos de localización y contacto, número de tarjeta de crédito, números de cuentas, redes sociales o cuentas de correo. Los principales medios de propagación son: correos electrónicos, redes sociales, SMS/MMS, llamadas telefónicas o infección de malware, por ello es recomendable evitar enlaces sospechosos, además una forma

sencilla de advertir que una dirección electrónica no es segura, puede identificarse a través de la descripción de la URL, la cual debe iniciar con http:// o https://, así también, se podrá visualizar la imagen de un candado al lado izquierdo de la URL, otras recomendaciones son: jamás hacer clic en un link sospechoso, no facilitar datos por correo electrónico ya que los Bancos jamás solicitan datos por dicho medio, no hacer clic en enlaces, uno mismo debe escribir la dirección, revisar tu estado de cuenta de forma frecuente, mantener actualizado tu software y usar antivirus.

2. “Equipo de respuesta ante incidentes de seguridad digital” certificado por el Centro Nacional de Seguridad Digital

Debo precisar que como parte de mi investigación he participado del curso virtual “Equipo de respuesta ante incidentes de seguridad digital” dictado por el propio responsable del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros Dr. Mauricio Frayssinet, ello a través del acceso al Aula Digital para capacitación en seguridad digital, lo cual me posibilitó absolver los siguientes cuestionamientos.

¿La creación del Centro Nacional de Seguridad Digital desplaza en sus funciones y objetivos al Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional – PECERT?

El Equipo de Respuestas ante incidentes de seguridad digital, también denominado PECERT, forma parte del Centro Nacional de Seguridad Digital, con el adicional de que ahora se ha formado una red nacional, internacional y sectorial de CSIRT dentro de la cual están comprendidos otros países como Chile, Colombia, México,

entre otros, como países miembros de la Alianza del Pacífico, parte del marco de acuerdo del pacifico, pero también integrado por otros países de la OEA.

El Centro Nacional de Seguridad Digital es el primero existente en todo América del Sur, el cual constituye pieza clave para garantizar la trasformación digital, la confianza digital y la mejora en niveles de seguridad digital. La gestión de Alerta Integrada de seguridad digital aún convive con la Plataforma Nacional de Gestión de Incidentes, pero lo que se quiere es que todos puedan acceder a la plataforma y publicar los incidentes que les han afectado.

Análisis personal:

Lo expuesto permite concluir que el Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional – PECERT, ahora forma parte del Centro Nacional de Seguridad Digital, la cual ha ampliado sus funciones ya que ahora comprende una red nacional, internacional y sectorial de CSIRT.

Cabe señalar que algunas de las responsabilidades de un CSIRT son: Realizar estudios forenses sobre los incidentes para determinar cómo sucedió el ataque, investigar nuevas formas de amenazas, desarrollar planes de comunicación para públicos, clientes, trabajadores y directorio, coordinar y ejecutar las estrategias de respuesta, mantener un registro de todas las actividades para referencias futuras, con lo cual se posibilita una comprensión avanzada de las amenazas, maduración del conocimiento, prevención y respuesta ágil.

¿Es posible a la fecha la implementación de lo dispuesto en el artículo 9° del Decreto de Urgencia N° 007-2020, por el cual una de las obligaciones de todo

proveedor de servicios digitales es notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital?

La duda más grade está referida a de donde saco personal para contratar y hacer CSIRT, pero ello no es necesario ya que en cada entidad se posee una brigada para reaccionar a un determinado evento, como podría ser aquella conformada por el gerente de tecnologías de la información, el administrador de red y el oficial de seguridad, los cuales sólo se agruparan cuando se presente una brecha de seguridad, y es que los CSIRT pueden ser constituidos como equipos con roles y tareas bien definidas, cuyos miembros se agrupan cuando se presente una brecha de seguridad. Entonces no necesitas presupuesto para hacer CSIRT y tampoco deben hacerse gastos para hacer plataformas ya que estas se encuentran instaladas en el Centro Nacional de Seguridad Digital.

Análisis personal:

En atención a la pregunta formulada, debemos recordar que de conformidad con el artículo 9 del Decreto de Urgencia N° 007-2020 referido a las obligaciones del proveedor de servicios digitales, esta norma está destinada a todas las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, lo cual me permite concluir que lo afirmado por la PCM si bien podría ser viable en el caso de una entidad del sector financiero la cual cuenta con el presupuesto necesario para destinar incluso un brigada exclusiva de seguridad para conformar una CSIRT, ello no es el caso de una escuela que contrata a una sola persona para la creación de una plataforma educativa y su respuesta ante un ataque, además de ello como ya lo he mencionado antes al no

haberse establecido cual es la sanción ante el incumplimiento de notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital se corre el riesgo de que no se cumplan las obligaciones establecidas en el artículo 9 del Decreto de Urgencia N° 007-2020. Así lo ha entendido la Organización de los Estados Americanos (2018) la cual refiere en alusión a los reportes de incidentes de seguridad digital, que existe la necesidad de que las entidades del sistema financiero cuenten con mecanismos de reporte interno, a fin de que sus usuarios internos (empleados y contratistas) reporten ataques exitosos de seguridad digital sufridos, pero también hacer posible que sean los propios clientes de servicios financieros sean quienes reporten a la entidad incidentes de seguridad digital sufridos, ya que los incidentes reportados en su gran mayoría están vinculados al fraude de *phishing.*

CAPÍTULO IV

DISCUSIÓN

En cuanto a lo afirmado por los autores Jiménez Herrera y Rayón Ballesteros & Gómez Hernández, estos concluyen que los problemas que presenta la persecución y castigo del delincuente informático, se fundan en la complejidad de estos ilícitos y el escaso conocimiento que sobre el mundo tecnológico tienen los encargados de su persecución y castigo; al respecto, comparto lo afirmado por los citados autores y es que la constante evolución que presenta el mundo tecnológico ha facilitado la consumación de nuevos tipos delictivos, lo que hace exigible que los operadores jurídicos encargados de conducir la investigación, como es el caso de los representantes del Ministerio Público, así como del personal que coadyuva en la investigación como lo son los miembros de la Policía Nacional deban estar debidamente capacitados en la investigación criminal de delitos informáticos y peritaje forense ya que la dilación en la atención de requerimientos formulados a los peritos informáticos se debe al desconocimiento de los fiscales respecto de las diligencias a seguir en casos de investigación por delitos de fraude informático, como lo son la identificación del IP, las solicitudes de información de cuentas de correos electrónicos, determinar la ubicación de una página web, identificar al propietario de una página web, la ubicación física de un servidor web, la información de una página web, la recuperación de archivos eliminados o borrados, entre otros. Es menester que los fiscales conozcan acerca de los procedimientos de informática forense, esto es, que conozcan que información se puede recuperar y cual no, acerca del manejo de la evidencia digital en la investigación, los requerimientos a proveedores de

servicios informáticos extranjeros, a proveedores de redes sociales y correos electrónicos, lo cual posibilitaría que puedan formular un requerimiento adecuado a los peritos informáticos, centrando así su análisis (Oficina de Análisis Estratégico contra la Criminalidad, 2021).

Los miembros de la DIVINDAT vienen recibiendo capacitaciones, cursos de especialización tanto a nivel nacional como internacional, a los que pueden acceder gracias a los convenios internacionales suscritos, así como por apoyo del sector financiero y de empresas dedicadas a la tecnología de la información; sin embargo, son pocos los efectivos policiales los que se ven beneficiados con estas capacitaciones, y aquel personal capacitado es el encargado de transmitir sus conocimientos a otros compañeros de la División de Investigación de Alta Tecnología - DIVINDAT, lo cual resulta insuficiente ya que como suele suceder en los distintos centros laborales, el personal es susceptible de ser rotado lo cual demanda una capacitación constante del personal que ingresa, ello además considerando que antes de ingresar a esta área los efectivos policiales no contaban con preparación alguna en materia de ciberseguridad ni el uso de las tecnologías de la información y comunicación, aunado a ello deben enfrentarse además a la carencia de equipos sofisticados, como técnicos (software y herramientas informáticas), para investigar dichos hechos delictivos, lo cual sustenta la tesis propuesta por los autores Rayón Ballesteros & Gómez Hernández y Acurio del Pino, quienes afirman que se hace necesaria en la persecución de este tipo de delitos, el contar con equipos sofisticados, como técnicos (software y herramientas informáticas), para investigar dichos hechos delictivos, ya que

como lo vengo afirmando, el mundo tecnológico es altamente cambiante, y es esa característica la que facilita su comisión, frente a los vacíos legales.

