Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú

Electronic Contracting and Computer Crimes. In Consumer Protection in Peru

Yasmina Riega Virú* https://orcid.org/0000-0002-1725-9030
Hubert Luque Huamani Chirinos** https://orcid.org/0000-0002-6833-1880
Jorge Antonio Machuca Vílchez*** https://orcid.org/0000-0001-7001-2259

http://dx.doi.org/10.21503/lex.v19i28.2318

* Abogada y Magister (Universidad Nacional Federico Villarreal), Doctora en Derecho (Universidad Alas Peruanas). Especialista en Derecho Penal Económico (Universidad de Castilla La Mancha). Jefe de Investigación en Ciencias Sociales y Docente del Curso Derecho Penal (Universidad Privada del Norte-UPN). Perú.
Correo electrónico: yasmina.riega@upn.edu.pe

* Abogado y Magister en Derechos Humanos, Derecho Internacional Humanitario y Resolución de Conflictos por el Centro de Altos Estudios Nacionales, Master en Gerencia Publica por la Escuela de Negocios y Administración de Empresas EUCIM – España. Es Docente Universitario en la Universidad Nacional de Cañete, Universidad Cesar Vallejo, Universidad San Ignacio de Loyola. Perú.
Correo electrónico: hubertluque1974@gmail.com

*** Abogado especialista en Derecho Financiero (Pontificia Universidad Católica del Perú). Magíster en Derecho Bancario y Financiero (Pontificia Universidad Católica del Perú). Facilitador experto en temas financieros por la Fundación Sparkassenstiftung. Docente en Universidad Privada del Norte (UPN), Universidad Nacional Federico Villarreal (UNFV) y Universidad César Vallejo (UCV). Perú
Correo electrónico: jorge.machuca@upn.pe

Ocaso amazónico. Óleo sobre lienzo, 100 x 81 cm.

Cliver Flores Lanza (Iquitos, Loreto, Perú , 1965)
Correo electrónico: floreslanza@yahoo.com
www.cliverpintoramazonico.blogspot.com

RESUMEN

El artículo tiene por objeto revisar los antecedentes y retos de la contratación electrónica en el Perú, con especial énfasis en la protección legal de la que disponen los usuarios frente a los delitos informáticos. Para ello, se realizó una búsqueda bibliográfica a fin de tener un mejor entendimiento del tema en cuestión. Luego del análisis realizado, se encontró que en el Perú aún no se ha implementado las normas necesarias que aseguren la confianza y seguridad de los usuarios; empero, ya se está dando los pasos necesarios para un mejor desarrollo en estas políticas de seguridad informática; otro de los principales problemas, es el desconocimiento por parte del público sobre estas normas. El presente artículo sirve como pauta de revisión al actual estado de las normativas de la política de seguridad informática del Perú para futuras investigaciones.

Palabras clave: *contratación electrónica, cibercomercio, ciberdelincuencia, firma digital, seguridad informática.*

ABSTRACT

The purpose of this article is to review the antecedents and challenges of electronic contracting in Peru, with special emphasis on the legal protection that users have against computer crimes. For this, a bibliographic search was carried out to have a better understanding of the subject in question. After the review is carried out, it is concluded that Peru still does not implement the necessary standards to be able to fully ensure the trust and safety of users, but that in turn it is already taking the necessary steps for a better development of these security policies information technology being also one of the main problems the ignorance on the part of the public about these norms and advances that Peru is having. This article serves as a guideline for reviewing the current state of the regulations of the computer security policy of Peru for future research.

Key words: *cyber-commerce, cybercrime, electronic contracting, digital signature, IT security.*

I. INTRODUCCIÓN

En el contexto social, todas **las personas naturales y jurídicas** acuerdan tomar diferentes acciones y comprar bienes y servicios para satisfacer las necesidades socioeconómicas de sus respectivos ámbitos. Los contratos son una expresión del deseo de proteger y contener diversas situaciones cotidianas para asegurar que estén protegidas por el sistema legal vigente. En orden de cumplir con los principios *ad solemnitatem y probationem* declarados por nuestro Código Civil.