Como cita Posada Maya (2017), una característica principal de los sujetos activos en el cibercrimen es su anonimato, lo cual se hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes, es así que la identificación del autor en este tipo de delitos se establecerá al determinarse la relación entre la IP del equipo informático, la cual identifica una red o dispositivo en internet y el ciberdelincuente, asimismo Rayón Ballesteros y Gómez Hernández (2014) añade que la volatilidad de la prueba electrónica hace necesaria la actuación de protocolos que garanticen su inalterabilidad o daño como consecuencia de una actuación inadecuada, como encender o apagar un ordenador, es por ello que el autor concluye que resulta necesaria la formación adecuada de todos los profesionales del derecho en materia de prueba electrónica, lo cual garantizará su admisibilidad en el proceso (Rayón Ballesteros y Gómez Hernández, 2014).

En este punto es necesario advertir la falta de peritos en la materia lo cual constituye un detrimento en la investigación, y es que el perito informático cumple un rol importante en la fase de investigación del delito de fraude informático, a fin de identificar la dirección IP de dispositivos informáticos, que posibiliten la identificación del autor delictivo, pero a su vez contribuye con su apoyo en otras etapas, ya sea en la identificación del autor delictivo, la adquisición, aseguramiento y análisis de la prueba electrónica, así como de la presentación de informe hasta su disposición final, tendientes a llevar

adelante una causa judicial. De lo expuesto, se advierte que la creación de un red de fiscalías especializadas en ciberdelincuencia a nivel nacional, demanda también la necesidad fortalecer la unidad de peritos en esta materia, los cuales estén provistos de equipos informáticos y softwares forenses necesarios, ya que actualmente la demora en la investigación de los delitos de fraude informático se genera por el retraso en obtener la información solicitada, como es el caso de la dirección de IP, lo cual permitirá vincular a una determinada persona con los hechos imputados, ya que al no existir Unidades de Alta Tecnología de la Policía Nacional a nivel nacional, se terminan por remitir las pruebas requeridas de todos los delitos informáticos a la ciudad de Lima, surgiendo así una alta demanda de requerimientos, lo cual además acarrea el desvanecimiento de la posibilidad de vincular a alguna persona con los hechos investigados.

Como cita Posada Maya (2017), una característica principal de los sujetos activos en el cibercrimen es su anonimato, lo cual se hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes, es así que la identificación del autor en este tipo de delitos se establecerá al determinarse la relación entre la IP del equipo informático, la cual identifica una red o dispositivo en internet y el ciberdelincuente. En efecto concuerdo que una de las principales dificultades que presenta la investigación y enjuiciamiento del delito de fraude informático y que de forma general afecta a todos los delitos informáticos es que existe poca información que permita identificar al autor, lo cual se hace posible debido a las técnicas

de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes, lo cual aunado acarrea el archivamiento o sobreseimiento de las investigaciones, ya que la formalización de una denuncia o investigación preparatoria que permita el ejercicio de la acción penal, exige como requisito la individualización de la persona imputada, lo cual implica identificarlo con sus nombres y apellidos. Cabe mencionar que el Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público, referido a la ciberdelincuencia, advierte un alto porcentaje de denuncias archivadas, siendo que la principal causa atribuible al resultado es la poca información y dificultades para identificar al autor.

A ello debe añadirse la falta de mecanismos de cooperación con las entidades del sistema financiero, a fin de que estos provean datos relevantes que posibiliten la identificación de las partes intervinientes, sin precisar ningún detalle que ponga en peligro el secreto bancario. En este extremo debo precisar que de la entrevista realizada al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, éste me manifestó que muchas veces en el desarrollo de los actos de investigación, ante la negativa de las entidades del sistema financiero de proveer los nombres de los titulares de las cuentas a las cuales habían sido transferidos fondos no autorizados, y siempre que se contara con la cooperación del agraviado, ellos se veían viable en la necesidad de realizar depósitos de pequeñas sumas de dinero en las cuentas identificadas a fin de conocer el nombre de los titulares de las cuentas, y así poder continuar con la investigación, situación que podría evitarse a su entender si esta información fuera provista por las entidades

financieras como consecuencia de un acto de cooperación normado.

Es menester precisar en referencia a la investigación que el Inciso 1 del Artículo 334 señala que el Fiscal al calificar la denuncia o después de haber realizado o dispuesto realizar diligencias preliminares, considera que el hecho denunciado no constituye delito, no es justiciable penalmente, o se presentan causas de extinción previstas en la ley, declarará que no procede formalizar y continuar con la investigación preparatoria, así como ordenará el archivo de lo actuado. Finalmente, el Inciso 1 del Artículo 336 señala que si de la denuncia, del Informe Policial o de las Diligencias Preliminares que realizó, aparecen indicios reveladores de la existencia de un delito, que la acción penal no ha prescrito, que se ha individualizado al imputado y que, si fuera el caso, se han satisfecho los requisitos de procedibilidad, el Fiscal dispondrá la formalización y la continuación de la Investigación Preparatoria. Estando a lo antes expuesto, debe indicarse que el Nuevo Proceso Penal se encuentra dividido en tres etapas, Investigación Preparatoria, Etapa Intermedia y Juzgamiento, la primera de esta se divide a la vez en dos sub etapas: La Investigación Preliminar y la Investigación Preparatoria propiamente dicha, cada una de las cuales con su propia naturaleza, objetivos y características. En la investigación preliminar se han de realizan todas las diligencias urgentes e inaplazables destinadas a corroborar los hechos denunciados y determinar su delictuosidad, teniendo como objetivo reunir los elementos de convicción, de cargo o descargo que permitan al Fiscal decidir si formula o no la acusación, como por ejemplo, estudiar la escena de los hechos, obtener la ficha de identificación de los presuntos

responsables, analizar el objeto, instrumentos o efectos del delito y de ser urgentes e indispensables para cumplir el objetivo de dicha etapa, recibir las declaraciones del denunciante, denunciado y posibles testigos preséncniales de los hechos denunciados, cuyo inicio solo requiere la sospecha de la comisión de un delito, en cambio para la investigación preparatoria propiamente dicha la presencia de indicios reveladores que vinculen al imputado con la comisión de un delito.

Respecto al rol del sujeto pasivo, Acurio del Pino (s.f.) define al sujeto pasivo como el titular del bien jurídico protegido sobre la cual recae la actividad típica del sujeto activo; el autor agrega que a través del sujeto pasivo es posible conocer los diferentes ilícitos que cometen los delincuentes informáticos, información que es utilizada en la prevención de estas acciones. En tanto, Di Piero (2013), respecto al rol protagónico que posee la víctima en el ciberespacio, señala que su accionar no implica que la sociedad deba cargar con los costos de asumir comportamientos imprudentes o inclusos dolosos de la víctima, y que debe ser esta quien asuma la obligación de adoptar medidas de protección eficaces y efectivas, debiendo limitarse la intervención del Derecho penal sólo a supuestos en que no es posible la autoprotección.

Al respecto, otra de las dificultades advertidas que presenta la investigación de los delitos de fraude informático es que el denunciante no colabora en esclarecer los hechos y posee escasa cultura en seguridad digital .En este punto, corresponde señalar que, en efecto la víctima constituye una fuente de información valiosa sobre todo en este tipo de delitos mutables en el

tiempo, debido al surgimiento de nuevas tecnologías, haciendo posible identificar las distintas modalidades en su comisión, así como los bienes jurídicos afectados, lo cual ha de servir para construir políticas orientadas en la prevención y sanción de este tipo de conductas. No solo ello, sino que además la información provista por los agraviados en sus denuncias, así como de aquella que se obtiene a raíz de una investigación, con el uso de la tecnología también puede ser usada contra el crimen, ya que es posible que, a través del uso de inteligencia artificial, puedan agruparse cientos de denuncias, a fin de encontrar en cuestión de minutos, patrones y asociaciones criminales que antes eran imposibles de identificar. Cabe señalar que las principales razones por las que los denunciantes no colaboran en esclarecer los hechos, es la frustración que en ellos genera la dificultad de identificar al autor, ese sentimiento de injusticia los lleva a desistirse de continuar colaborando con la investigación. Aunado a ello, y como ya lo he mencionado antes, una de las razones advertidas por los agentes de la DIVINDAT, quienes son los encargados de recibir las denuncias y realizar los actos de investigación en los delitos de fraude informático, así como de otros delitos informáticos, como es el caso del SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, quien considera que las entidades del sistema financiero terminan por desempeñar un rol importante en el esclarecimiento de los hechos, no solo porque estos podrían proporcionar datos importantes como los nombres de titulares de cuentas, lo cual coadyuvaría en la identificación del sujeto activo del delito de fraude informático, sino también porque las empresas del sistema financiero, a fin de mantener una imagen de seguridad en el uso de sus plataformas virtuales

o de los cajeros automáticos, luego de tomar conocimiento de los reclamos formulados por sus clientes quienes desconocen operaciones no efectuadas por ellos o denuncian la sustracción de su dinero de las cuentas de los bancos en los que son clientes, éstos devuelven los montos sustraídos de las cuentas de sus clientes, razón por la cual los agraviados desisten de continuar con las investigaciones, incluso cuando los hechos hayan sido denunciados. Debe mencionarse que incluso los bancos ofrecen a sus clientes seguros de protección de tarjeta, justamente para que cubran casos como la clonación de tarjetas, la de transferencias no autorizadas de fondos, en caso de pérdida o robo de tarjeta, o incluso cuando sus clientes han sido víctimas del *phishing*. Otra de las principales razones por las que los denunciantes no colaboran en esclarecer los hechos, es la percepción de injusticia que estos advierten, por el tiempo que demanda estar involucrado en una investigación y posterior enjuiciamiento, lo cual genera en la víctima un estrés que algunos prefieren no asumir. Esta situación genera un grave problema en la investigación y enjuiciamiento de la ciberdelincuencia, ya que no se logra identificar y sancionar al autor delictivo, además de no permitir que se conozcan las cifras reales de comisión del delito de fraude informático, ni tampoco conocer las nuevas modalidades delictivas usadas para afectar el patrimonio de las víctimas en el delito de fraude informático.

En este extremo debo agregar que, otra característica que define al usuario víctima del delito de fraude informático según la Organización de los Estados Americanos (2018), es que los usuarios no se informan de las nuevas amenazas de ciberseguridad, existe una falta de conciencia sobre las amenazas a la seguridad, y aunque cada vez más existe información

disponible sobre las nuevas formas de ataques y amenazas de seguridad, estas no son muy difundidas en los medios de comunicación tradicionales como los periódicos, la TV y radios locales. Finalmente, otro aspecto que resulta de vital importancia al momento de estudiar los delitos informáticos, es la actuación del sujeto pasivo, y es que autores como Jiménez Herrera, Acurio del Pino y Di Piero, señalan que constituye un factor determinante en la comisión de delitos informáticos la falta de conocimientos de los sujetos pasivos de la tecnología, lo cual los convierte en blanco fácil para ser víctimas de estos delitos recayendo en ellos la obligación de adoptar medidas de protección eficaces y efectivas, limitando la intervención del Derecho penal sólo a supuestos en que no es posible la autoprotección.

Falta de mecanismos de cooperación con las entidades financieras. Como ya lo habíamos mencionado con anterioridad las entidades del sistema financiero terminan por desempeñar un rol importante durante el proceso de identificación del autor delictivo de fraude informático, ya que poseen la información identificatoria de los titulares con cuentas en su entidad, información que actualmente debe ser requerida por los fiscales a los jueces penales, conforme a lo establecido en el artículo 235 del Código Procesal Penal, y la Resolución de la Fiscalía de la Nación 4933-2014-MP-FN, la cual aprueba cuatro “Protocolos de Actuación Conjunta” de las medidas limitativas de derechos, de allanamiento, impedimento de salida, intervención de las comunicaciones telefónicas, y levantamiento del secreto bancario, reserva tributaria y bursátil, señalando que frente a operaciones financieras anómalas vinculadas a la presunta comisión del delito, el fiscal

solicitará al juez penal competente el levantamiento del secreto bancario, debiendo precisar en su requerimiento la identidad del sujeto sobre el cual incidirá la medida, entre otras, información que deberá ser proporcionada por la entidad en un máximo de treinta días, tiempo que resulta excesivo cuando se trata de delitos en los cuales la evidencia digital es altamente volátil. En este punto debo precisar que de la entrevista realizada al SO1 PNP Miguel Antonio Torres Moreno – Agente DIVINDAT, éste me pudo explicar que en este punto de la investigación ellos optan primero por identificar a los *phisher-mule* con la colaboración de los denunciantes solicitándoles el reporte de sus últimos movimientos bancarios, a fin de obtener los números de cuenta de las personas a quienes se han transferido sumas de dinero para posteriormente acercarse a algún agente y realizar depósitos por mínimas sumas de dinero y así poder conocer el nombre del titular de la cuenta, y es que se ven en la necesidad de realizar este tipo de prácticas, con la finalidad de acelerar la investigación y debido a que no cuentan con cantidad suficiente de softwares y personal especializado que permita la obtención oportuna de la información requerida, debiendo precisarse que este accionar sólo es posible con la colaboración del denunciante.

Respecto a la falta de recursos humanos con formación académica en ciberseguridad. La Organización de los Estados Americanos (2018), considera que se hace necesario realizar seminarios web, talleres y mesas redondas, sesiones de capacitación y entrenamientos, a fin de crear conciencia, competencia y transferir habilidades sobre incidentes de seguridad digital. Debemos recordar que, conforme al artículo 9 del Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y

dispone como obligaciones del Proveedor de servicios digitales el notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, así como implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones o como el gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información, todas estas acciones requieren contar por lo menos con un área responsable de la seguridad digital en la entidad bancaria, dependiendo del tamaño de la organización, lo cual implica una necesidad de contar con capital humano suficiente para cubrir la demanda, cabe resaltar que conforme se desprende de la norma antes acotada esta obligación debe ser cumplida por toda empresa proveedora de servicios digitales pública o privada, esto es, no solo empresas del sistema financiero sino todo proveedor de servicios digitales, ya sean de servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, por lo cual se hace necesario contar con profesionales formados en ciberseguridad, en países como Brasil, Chile y Argentina existen muchas oportunidades para que la población acceda a una educación en ciberseguridad, tanto en universidades públicas como privadas, así como posgrados y diplomados de especialización relacionados con la ciberseguridad, iniciativas que debemos copiar a efectos de darle lucha a la ciberdelincuencia. La Organización de los Estados Americanos (2018), resalta la importancia de destinar y mantener un recurso

humano adecuado, a fin de llevar a cabo actividades relacionadas con la gestión de riesgos de seguridad, ya que nos actualmente nos encontramos frente a problemas tales como la falta habilidades en ciberseguridad que puedan ser integraos a sus organizaciones.

Además, considero necesaria no solo la preparación de personal humano para que se inserten laboralmente, sino que constituye de vital importancia capacitar a la población, lo cual podría evitar que estos sean víctimas del fraude electrónico, como sucede en el caso del *phishing*, a efectos de que puedan identificar cuando una página a la que acceden es oficial, lo cual puede descubrirse de forma sencilla si advertimos que en la barra direcciones aparece un candadito, lo cual significa que la página es segura y, en algunos casos, hasta incluso advertir quién es el propietario.

Cuando hablamos del estudio de delitos informáticos, la actuación del sujeto pasivo resulta de vital importancia, para los autores Jiménez Herrera, Acurio del Pino y Di Piero, la conducta del sujeto pasivo constituye un factor determinante en la comisión de delitos informáticos, ya que la falta de conocimientos de éstos en el uso de la tecnología, los convierte en blancos fáciles para ser víctimas de estos delitos, recayendo en ellos la obligación de adoptar medidas de protección eficaces y efectivas, al respecto debo mencionar que no concuerdo en todo lo afirmado por los citados autores, pues también asumen de forma alguna que el accionar negligente del sujeto pasivo los hace capaces de asumir las consecuencias, sin embargo, considero que no puede atribuírsele esa responsabilidad a los ciudadanos, ya que su desconocimiento en el uso de las tecnologías de la información y comunicación se fundan en la educación deficiente que proporciona el

Estado, ya que éste no es capaz de garantizar que todo niño reciba educación, situación que se ha maximizado con la pandemia por el Covid – 19, la cual además ha evidenciado que nos encontramos lejos de considerarnos un gobierno digital, ya que un porcentaje significativo de la población no puede acceder al internet, ni al uso de herramientas básicas para acceder a esta. Es por ello que considero que resulta de vital importancia que se promueva una formación en el uso de las tecnologías de la información y comunicación a todo ciudadano, sobre todo en materia de ciberseguridad, a fin de lograr minimizar los riesgos de ser víctimas de delincuentes informáticos y limitar con ello la intervención del Derecho penal sólo a supuestos en los que no es posible la autoprotección.

Así también, resulta tan importante como lo mencionado, que en el Perú se promuevan estudios de especialización en materia de ciberseguridad, que no estén únicamente dirigidas a los operadores jurídicos, sino a las nuevas generaciones, a fin de formar material humano capaz de hacer frente a la nueva revolución que amenaza el crecimiento económico el país, los cuales, insertados tanto en el sector público como el privado, puedan coadyuvar a la lucha.