Desde hace algún tiempo, los contratos electrónicos han surgido en todo el mundo como una alternativa práctica y rentable a los contratos de sucesión. Hace más de una década, el sistema financiero de Perú fue testigo de la expansión y los gustos populares. Esta tendencia llamativa que, en 2011, varios países que fueron miembros de la Alianza para la Inclusión Financiera (AFI), incluido Perú[1], promovieron el ecosistema digital, mediante una suscripción de una declaración en la Riviera Maya (México), especialmente para los consumidores de servicios financieros[2].

De acuerdo con lo establecido en los artículos de la Declaración Universal de Derechos Humanos, en concordancia con los artículos 1.3, 55 y 56 de la Carta de las Naciones Unidas, el derecho al desarrollo es "aquel derecho que busca establecer y determinar el libre desenvolvimiento de cada agente frente a su flujo económico, para el crecimiento de cualquier actividad personal y empresarial bajo políticas normativas que tipifiquen su adecuada actuación, en cumplimiento con el fin lícito, orden público y buenas costumbres que coadyuven a mantener el equilibrio económico en forma idónea y eficiente".

1. Las instituciones que suscribieron la Declaración Maya fueron las siguientes: "Central Bank of the Republic of Armenia; Microcredit Regulatory Authority, Bangladesh; Banco Central do Brasil; Banque de la Republique du Burundi; Banque Centrale du Congo; Banco Central del Ecuador; National Bank of Ethiopia; Reserve Bank of Fiji; Bank of Ghana; Banque Centrale de la Republique de Guinée; Bank Indonesia; Central Bank of Kenya; Reserve Bank of Malawi; Comisión Nacional Bancaria y de Valores, México; Bank of Namibia; Central Bank of Nigeria; Central Bank of Pakistan; Banco Central del Paraguay; **Superintendencia de Banca, Seguros y AFP del Perú**; Bangko Sentral ng Pilipinas; National Bank of Rwanda; Ministère de l'Economie et des finances du Sénégal; Central Bank of Solomon Islands; Bank of Tanzania; Bank of Uganda; Bank of Zambia."

2. Alliance for Financial Inclusion. Declaración Maya (2011). Disponible en:
https://www.afi-global.org/sites/default/files/publications/2017-04/Maya%20Declaration_SP.pdf

Los derechos de la contratación, objeto de investigación del presente artículo, no se crean ni se restringen, siendo así que los medios informáticos (electrónicos) son uno de los posibles tipos de apoyo, que incluyen una declaración de voluntad, una declaración de acuerdo vinculante para revelar cuestiones legales. Desde el punto de vista legal, especialmente en lo referido a la obligación y el contrato, los nuevos medios informáticos han transformado el soporte básico expresado actualmente por la voluntad, a veces parcial o completamente según sea necesario. Es adecuado para este nuevo medio y crea un nuevo mecanismo que tiene el mismo propósito que el papel de respaldo.

En línea con estas políticas, la tendencia a la transformación en curso hacia un entorno digital es clara. Hoy se habla de un ecosistema digital, es decir, un grupo interdependiente de empresas, personas y / o cosas que comparten plataformas digitales estandarizadas para un propósito mutuamente beneficioso, como ganancia comercial, innovación o interés común[3].

Sin embargo, el cambio genera problemas. Y frente a esta tendencia, han surgido serias amenazas que pueden afectar la estabilidad del sistema financiero y el propósito de protección al consumidor. Esto debido a los delitos cibernéticos (informáticos).

En efecto, en el segundo trimestre de 2018, los bancos de la región fueron víctimas del ciberdelito, primero en México y luego en Chile. Más tarde, en Perú, se descubrió que algunas de las herramientas robadas por *Shadow Broker* estaban siendo utilizadas para ingresar a bancos en Chile y México. Ante esta situación, los dos países han decidido modernizar el protocolo de ciberseguridad de Chile y fortalecer su sistema de seguridad. Esto significa promulgar una nueva ley en el Banco de México[4].