Montoya Guillén (2018) considera que en referencia al artículo 8 de la Ley N° 30096, existe una regulación general, en la que es posible encajar en múltiples conductas, lo cual vulnera el tipo penal que constituye garantía hacia las personas que pueden verse acusadas por delitos que previamente debe estar tipificados, razón por la cual se hace necesario que en nuestro país se prevea el delito de clonación de tarjetas de manera expresa,

detallando la tipificación clara sobre todas las formas que se contemplan con relación a las tarjetas de crédito y débito.

En tanto, Mengoa Valdivia (2021), en su investigación realizada sobre la Punibilidad del comportamiento del *phisher-mule* en referencia al delito de fraude informático en el Perú, señala que la forma general en la que ha sido redactada conforme el artículo 8 de la Ley N° 30096, no permite sancionar el comportamiento del *phisher-mule*, quien es la persona que brinda su o sus números de cuentas bancarias ya sean nacionales o internacionales, a fin de efectuar las transferencias bancarias que posibilitan el movimiento del dinero sustraído, a cambio de recibir un porcentaje del monto total sustraído; en ese entender, el comportamiento del *phisher-mule* debe ser concebido como aquel brinda ayuda a su cómplice con la receptación del monto sustraído de manera ilícita, quedándose con un pequeño porcentaje de lo sustraído. De las tesis antes citadas se advierte que el tipo penal de fraude informático presentan deficiencias en su regulación, por lo cual resulta necesario perfeccionar su redacción y su marco punitivo.

Nos encontramos frente a delitos de suma complejidad, lo cual se agrava con la inmersión de la criminalidad organizada, pero también debido a características propias del desarrollo delictivo, por ejemplo, la determinación de la flagrancia, es por ello que se necita de fiscales capaces no sólo de tipificar adecuadamente los delitos, sino de identificar las distintas figuras legales, desde esa posición es que se defiende el presente trabajo de investigación.

Autores como Guerrero Argote y Elías Puelles afirman que en nuestro país se hace necesario contar con un Plan Nacional de Ciberseguridad, el cual tenga por objetivo la implementación de políticas legislativas destinadas a la creación de la misma, la cual deberá contar con la participación del Estado, del sector privado, la sociedad civil organizada y la ciudadanía. Al respecto,

Morachimo (2020) advierte que las entidades públicas no están preparadas para recibir reportes de ciberseguridad, ya que lo toman como críticas directas a su trabajo y tampoco reconocen cuando se equivocan, lo cual los condena a seguir repitiendo los mismos errores en perjuicio de todos los ciudadanos. Al respecto debe precisarse que, de conformidad con el Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital, todos los proveedores de servicios digitales del sector financiero, deben notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital. En este punto debe precisarse que desde la creación del PECERT y la actual creación del Centro Nacional de Seguridad Digital, siempre existió la disposición de promover la coordinación entre las entidades del sector público y privado en materia de prevención, detección, detención, manejo y recopilación de información, para lo cual se hacía necesario contar con un Equipo de Respuesta ante Incidentes de Seguridad Digital; sin embargo, es a partir de la publicación del Decreto de Urgencia N° 007-2020 que se le agregó el carácter obligatorio, aunque la norma no precisa cual es la sanción a imponer a las entidades del sistema financiero que no cumplan con dicha disposición, por lo cual considero que sería de utilidad que sean los propios clientes afectados los que puedan reportar los incidentes de seguridad digital de los que son víctima.

Lo mencionado encuentra respaldo en lo señalado por la Organización de los Estados Americanos (2018) la cual ha identificado en alusión a los reportes de incidentes de seguridad digital, que existe la necesidad de que las entidades del sistema financiero cuenten con mecanismos de reporte interno, a fin de que sus usuarios internos (empleados y contratistas) reporten ataques exitosos de seguridad digital sufridos, pero también hacer posible que sean los propios clientes de servicios financieros quienes reporten a la entidad incidentes de seguridad digital sufridos, cabe precisar que estos incidentes en su gran mayoría están vinculados al fraude de phishing. De la lectura de los objetivos desplegados por Centro Nacional de Seguridad Digital podría surgir la interrogante de si su creación conlleva al desplazamiento del PECERT en sus funciones, pero esto no es así, debemos recordar que las alertas constituían un análisis técnico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, con el objetivo de informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital, pero en el caso del Centro Nacional de Seguridad, a cargo de la Presidencia del Consejo de Ministros, su objetivo es realizar coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza**,** así como identificar, proteger, detectar, responder, recuperar y recopilar información sobre

incidentes de seguridad digital en el ámbito nacional que son notificados por todo proveedor de servicios digitales.

CONCLUSIONES

1. De los datos estadísticos proporcionados por la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, así como la División de Investigación de Alta Tecnología, evidencian que del universo de delitos informáticos previstos en la Ley N° 30096, modificada por la Ley N° 30171, en el periodo comprendido entre el 2013 y el 2020, sé advierte que el fraude informático es el de mayor incidencia delictiva, siendo sus modalidades recurrentes: la clonación de tarjetas, las compras fraudulentas por internet, las transferencias de fondos no autorizados y los retiros no autorizados.

2. Que, si bien la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, así como la División de Investigación de Alta Tecnología identifican como modalidades de comisión de fraude informático más recurrentes a la clonación de tarjetas, las compras fraudulentas por internet, las transferencias de fondos no autorizados y los retiros no autorizados, estos no se encuentran tipificados expresamente en la Ley 30096, Ley de delitos Informáticos; al respecto, como lo afirma Montoya Guillén (2018) en su investigación realizada sobre la Regulación expresa del delito informático de clonación de tarjetas - Sede DIVINDAT, 2017, el delito de fraude informático tipificado en el artículo 8 de la Ley N° 30096 no es claro, siendo que en nuestro país no se tiene previsto el delito de clonación de tarjetas de manera expresa lo cual genera deficiencias al momento de su aplicación por los operadores de justicia al no existir una tipificación clara sobre todas las formas que se contemplan, en este punto cabe precisar que, la última modificación a la Ley 30096 - Ley de delitos Informáticos, se produjo con la Ley 30171, publicada el

10 de marzo del 2014, la cual si bien modifica el artículo 8° de la Ley 30096, referido al delito de Fraude informático, lo hace sólo en el extremo que reafirma que dicho tipo penal se comete de forma dolosa.

3. En ese mismo sentido, Mengoa Valdivia (2021) en su investigación realizada sobre la Punibilidad del comportamiento del *phisher-mule* en el delito de fraude informático en el Perú, señala que la forma general en la que ha sido redactado el artículo 8 de la Ley N° 30096 no permite sancionar el comportamiento del *phisher-mule*, quien es la persona que brinda su o sus números de cuentas bancarias ya sean nacionales o internacionales, a fin de efectuar las transferencias bancarias que posibilitan el movimiento del dinero sustraído, a cambio de recibir un porcentaje del monto total sustraído; por lo que recomienda que esta conducta sea incluida de forma expresa en la legislación sobre los delitos informáticos contra el patrimonio, estableciéndose la diferenciación entre las modalidades de estafa, fraude, sabotaje o hurto informático.

4. Lo antes expuestos nos permite afirmar que, a la fecha no se han efectuado modificaciones a la Ley 30096 - Ley de delitos Informáticos, orientadas a perfeccionar su redacción y su marco punitivo, lo cual posibilite la sanción de diversas modalidades de comisión de delitos informáticos contra el patrimonio, que a la fecha vienen generando deficiencias al momento de su aplicación por los operadores de justicia.

5. La labor desempeñada por la División de Investigación de Delitos de Alta Tecnología – DIVINDAT constituye pieza importante en la lucha contra la ciberdelincuencia; sin embargo, el desmesurado incremento delictivo en materia

de delitos informáticos sobrepasa todo esfuerzo, más aún cuando su ejercicio afronta de equipos sofisticados, como técnicos (software y herramientas informáticas), así como debido al insuficiente número de personal debidamente capacitado.

6. La mayor dificultad que afronta la investigación del delito de fraude informático es lograr la identificación del autor de los hechos, quien como ya hemos mencionado se encuentra premunido del anonimato, lo cual constituye el principal motivo de archivamientos y sobreseimientos de los procesos relacionados a los delitos informáticos. Al respecto, cabe señalar que, de conformidad con el inciso 2 del artículo 334 del Código Procesal Penal, las diligencias preliminares tienen un plazo de sesenta días, salvo que se produzca la detención de una persona, pudiendo el fiscal fijar un plazo distinto atendiendo a las características, complejidad y circunstancias de los hechos objeto de investigación, en este punto, debe tenerse presente que de no lograrse la identificación del autor el fiscal no podrá disponer la formalización de la investigación preparatoria la cual debe contener de acuerdo al artículo 336 del NCPP el nombre completo del imputado, los hechos y la tipificación específica correspondiente, el nombre del agraviado si fuera posible y las diligencias que inmediatamente deban actuarse. Respecto a la individualización del imputado, debe precisarse que esta implica que el imputado sea identificado con sus nombres, apellidos y su documento nacional de identidad si fuera posible, así como otros datos personales que lo singularicen, como su edad, lugar de nacimiento, el nombre de sus padres, grado de instrucción, ocupación y características físicas.

7. En la actualidad no existen mecanismos de cooperación que posibiliten que las entidades del sistema financiero puedan proveer información necesaria y oportuna que posibiliten la identificación del autor delictivo al Ministerio Público, entidad encargada de liderar la investigación del delito en equipo con la policía, en este punto debe precisarse que de conformidad con el inciso primero del artículo 235° Levantamiento del secreto bancario, el Juez de la Investigación Preparatoria, a solicitud del Fiscal, podrá ordenar, reservadamente y sin trámite alguno, el levantamiento del secreto bancario, cuando sea necesario y pertinente para el esclarecimiento del caso investigado; sin embargo, el plazo para que las entidades requeridas proporcionen la información solicitada es de máximo 30 días hábiles, lo cual constituye una demora que podría acarrear el archivo de la investigación por la excesiva duración en el plazo de las diligencias preliminares, ello teniendo en cuenta además que conforme a la información proporcionada por los agentes DIVINDAT, en el supuesto de que se logre la identificación del *phisher-mule* ello no determinaría la identificación del autor delictivo, ya que esta no suele ser conocida por el *phisher-mule*, quien es la persona que brinda su o sus números de cuentas bancarias ya sean nacionales o internacionales, a fin de efectuar las transferencias bancarias que posibilitan el movimiento del dinero sustraído, a cambio de recibir un porcentaje del monto total sustraído, dificultando a su vez la identificación del autor.

8. La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público tiene entre sus principales funciones establecer lineamientos que orienten las investigaciones en los delitos informáticos, así como unificar criterios en procedimientos y métodos de investigación, a través de la información

proporcionada por los fiscales y por los órganos de apoyo a nivel nacional, y una vez que ha sido analizada y sistematizada, es puesta a disposición de la Fiscalía de la Nación y de los fiscales de los 32 distritos judiciales. Del mismo modo, la información es difundida entre diversas entidades públicas, privadas y organizaciones de la sociedad civil, tanto nacionales como internacionales, cuyas funciones u objetivos están vinculados a la seguridad ciudadana. En mi opinión, existe similitud entre los objetivos de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público y el Observatorio de Criminalidad es adscrito a la Fiscalía de Nación, ya que este último se encarga de sistematizar, analizar y difundir información sobre la criminalidad, las infracciones a la ley penal y la violencia en el Perú, con la finalidad de proporcionar información confiable, oportuna y de calidad que sirva de base para el diseño, implementación y evaluación de las políticas de prevención, persecución inteligente del delito y protección de la víctima, debiendo entenderse que la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público hace sus veces, pero en referencia a los delitos informáticos.

9. El PECERT se encarga de liderar los esfuerzos para resolver, anticipar y enfrentar los desafíos informáticos con el objetivo de informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital, el cual en la actualidad forma parte de la estructura del Centro Nacional de Seguridad.

10. Las entidades públicas y privadas no están preparadas para identificar los incidentes de seguridad, ya que su ejecución conlleva a que todo proveedor digital cuente con un área especializada en ciberseguridad para tal fin, lo cual no sería posible debido a la carencia de recursos humanos en nuestro país. A lo

expuesto, debe agregarse que de conformidad con el Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone como medidas para su fortalecimiento, todo proveedor de servicios digitales debe notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, lo cual tiene carácter obligatorio, sin embargo, la norma no precisa cual es la sanción a imponer a las entidades del sistema financiero que no cumplan con dicha disposición.

11. Debe entenderse por incidente en seguridad digital, aquel acto que logra afectar negativamente a la organización o incluso a la información. esto es, afecta la operación de la organización y sus objetivos de negocios, puede presentar pérdida o corrupción de la información y ocasionar un retraso en las operaciones.

12. La Organización de los Estados Americanos (2018) en alusión a los reportes de incidentes de seguridad digital, precisa que existe la necesidad de que las entidades del sistema financiero cuenten con mecanismos de reporte interno, a fin de que sus usuarios internos (empleados y contratistas) reporten ataques exitosos de seguridad digital sufridos, pero también hacer posible que sean los propios clientes de servicios financieros sean quienes reporten a la entidad incidentes de seguridad digital sufridos, cabe precisar que estos incidentes en su gran mayoría están vinculados al fraude de phishing.

13. Otra de las dificultades que afronta la investigación en los delitos de fraude informático es la falta de colaboración del denunciante en los hechos denunciados, siendo una de las principales razones advertidas por los agentes de la DIVINDAT el hecho de que las empresas del sistema financiero a efectos

de mantener una imagen de seguridad en el uso de sus plataformas virtuales o de los cajeros automáticos, al tomar conocimiento de los reclamos formulados por sus clientes quienes desconocen operaciones no efectuadas por ellos o denuncian la sustracción de su dinero de sus cuentas, éstos devuelven los montos sustraídos de las cuentas de sus clientes, razón por la cual los agraviados desisten de continuar con las investigaciones, incluso cuando los hechos hayan sido denunciados, acción que se sustenta en los seguros de protección de tarjetas que los bancos ofrecen a sus clientes, la cual requiere como requisito para que se efectúe el desembolso, la denuncia efectuada en la comisaría o DIRINCRI, entidad especializada que investiga los fraudes electrónicos; en el supuesto de los usuarios que no adquieren los seguros, la situación es distinta, ya que no les será devuelto el dinero sustraído y estos tampoco deciden colaborar con el esclarecimiento de los hechos debido a la percepción de injusticia que estos advierten, lo expuesto permite afirmar que las cifras consignadas en las estadísticas reportadas por la DIVINDAT y la Unidad Fiscal Especializada en Ciberdelincuencia, no revelan datos reales de la comisión de delitos de Fraude Informático.

14. Se evidencia la falta de peritos informáticos, los cuales cumplen un rol importante en la fase de investigación del delito de fraude informático, ya que hacen posible identificar la dirección IP de los dispositivos informáticos, lo cual permitirá identificar al autor delictivo, para lo cual el perito actúa conforme a los lineamientos y procedimientos establecidos en la Guía de Análisis Digital Forense, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG del 11 de agosto de 2020; cabe señalar que, la creación de un red de fiscalías especializadas en ciberdelincuencia a nivel nacional demanda también la

necesidad fortalecer la unidad de peritos en esta materia los cuales estén provistos de equipos informáticos y softwares forenses necesarios, ya que actualmente la demora en la investigación de los delitos de fraude informático se genera por el retraso en obtener la información solicitada, como es el caso de la dirección de IP, lo cual se debe a su vez al hecho de que al no existir Unidades de Alta Tecnología de la Policía Nacional a nivel nacional, se terminan por remitir las pruebas requeridas de todos los delitos informáticos a la ciudad de Lima, surgiendo así una alta demanda de requerimientos.

15. Otro problema que genera dilación en la atención de requerimientos formulados a los peritos informáticos, es el desconocimiento de los fiscales respecto de las diligencias a seguir en casos de investigación por delitos de fraude informático, como lo sería la identificación del IP, determinar la ubicación de una página web, identificar al propietario de una página web, la ubicación física de un servidor web, la información de una página web, la recuperación de archivos eliminados o borrados, entre otros. Así también, resulta necesario que los fiscales conozcan acerca de los procedimientos de informática forense, lo cual posibilitaría que puedan formular un requerimiento adecuado a los peritos informáticos, esto es, que conozcan que información se puede recuperar y cual no, acerca del manejo de la evidencia digital en la investigación, los requerimientos a proveedores de servicios informáticos extranjeros, a proveedores de redes sociales y correos electrónicos, lo cual permitirá centrar su análisis (Oficina de Análisis Estratégico contra la Criminalidad, 2021).

16. Falta de recursos humanos con formación académica en ciberseguridad, debemos recordar que, conforme al artículo 9 del Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone como obligaciones del Proveedor de servicios digitales el notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, así como implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones o como el gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información, todas estas acciones requieren contar por lo menos con un área responsable de la seguridad digital en la entidad bancaria, dependiendo del tamaño de la organización, lo cual implica una necesidad de contar con capital humano suficiente para cubrir la demanda, cabe resaltar que conforme se desprende de la norma antes acotada esta obligación debe ser cumplida por toda empresa proveedora de servicios digitales, esto es, no solo empresas del sistema financiero sino todo proveedor de servicios digitales, ya sean de servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, por lo cual se hace necesario contar con profesionales formados en ciberseguridad; en países como Brasil, Chile y Argentina existen muchas oportunidades para que la población acceda a una educación en ciberseguridad, tanto en universidades públicas como privadas, así como posgrados y diplomados de especialización relacionados con la

ciberseguridad, iniciativas que debemos copiar a efectos de darle lucha a la ciberdelincuencia.