Asimismo, en mayo de 2019, la ciudad de Baltimore, Maryland, EE. UU., fue víctima de un ciberataque que bloqueó las computadoras de miles de empleados e impidió a los residentes acceder al correo electrónico y pagar facturas. Los ciberdelincuentes utilizaron *ransomware* para perpetuar el ataque y exigieron un pago de alrededor de 100.000 € en Bitcoin[5].

Por otro lado, un incidente reciente ocurrió en Estados Unidos el 7 de mayo de 2021, el Gran Oleoducto Colonial, una de las principales arterias energéticas del país, fue cerrado por un ataque informático el viernes 7 de mayo. Debido a esto tuvo que cerrarse por completo, poniendo en peligro el 45% del suministro de combustible de la costa este del país. El pánico por la escasez de combustible ha obligado a millones de residentes y negocios de la costa este a llenar sus tanques de combustible,

3. Gartner research, 2017. *Seize the digital ecosystem opportunity.* Disponible en: https://www.gartner.com/imagesrv/cio/pdf/Gartner_CIO_Agenda_2017.pdf

4. Marcela Mendoza Riofrío, (2018, julio 31). "Fortinet: Se eleva la incidencia de ataques a bancos en Perú". *El Comercio,* 31 de julio 2018.

5. R. Rodríguez, "Unos hackers tienen secuestrada una ciudad entera de EEUU desde hace dos semanas", 23 de mayo de 2019. Obtenido de *El Confidencial*: https://www.elconfidencial.com/tecnologia/2019-05-23/baltimore-secuestro-hackers-ransomware-robinhood_2018306/

aumentando la demanda y exacerbando los problemas de suministro. El problema surgió a pesar de que Colonial pagó a los ciberdelincuentes casi 5 millones de dólares en rescate de criptomonedas el mismo día del ataque para que pudieran operar con normalidad. DarkSide, el grupo detrás de este ciberdelito es una de las organizaciones criminales involucradas en el robo de datos críticos en el ciberespacio de empresas e instituciones que solo son liberados luego de obtener un pago a cambio[6].

Es así que el diario "El País" informó: La memoria de la fiscalía advirtió sobre un aumento de los delitos informáticos, que se percibieron como "imparables" principalmente como un medio de fraude y estafa. Según el texto emitido por los mismo, en 2019 se iniciaron 13,143 procesos en todo el estado en esta categoría penal. Este número ha aumentado un 44,92% en comparación con principios de 2018 (9.069 en total) y casi el 97% en comparación con los 6.676 registros en 2017. "El aumento de la ciberdelincuencia está relacionado con la delincuencia tradicional y está aumentando lentamente desde el 2,1% en 2011. Según el Ministerio del Interior, sigue creciendo hasta el 4,6% en 2016 y el 9,9% en 2019. Se estima que el 35,8% es que el número de investigaciones penales en línea aumenta cada año"[7].

Es a consecuencia de lo anterior que la Encuesta Nacional de Demanda de Servicios Financieros y Nivel de Cultura Financiera, hecha en el Perú, muestra que el 36% de la población no usa los servicios financieros en línea porque los considera riesgosos. (Superintendencia de Banca, Seguros y AFP de Perú, 2019)[8]; lo cual no es de extrañar. Esta opinión proviene de una encuesta realizada por la consultora Deloitte, en 2017, el 40% de los clientes bancarios experimentaron intentos de fraude financiero en los últimos cinco años, con un enfoque particular en el uso de tarjetas de crédito (Diario Gestión)[9]. De manera similar, en 2018, se encontró que la Asociación de Banqueros del Perú (Asbanc) había informado al público que el sistema financiero había sido golpeado por una serie de ataques financieros en un intento de poner en peligro la seguridad de los bancos (La República)[10].

En armonía con lo expuesto, este artículo analiza en detalle la importancia de los derechos contractuales libres, sobre dispositivos electrónicos, y la afectación de estos por los posibles delitos informáticos que puedan darse. Este es un derecho que los notarios deben ejercer con responsabilidad y es un factor importante en el desarrollo de nuestra economía. Un país que celebra sus acciones además de comprar bienes y servicios.