17. La Organización de los Estados Americanos (2018), resalta la importancia de destinar y mantener un recurso humano adecuado, a fin de llevar a cabo actividades relacionadas con la gestión de riesgos de seguridad, ya que nos actualmente nos encontramos frente a problemas tales como la falta habilidades en ciberseguridad.

18. Además, considero necesaria no solo la preparación de personal humano para que se inserten laboralmente, sino que constituye de vital importancia capacitar a la población, lo cual podría evitar que estos sean víctimas del fraude electrónico, como sucede en el caso del *phishing*, a efectos de que puedan identificar cuando una página a la que acceden es oficial, lo cual puede descubrirse de forma sencilla cuando advertimos que en la barra direcciones aparece un candadito, lo cual significa que la página es segura y, en algunos casos, hasta incluso advertir quién es el propietario.

19. En cuanto, a la inmersión de la criminalidad informática en los delitos informáticos, Sánchez García de Paz y el Programa de Asistencia contra el Crimen Transnacional Organizado (EL PACCTO) advierten que el nuevo escenario que se evidencia con el uso de las redes informáticas, ha favorecido el incremento delictivo cometido por redes criminales.

20. En este extremo debo mencionar que los datos estadísticos con los cuales cuentan la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, así como la División de Investigación de Alta Tecnología, respecto de las denuncias por delito de fraude informático realizados entre el 2013 y el 2020, representan sólo un 30% de la cifra real, ya que existe una alta cifra oculta que no es de conocimiento de los operadores de justicia, debido a que los agraviados no denuncian estos hechos, muchas veces promovidos en este tipo de delitos por la postura que asumen las entidades del sistema financiero, las cuales al tomar conocimiento de que sus clientes han sido víctimas de fraude informático, en sus diversas modalidades, intervienen realizando una investigación interna, cuyos resultados no son de conocimiento del cliente afectado, para posteriormente devolver las sumas sustraídas, a fin de no dañar su imagen de transacciones seguras, lo cual genera esta cifra oculta respecto de los datos reales en cuanto a la comisión de este tipo de delitos.

21. Una de las principales dificultades que presenta la investigación y enjuiciamiento de la ciberdelincuencia es generada justamente por la poca información que se tiene y la dificultad para identificar al autor, lo cual se hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes, las cuales acarrean el archivamiento o sobreseimiento de las investigaciones, ya que uno de los requisitos para formalizar una denuncia o investigación preparatoria y poder ejercitar la acción penal, exige la individualización de la persona imputada esto es, identificarlo con sus nombres y apellidos.

22. Cabe mencionar que el Informe de análisis N° 04, elaborado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Público referida a la ciberdelincuencia, advierte un alto porcentaje de denuncias archivadas, siendo que la principal causa atribuible al resultado es la poca información y dificultades para identificar al autor, ya que los jueces en base al Art. 230 del NCPP (no identificación el autor), niegan el levantamiento del secreto de las comunicaciones.

23. De acuerdo a los reportes estadísticos los delitos con mayor índice delictivo son el fraude informático, en sus diversas modalidades, y la suplantación de identidad, los cuales se han incrementado de forma exponencial a razón de la pandemia por el COVID -19, esto a razón del incremento de las transacciones a través de la banca por internet por parte de los usuarios, ello en el caso del fraude electrónico; en el caso de la suplantación de identidad, la modalidad más recurrente se ejecuta a través de la creación de perfiles falsos en páginas de internet, por las cuales haciendo uso de la identidad de la persona suplantada se solicitan donativos económicos para apoyar a un familiar enfermo de COVID-19.

24. La creación de una fiscalía especializada en delitos informáticos, constituye un gran avance en la lucha contra la ciberdelincuencia, pero existe otro factor que influye en su impunidad y es la falta de coordinación entre las entidades del sector público y privado en materia de prevención, detección, detención, manejo y recopilación de información, así como el desarrollo de soluciones para incidentes de seguridad, acciones de coordinación e intercambio de información,

acciones que deberían ser ejecutadas por el PECERT, pero que aún presentan deficiencias en su ejecución, todo ello con la finalidad de difundir información útil para incrementar los niveles de seguridad de las redes del Perú.

25. En ese sentido, tal como se ha evidenciado en el desarrollo teórico expuesto, la doctrina actual, entre ellos Jiménez Herrera y Rayón Ballesteros & Gómez Hernández, concluyen que los problemas que presenta la persecución y castigo del delincuente informático, se fundan en la complejidad de estos ilícitos y el escaso conocimiento que sobre el mundo tecnológico tienen los encargados de su persecución y castigo, ya que la tecnología ha facilitado la perpetración de nuevas conductas dañosas, así como la ocultación del rastro de las mismas, lo cual aunado al vacío legal que se produce por aspectos propios del uso de la red, genera dificultad en su persecución.

RECOMENDACIONES

1. La creación de más fiscalías especializadas en ciberdelincuencia a nivel nacional, hace necesaria la implementación de más áreas de Análisis Digital Forense a nivel nacional, a fin de reducir la alta demanda de requerimientos, así también se deberán elaborar protocolos y guías estandarizadas que direccionen el accionar de los fiscales en la realización de la investigación de delitos los de fraude informático.
2. Deben generarse oportunidades que posibiliten que los estudiantes egresados de escuelas y universidades puedan continuar una educación en ciberseguridad, a fin de contar con el recurso humano necesario para hacer frente a la lucha contra la ciberdelincuencia y a efectos de componer los CSIRT de todos los proveedores de servicios digitales.
3. Debe difundirse una cultura de ciberseguridad, eventos de prevención y concientización sobre el correcto uso de las nuevas tecnologías dirigidos a docentes, alumnos de nivel secundario y público en general.
4. Las entidades del sistema financiero deben contar con mecanismos de reporte interno de incidentes, a fin de que sus clientes puedan reportar los ataques de seguridad digital sufridos, lo cual permitiría confrontar la información reportada por la entidad del sistema financiero, ello frente a la ausencia de sanción ante el incumplimiento de los proveedores de servicios digitales de reportar las incidencias en seguridad digital padecidas por sus usuarios al Centro Nacional de Seguridad Digital, ello a razón de la obligación contenida en el Decreto de Urgencia N° 007-2020.

FUENTES DE LA INFORMACIÓN

Referencias Bibliográficas

Jiménez Herrera, J. C. (2017). *Manual de derecho penal informático.* Lima: Jurista Editores E.I.R.L.

Peña Cabrera Freyre, A. (2020). *Crimen organizado, aspectos generales, tópicos de la parte general y parte especial.* Lima: Gaceta Jurídica S.A.

Pérez López, J. (2019). *Delitos regulados en leyes penales especiales.* Lima: Gaceta Jurídica S.A.

Prado Saldarriaga, V. (2019). *Derecho penal y política criminal.* Lima: Gaceta Jurídica S.A.

Ramos Suyo, J. A. (2014). *Criminología y política criminal en la globalización*. Lima: Editora y librería jurídica Grijley E.I.R.L.

Sánchez García de Paz, I. (2005). *La criminalidad organizada aspectos penales, procesales, administrativos y policiales.* España: Dikson.S.L.

Referencias Electrónicas

Acurio del Pino, S. (s.f.). *Delitos Informáticos: Generalidades.* Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Asociación por los derechos civiles (2018). *La Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas.* Volumen 1 Recuperado de: https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf

Banco Interamericano de Desarrollo (2020). *Ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe.* Reporte de ciberseguridad 2020. Recuperado de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Di Piero, C. (2013). *El Cibercrímen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Barcelona. Revista para el análisis del derecho INDRET. Recuperado de https://indret.com/wp-content/themes/indret/pdf/984.pdf

Elías Puelles, R. (2014). *Luces y sombras en la lucha contra la delincuencia informática en el Perú.* Lima. Hiperderecho. Recuperado de https://hiperderecho.org/wp-content/uploads/2014/07/01_delitos_informaticos_elias.pdf

El PACCTO (s.f.). Programa de Asistencia contra el crimen trasnacional organizado. Europa Latinoamérica. Recuperado de https://www.elpaccto.eu/sobre-el-paccto/estrategia/

Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. DERECHOS DE AUTOR© (2018) Organización de los Estados Americanos. Recuperado de: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Guerrero Argote, C. (2018). De Budapest al Perú: Análisis sobre el proceso de implementación del convenio de ciberdelincuencia. Lima. Hiperderecho. Recuperado de https://www.derechosdigitales.org/publicaciones/de-budapest-al-peru-analisis-sobre-el-proceso-de-implementacion-del-convenio-de-ciberdelincuencia-impacto-en-el-corto-mediano-y-largo-plazo-2018/