6. A. Mars, "El ciberataque que exhibió la fragilidad de Estados Unidos", 16 de mayo de 2021. Obtenido de *El País:* https://elpais.com/internacional/2021-05-15/el-ciberataque-que-exhibio-la-fragilidad-de-estados-unidos.html

7. J. M Brunet, "La Fiscalía denuncia el imparable aumento de delitos informáticos", 7 de septiembre de 2020. Obtenido de *El País*:
https://elpais.com/espana/2020-09-07/la-fiscalia-denuncia-el-imparable-aumento-de-delitos-informaticos.html

8. Encuesta Nacional de Demanda de Servicios Financieros y Nivel de Cultura Financiera (2019, julio 19). https://www.sbs.gob.pe/inclusion-financiera/cifras/encuestas

9. Defraudadores tienen en la mira a 76,000 clientes del sistema financiero", *Diario Gestión*, 28 de junio 2019.

10. Asbanc confirma que ataque financiero mundial afectó al Perú". *La República,* 17 de agosto de 2018.

Es decir, se hace la pregunta: ¿La regulación del ciberdelito es suficiente para proteger a los usuarios que tengan contratos electrónicos?

II. LA CONTRATACIÓN ELECTRÓNICA: VENTAJAS Y NUEVOS ACTORES.

Las tendencias mundiales indican una tendencia a la contratación electrónica. Hoy se ha eliminado la "negociación", como ejemplo, solo hay una decisión que tomar al comprar en línea. "Sí o no". Anteriormente, la expresión de voluntad se daba de forma directa y presencial. Hoy, la expresión del deseo se refleja en los medios electrónicos.

El primer párrafo del artículo 103 de la Constitución Política del Perú establece que una legislación especial puede ser promulgada según la naturaleza de las cosas. En este sentido, podemos ver que hubo contratos. Como se explica en la Casación 2066-2016-Ventanilla, el texto se resume de la siguiente manera: "negocio jurídico que se encuentra adherido a la contratación electrónica teniendo su estructura, los presupuestos normativos de un contrato civil establecidos en los artículos 1351 (definición del contrato), 1352, (perfección de contratos) 1354 (libertad contractual) y 1373 (perfeccionamiento del contrato) del Código Civil, por contener la celebración de actos, así como el diverso tipo de adquisición de bienes y servicios, sin embargo al no contener una formalidad prevista por la ley bajo sanción de nulidad por ser un contrato civil, de acuerdo a lo regulado por el inciso 2 del artículo 140 (objeto física y jurídicamente posible),articulo 1411 (requisito formal) y primer párrafo del artículo 1412 (exigencia de las partes del cumplimiento de la formalidad) del mismo cuerpo normativo". Este escenario es la causa de nuevos procedimientos que requieren tiempo y dinero. para una adecuada resolución judicial en el poder judicial.

Con base en esta premisa, los legisladores deben considerar la necesidad de un mercado interno para proteger los contratos electrónicos, como se reconoce en el segundo párrafo del artículo 103 de la Constitución Política del Perú. Además, siendo el derecho a la libre contratación el eje central del derecho al desarrollo y cuya política efectiva y regulada legalmente, debe estar protegida.

Artículo 2 en su primer párrafo del Decreto Legislativo N° 1049 establece que el notario es "perito en materia jurídica y está facultado para probar las acciones y contratos que se le presenten". El primer párrafo del artículo 24 del mismo texto normativo establece que "Un notario público y sus instrumentos estatales notariales de conformidad con la ley genera confianza en la ejecución de la acción judicial y los hechos y circunstancias probados por el mismo".

Como se puede ver, mantener y asegurar la existencia de un documento de contrato es una parte importante de la función del notario; y en tiempos actuales, cuando los contratos derivan de una relación jurídica electrónica, debido al COVID-19, requieren mayor protección y tutela, siendo que, los notarios son conscientes de las implicaciones legales. (Artículo 27 Ley N ° 1049)[11].

11. J. G. Valderrama Chevarría, J. G. "¿Se puede legislar la contratación electrónica y ser tutelada a través de la función notarial?: una nueva necesidad a raíz de la COVID 19", 7 de Mayo de 2020. Obtenido de *La Ley*: https://laley.pe/art/9678/se-puede-legislar-la-contratacion-electronica-y-ser-tutelada-a-traves-de-la-funcion-notarial-una-nueva-necesidad-a-raiz-de-la-covid-19

Los contratos electrónicos se realizan por personas que se encuentran en lugares diferentes durante el periodo de celebración contractual, pero existe la manifestación de la voluntad para su perfeccionamiento[12] y con las partes intervinientes habiéndolo acordado. Las mejoras de dicho contrato se pueden ver intercambiando datos con los deseos de las partes involucradas en el contrato electrónico.

Por lo tanto, puede indicarse que el contrato electrónico tiene componentes tradicionales y modernos: en el primer caso, claramente tenemos el carácter consensual; en el segundo caso, el hecho que la emisión de las declaraciones de voluntad se produce a través de medios electrónicos. Además, no es necesaria la presencia física de las partes en el mercado virtual cuando se trata. Es oportuno diferenciarlo de los contratos informáticos, cuyo objeto únicamente se centra en la contratación de bienes y/o servicios relacionados con la informática[13]. A diferencia de aquél, el contrato electrónico tiene como base el empleo de medios electrónicos, sin mayores límites en cuanto a su objeto.

A continuación, se analizará los caracteres jurídicos de los contratos electrónicos realizados por Internet: (Notaria Rodriguez)[14]

• Este es un contrato estándar pero hecho por medios electrónico. Cabe señalar que los contratos electrónicos generalmente no tienen sus propias reglas, ya que nuestro país no cumple con ciertas regulaciones legales. Sin embargo, en general, este acuerdo es plenamente válido según lo enmendado por el Código Civil en la Ley 27291, de arreglo con los acuerdos consuetudinarios existentes y las disposiciones generales reguladas por el mismo.

• Podrían ser el contrato principal, y en ese sentido tendrían "vida propia", ya que puede no depender de otros contratos anteriores.

• Esto puede ser un problema, ya que todas las partes pueden sufrir pobreza, pero los beneficios lo compensan. Además, al igual que otros contratos, esta confusión no significa necesariamente que los beneficios sean económicamente iguales y, a menudo, existe un desequilibrio entre los dos.

• Este acuerdo se logró mediante la aplicación de lo dispuesto en el artículo 1352 del Código Civil. En otras palabras, se realiza con el consentimiento de todas las partes.

• Esto es mutuamente beneficioso y depende del costo. Si fuera gratis, sería unidireccional, pero los contratos electrónicos también son onerosos.

12. Joselyn Joan Bustamante Gavilano . "La función pública notarial en la contratación electrónica en Lima Metropolitana 2017". (Tesis para optar título profesional. Universidad César Vallejo, Lima, 2017).

13. Carlos Alberto Soto Coaguila, "La contratación electrónica: los supuestos «contratos informáticos» y los contratos celebrados a través de medios electrónicos". *Derecho PUCP*, 55 (2002): 181-221. https://doi.org/10.18800/derechopucp.200201.009.

14. Notaria Rodriguez Velarde. *La contratación electrónica.* 5 de agosto de 2018. Obtenido de Notaria Rodríguez Velarde: https://rodriguezvelarde.com.pe/2018/08/05/la-contratacion-electronica/

• Los acuerdos plurilaterales son posibles porque puedes participar más de una parte.

• El objeto debe ser tangible o intangible, o contar con servicios de valor económico. Puede que exista realmente o puede que exista en el futuro, pero debe estar determinado o ser posible de determinar y no estar prohibido por ley.

• Se trata de una especie de contrato en tiempo real entre los ausentes, ya que el tiempo desde la propuesta hasta la aceptación es muy corto.