Jiménez Díaz, M. J. (2014). *Sociedad del riesgo e intervención penal.* Revista Electrónica de Ciencia Penal y Criminología, ISSN 1695-0194: Recuperado de http://criminet.ugr.es/recpc/16/recpc16-08.pdf

Jiménez Serrano, J. (2015). *Crimen Organizado: Una aproximación al fenómeno.* España. Revista Electrónica de Ciencia Penal y Criminología, Gaceta Internacional de Ciencias Forenses ISSN 2174-9019. Recuperado de https://www.uv.es/gicf/4A3_Jimenez_GICF_14.pdf

Mengoa Valdivia (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú*. Tesis para obtener el título de abogada, Universidad Cesar Vallejo. Recuperado de: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoa_VMM-SD.pdf?sequence=1

Montoya Guillén (2018). *Regulación expresa del delito informático de clonación de tarjetas - Sede DIVINDAT, 2017*. Tesis para obtener el título de abogado, Universidad Cesar Vallejo. Recuperado de: file:///C:/Users/LENOVO/Downloads/Montoya_GFA%20(2).pdf

Morachimo, M. (2020). *Lo que nos enseña la suplantación y robo a los beneficiarios del Bono Familiar Universal.* Lima. Hiperderecho. Recuperado de: https://hiperderecho.org/2020/06/lo-que-nos-ensena-la-suplantacion-y-robo-a-los-beneficiarios-del-bono-familiar-universal/

Oficina de análisis estratégico contra la criminalidad (2021). *Informe de análisis N°04 ciberdelincuencia*: *Pautas para una investigación fiscal especializada.* Recuperado de:

https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Organización de los Estados Americanos (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe*. Recuperado de: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Salamanca. Revista nuevo foro penal. N° 88. Universidad EAFIT. Recuperado de https://dialnet.unirioja.es/descarga/articulo/6074006/pdf

PECERT (s.f). *Centro de Operaciones de PECERT*. Recuperado de https://www.pecert.gob.pe/index.php/acerca-de-nosotros

Presman, G. (s.f.). *La cadena de custodia en la evidencia digital.* Buenos Aires. Recuperada de: https://mail.google.com/mail/u/0/?tab=rm&ogbl#search/javier/FMfcgxwJWrZRdmwtGfwCksKscPJZFDvd?projector=1&messagePartId=0.1

Rayón Ballesteros, M. C. & Gómez Hernández, J. A. (2014). *Cibercrimen: particularidades en su investigación y enjuiciamiento.* Anuario Jurídico y

Económico Escurialense, 209-234/ISSN: 1133-3677 Cybercrimen. Recuperado de https://dialnet.unirioja.es › descarga › articulo › 4639646

Ramírez Luna, C. M.(s.f.). *El perfil criminológico del delincuente informático*. Recuperado de https://derecho.usmp.edu.pe/centro_estudios_criminologia/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

Salom Clotet, J. (s.f.). *El Ciberespacio y el crimen organizado.* Recuperado de https://dialnet.unirioja.es/descarga/articulo/3837304.pdf.

Referencias Legales

Legislación Internacional

- Convenio sobre la Ciberdelincuencia, Budapest - 2001

Legislación Nacional

- Ley N° 30096, Ley de Delitos Informáticos.
- Ley 30171 que modifica la ley 30096 Ley de Delitos Informáticos
- Ley N° 30077, Ley contra el crimen organizado
- Decreto Legislativo Nº 1244 que modificó el artículo 317 del Código Penal
- Ley N° 30618 Ley que modifica el decreto legislativo 1141, decreto legislativo de fortalecimiento y modernización del sistema de inteligencia

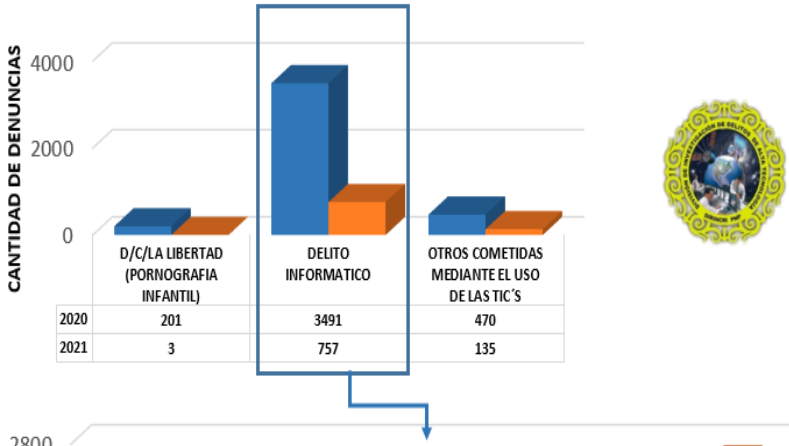
nacional - SINA y de la dirección nacional de inteligencia - DINI, a fin de regular la seguridad digital

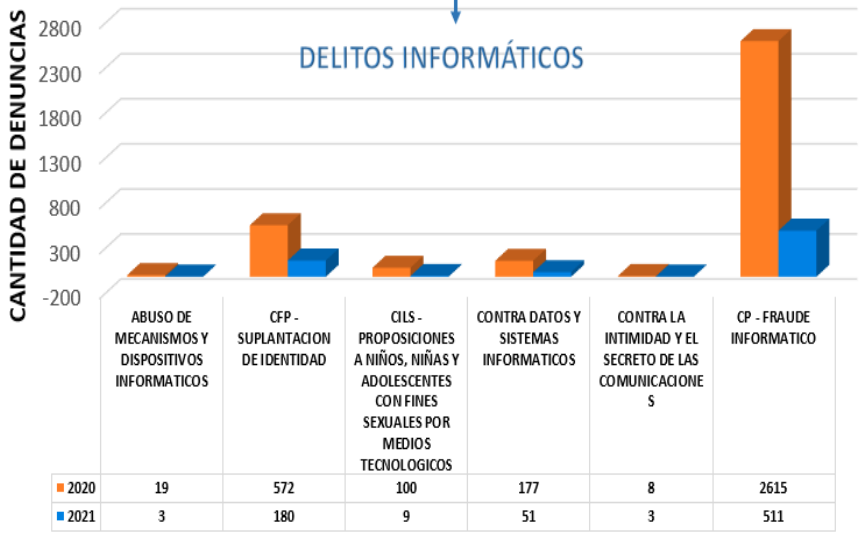
- Decreto Legislativo N°1141. Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional-SINA y de la Dirección Nacional de Inteligencia- DINI
- Decreto Supremo N° 106-2017-PCM. Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN).
- Decreto Legislativo N° 1412. Decreto Legislativo que aprueba la Ley de gobierno digital

ANEXOS

2. Cuadro estadístico comparativo de denuncias recibidas por la DIVINDAT

ESTADÍSTICAS DIVINDAT COMPARATIVA DE DENUNCIAS RECIBIDAS POR LA DIVINDAT AÑOS 2020 y 2021





DENUNCIAS RECIBIDAS POR MODALIDAD DE DELITO INFOMÁTICO

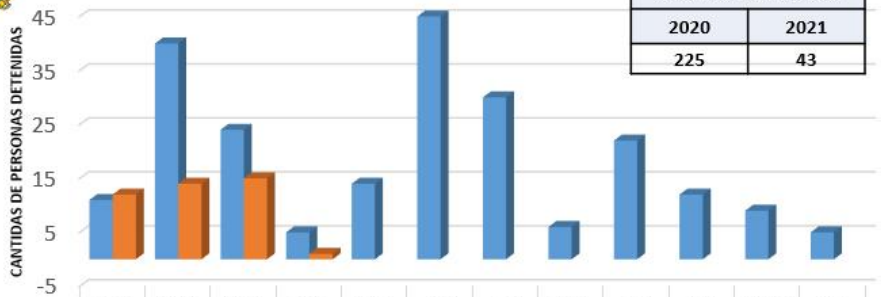
DENUNCIAS RECIBIDAS EN LA DIVINDAT	2020	2021
ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	**19**	**3**
ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	19	3
CFP-SUPLANTACIÓN DE INDENTIDAD	**572**	**180**
SUPLANTACION DE IDENTIDAD	568	180
SUPLANTACION DE IDENTIDAD VIRTUAL	4	
CILS-PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS	**100**	**9**
CONTRA LA INDEMNIDAD SEXUAL DE MENORES	2	1
PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS	98	8
CONTRA DATOS Y SISTEMAS INFORMÁTICOS	**177**	**51**
ACCESO ILICITO	151	11
ACCESO ILICTO A UNA BASE DE DATOS	2	
ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS	9	1
ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMATICOS	9	39
ATENTADO CONTRA LA INTEGRIDAD DE DATOS Y SISTEMAS INFORMÁTICOS	6	
CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	**8**	**3**
INTERCEPTACIÓN DE DATOS	2	
INTERCEPTACIÓN DE DATOS PERSONALES	1	3
TRÁFICO ILEGAL DE DATOS	5	
CP-FRAUDE INFORMÁTICO	**2615**	**511**
CLONACION DE TARJETA-SKIMMING	4	1
COMPRAS FRAUDULENTAS POR INTERNET-CARDING	261	78
OPERACIONES Y TRANSFERENCIA ELECTRONICAS Y/O DE FONDOS NO AUTORIZADOS	2350	432
TOTAL DENUNCIAS	**3491**	**757**