• Este puede ser un contrato final o preparatorio debido a las características generales del contrato y la rapidez de aceptación. El uso de herramientas electrónicas de contratación a menudo representa un propósito importante al vincular o establecer contratos de futuros, incluidos depósitos, multas, moratorias o disposiciones opcionales.

• No hay documento en papel, pero todo consta en el documento electrónico.

De forma similar se analiza los principios generales de la contratación electrónica: (Cabrejos & Guerrero)[15].

• **Autonomía de la Voluntad:** Este es uno de los principios que rigen la implementación de los contratos electrónicos y tradicionales, que permite a los consumidores celebrar contratos y establecer sus propias reglas. Este es uno de los pilares principales a los que se adhieren ambos lados. Los contratos electrónicos surgen porque las partes del contrato están obligadas a cumplir lo pactado en el contrato.

• **Buena Fe:** Este es el principio fundamental de toda legislación y se considera dentro del marco de los principios generales del derecho. Por lo tanto, si no se indica en la declaración legal, todo se declara inválido, dado que se basa en lealtad, y cada parte en una relación legal da la bienvenida y está de acuerdo con el negocio. Deben ayudarse a cumplir con su respectiva obligación moral según a lo acordado. Este principio significa no solo lealtad durante el proceso, sino también responsabilidad, de tal forma que las partes se sientan satisfechas, por lo que dependiendo de alguna de las partes el acto jurídico será declarado nulo. Este principio se aplica no solo a los contratos electrónicos, sino también a todo el derecho civil existente, y las partes deben adherirse plenamente a este principio independientemente del entorno en el que hagan negocios.

• **La Neutralidad Tecnológica:** Se considera un principio importante de los contratos electrónicos, pues designa la funcionalidad requerida por todas las normas reguladoras del comercio electrónico y la existencia de tecnologías existentes y futuras, sin la necesidad de cambios o alteraciones en la aplicación. Por lo tanto, el propósito principal es rastrear los hechos y circunstancias que pueden cumplir con

15. G. B. Cabrejos Valdez &T.Y. Guerrero Ortiz, "*Perfeccionamiento del contrato electrónico en el Perú como medida de protección jurídica del consumidor*", (Tesis de Título profesional. Perú: Universidad Señor de Sipán, 2018). Obtenido de https://hdl.handle.net/20.500.12802/4431

todas las reglas del comercio electrónico. En otras palabras, puede dar una interpretación realista, de la regulación de las reglas del comercio virtual de hoy en día; en consonancia con la tecnología en evolución.

Ventajas de la contratación electrónica

De lo ya expuesto se puede ver que la contratación electrónica tiene múltiples beneficios, a continuación, se mencionan algunas de las más resaltantes: (Peña)[16].

1. Superación de las limitaciones geográficas: Al realizar las contrataciones electrónicas permite que una persona al otro lado del mundo pueda participar del contrato.

2. Cantidad de participantes: Obtención de mayor número de posibles participantes del contrato tanto online como offline gracias al aumento de visibilidad que permite Internet.

3. Coste de inicio y de mantenimiento mucho menor que una negociación tradicional: Usualmente una negociación de contrato suele necesitar de un lugar y ciertos costos para poder operar dicho lugar, al ser una contratación electrónica estos factores son reducidos a prácticamente nada dado que el entorno de desarrollo viene a ser un correo electrónico, conferencia virtual, etc.

4. Mayor facilidad de mostrar los beneficios a las partes involucradas: Al ser una contratación electrónica la misma puede explayarse para poder ser los más explicativa posible para las partes involucradas.

5. Ahorro y optimización de tiempo a la hora de realizar las contrataciones.

6. Facilidad para ofrecer una comparativa entre contratos, incluyendo características y opciones.

La firma Electrónica

Los mayores riesgos de los contratos electrónicos son: el riesgo de que un tercero interfiera con el creador del mensaje (falsificación) o su contenido y el riesgo de que un tercero lea el mensaje que desea mantener confidencial. Las firmas escritas a mano pueden autenticarse y verificarse utilizando herramientas de prueba como las pericias de caligrafía. Esto proporciona un alto grado de seguridad para los autores de documentos escritos a mano o firmados. El desafío es lograr los niveles más altos de confiabilidad cuando se trata de trabajo humano y manipulación de documentos electrónicos, dado que en los documentos electrónicos no quedan registros de "huellas".

La firma electrónica tiene atribuida su definición en el artículo 3 de la Ley Nº 27269 en la cual se le define como "aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada

16. Y. J. Peña Jiménez, "Comercio electrónico ventajas y desventajas". (Trabajo de pregrado. Universidad Cooperativa de Colombia, Bogotá, 2019). Recuperado de http://hdl.handle.net/20.500.12494/16999

en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada". La Ley Nº 27269, modificada por la Ley Nº 27310, regula el uso de firmas digitales, garantiza la misma validez y efecto legal que las firmas manuscritas u otras firmas similares, establece reglas generales para los Prestadores de Servicios de Certificación Digital, y está a favor del cumplimiento normativo de la misma. Siendo necesaria establecer una agencia administrativa competente en este caso, (Congreso de la República)[17].

Cabe mencionar que, el artículo 49° del (Congreso de la República, 2017)[18], aprobado por Resolución SBS N° 3274-2017, establece que los contratos que no utilizan mecanismos escritos, como teléfono, comunicaciones electrónicas u otros mecanismos definidos por la empresa, requieren mecanismos adecuados para garantizar la seguridad en todas las etapas del contrato, hasta llegar a la aceptación de este por parte de los clientes.

Sin embargo, tiene dos inconvenientes: Primero, el uso de firmas digitales aún no está muy extendido. La implementación es cara y todavía quedan muchas aplicaciones sin utilizar. En segundo lugar, las firmas digitales solo evitan la falsificación de las identidades de las partes involucradas en la transacción. Estos inconvenientes no se eliminan mediante firmas digitales y pueden suponer un riesgo potencial de delito cibernético (por ejemplo, ataques a los sistemas informáticos de las instituciones financieras).

No obstante, lo señalado, el Gobierno ha dispuesto importantes normas cuyo objeto es promover y estandarizar en el sector público el uso de la firma digital. Primero, mediante la Ley de Gobierno Digital, aprobada por Decreto Legislativo N° 1412 de fecha 13.09.2018, la cual tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno. Y, segundo, a través el Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N° 029-2021-PCM de fecha 19.02.2021, mediante el cual se incorporaron los artículos 1A y 2A en el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, a fin que de forma programática se distingan y empleen los siguientes tipos de firma: 1) Firma Electrónica Simple. Dato en formato electrónico anexo a otros datos electrónicos o asociado de manera lógica con ellos, que utiliza un firmante para firmar; 2) La Firma Electrónica Avanzada. Aquella firma electrónica simple que cumple con las siguientes

17. Congreso de la República, *Ley N° 27269: Ley de firmas y certificados digitales*. 28 de mayo de 2000. Obtenido de El Peruano: https://cdn.www.gob.pe/uploads/document/file/356833/NORMA_1887_LEY_27269_Modificada_por_LEY_27310.pdf

18. Congreso de la República, Resolución SBS Nº 3274-2017: Reglamento de gestión de conducta de mercado del Sistema Financiero, 21 de agosto de 2017. Obtenido de El Peruano: http://ima01.gestion.pe/doc/0/0/2/4/3/243991.pdf

características: (i) está vinculada al firmante de manera única, (ii) permite la identificación del firmante, (iii) ha sido creada utilizando datos de creación de firmas que el firmante puede utilizar bajo su control, y (iv) está vinculada con los datos firmados de modo tal que cualquier modificación posterior de los mismos es detectable; y, 3) Firma Electrónica Cualificada. La que cumple con los estándares de seguridad más rigurosos.