Fuente: Trámite Documentario -DIVINDAT DIRINCRI PNP

DETENIDOS CUADRO 2019-2020 y 2021

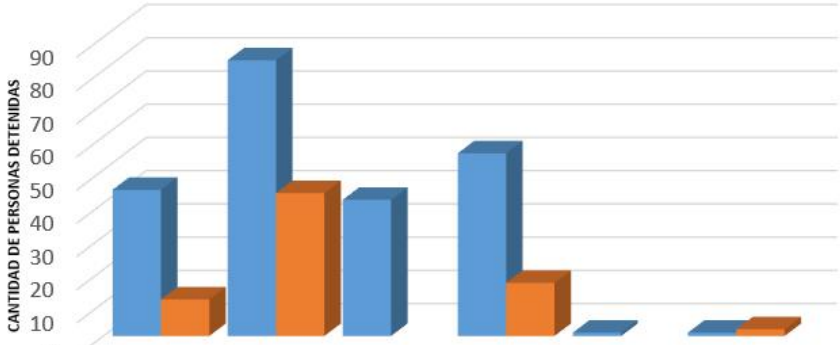
DETENIDOS POR MESES

TOTAL DE DETENIDOS	
2020	2021
225	43



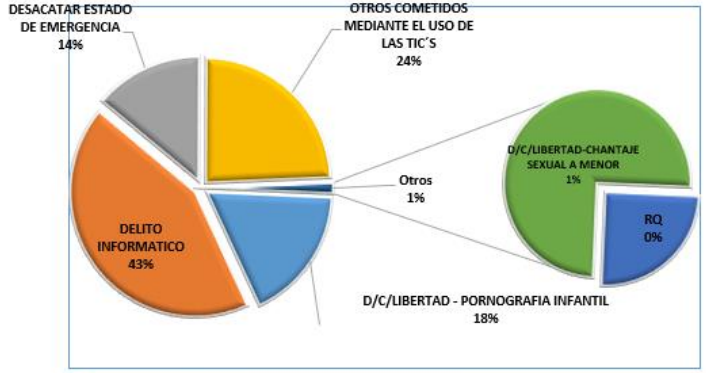
	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC
2020	11	40	24	5	14	47	30	6	22	12	9	5
2021	12	14	15	1								

DETENIDOS POR TIPO DE DELITOS



	D/C/LIBERTAD	DELITO INFORMATICO	DESACATAR EL ESTADO DE EMERGENCIA	OTROS COMETIDAS MEDIANTE EL USO DE LAS TIC´S	RQ	D/C/LIBERTAD-CHANTAJE SEXUAL A MENOR
2020	44	83	41	55	1	1
2021	11	43		16		2

DETENIDOS POR TIPO, PORCENTAJE DE LOS 2 ÚLTIMOS AÑOS

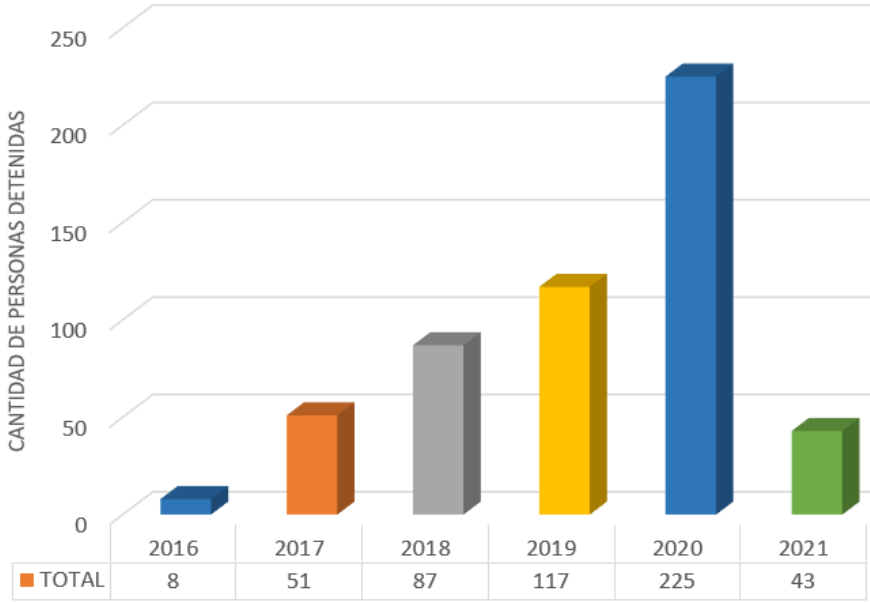


Fuente: Trámite Documentario -DIVINDAT DIRINCRI PNP

NOMBRES DE LAS ORGANIZACIONES Y/O BANDAS DESARTICULADAS EN LOS ÚLTIMOS 6 AÑOS

	ORGANIZACIÓN CRIMINAL
1	"CHILDREN PORN"
2	"TELON DE ACERO"
3	"EXTREMO CHILDREN PORN PERU"
4	RED INTERNACIONAL "LITTLE PRINCES"
5	"NIÑO SEGURO 2021"

PERSONAS DETENIDAS EN LA DIVINDAT EN LOS ÚLTIMOS 6 AÑOS HASTA 14ABR2021



	BANDA CRIMINAL
1	"EL CARTEL DEL FRAUDE"
2	"EL CLAN MOYANO"
3	"KINDER CHOCOLATE"
4	"LAS MULITAS DEL CALLAO"
5	"LOS BULGAROS"
6	"LOS CHICOS DE LAS FLORES"
7	"LOS CIBERNÉTICOS DE SAN JHON"
8	"LOS CIBERNETICOS DEL CONO NORTE"
9	"LOS CIBERNETICOS DEL FRAUDE"
10	"LOS CIBERVENTANALES"
11	"LOS CYBER PIRATAS DE TOMAS VALLE"
12	"LOS ELEGANTES DE LA BANCA"
13	"LOS HACKERS DE BERTEL"
14	"LOS HUELLEROS DEL CONO NORTE"
15	"LOS ILUTIONS"
16	"LOS LLANEROS DEL FRAUDE"
17	"LOS SAMARITANOS"
18	"LOS TRAMAS DE ATE"
19	"LOS TRAPEROS DE BELLAVISTA"
20	"SEÑALES"
21	"TEAMKINGN3T"
22	"EL CLAN INUMA"
23	"EL CLAN PONTE"
24	"LAS TURRIS DEL FRAUDE"
25	"LOS BABYS DEL FRAUDE"
26	"LOS CHIKYS DEL FRAUDE"
27	"LOS CIBERCHOSICANOS"
28	"LOS CIBERINTRUSOS DE CONDEVILLA"
29	"LOS CIBERNETICOS DE LA FLORIDA"
30	"LOS CIBERNETICOS DE VENTANILLA"
31	"LOS CIBERSANJUANEROS"
32	"LOS CYBERBANQUEROS"
33	"LOS DROOPS DEL TELECRÉDITO"
34	"LOS RICKYS DEL BONO"
35	BANDA CONTRA NNA
36	"LOS CIBERTRAFAS DE PACHACUTEC"
37	"LOS CIBERNETICOS DE SANTA MARIA"
38	"LOS HACKER DE CONDE"
39	"LOS CIBERNETICOS DE SAN MARTÍN DE PORRES"
40	"LA LOGIA"
41	"LOS PERUZOLANOS DEL FRAUDE"
42	"LOS DROOPERS DE SAN MARTIN"
43	"LOS CIBERDELINCUENTES DE ATE"
44	"LOS CIBERINTRUSOS DEL CALLAO"
45	"LOS CIBERNETICOS DEL COONO SUR "
46	"LOS CYBER INTRUSOS"
47	"LOS CHALACOS DEL CREDITO"
48	"LAS COMANCHERAS DEL FRAUDE"
49	"LOS CIBERNETICOS DE ALISOS"

Fuente: Trámite Documentario -DIVINDAT DIRINCRI PNP