II. LA CIBERDELINCUENCIA

La Ley N° 30618 del año 2017 define la seguridad digital como "un estado de confianza en el entorno digital ante amenazas que afectan las capacidades nacionales mediante la aplicación de medidas de gestión de riesgos, ciberseguridad y ciberdefensas"; para fines nacionales. La ley también establece que la Dirección Nacional de Inteligencia es responsable de "operar y establecer procedimientos para garantizar la seguridad digital dentro de su jurisdicción". (Congreso de la República)[19].

La ciberdelincuencia en contexto generales son las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación.

Los casos de ciberdelincuencia o delitos cibernéticos son definidos en los artículos 2 al 10 de la Ley Nº 30096, todos con excepción del artículo 9 fueron modificados por, las leyes N° 30171 y N° 30838 (Congreso del Perú)[20]. Estos casos son los siguientes:

1. "Artículo 2. Acceso ilícito"
2. "Artículo 3. Atentado contra la integridad de datos informáticos"
3. "Artículo 4. Atentado contra la integridad de sistemas informáticos"
4. "Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos"
5. "Artículo 6. Tráfico ilegal de datos"
6. "Artículo 7. Interceptación de datos informáticos"
7. "Artículo 8. Fraude informático"
8. "Artículo 9. Suplantación de identidad"
9. "Artículo 10. Abuso de mecanismos y dispositivos informáticos"

19. Congreso de la República, LEY Nº 30618. 27 de julio de 2017. Obtenido de El Peruano: https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/

20. Congreso del Perú, Ley N°30171: Ley que modifica la Ley N° 30096, Ley de delitos informáticos, 10 de marzo de 2014. Obtenido de El Peruano: http://www.mef.gob.pe/contenidos/servicios_web/conectamef_quechua/pdf/normas_legales_2012/NL20140310.pdf

Si bien el Perú aún no cuenta con una estrategia nacional de ciberseguridad, pero ha implementado una política nacional de ciberseguridad, especialmente una política nacional de ciberseguridad que enfatiza la necesidad de un comité nacional de ciberseguridad. La cual tiene por objetivos: (Congreso de la República)[21]

- Asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, la infraestructura nacional de información del Estado, los datos, la información y la tecnología utilizada para procesarla frente a amenazas externas o internas.

- Asegurarse de cumplir con las leyes y regulaciones de seguridad de la información o ciberseguridad contenidas en esta política y configure los recursos y las líneas presupuestarias adecuadas en consecuencia.

- Mantener la relevancia de las políticas nacionales de ciberseguridad, garantizar su efectividad y por ende su vigencia actualizada, e involucrar la participación de representantes de la sociedad civil y la academia, así como de actores del sector público y privado.

Existen varios proveedores privados de servicios de ciberseguridad en Perú, algunos de los cuales también ofrecen capacitación sobre este tema. Algunas universidades ofrecen a los peruanos la oportunidad de seguir una educación en ciberseguridad y organizar eventos organizados por asociaciones independientes para resolver problemas. Dado que el gobierno peruano también lidera las actividades de ciberseguridad, en junio de 2018 se celebró una conferencia internacional sobre seguridad digital y gobernanza organizada por el Servicio Nacional de Inteligencia y la Secretaría de Gobierno Digital.

El interés de la investigación en el campo de la vulneración de los derechos de información en los contratos electrónicos y los delitos informáticos o técnicos está estrechamente vinculado a las deficiencias legales en los delitos que atentan contra la integridad de los sistemas informáticos; tal y como se muestra en las conclusiones de investigaciones tales como: "El derecho a la información del consumidor en la Contratación electrónica en el Perú, 2016-2017"[22] y "La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos"[23], el autor concluye que es necesario promover el comercio electrónico y establecer reglas generales que protejan este derecho en el marco del comercio electrónico. Además, agregaron el hecho de que la ley. 30096- "Ley de Delitos Informáticos" no regula adecuadamente los delitos dirigidos a vulnerar la integridad de

21. Congreso de la República. (s.f.). *Política Nacional de Ciberseguridad*. Obtenido de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf."

22. Ruth Ydrogo Gavidia, "El derecho a la información del consumidor en la contratación electrónica en el Perú 2016-2017". (Tesis de grado, Universidad César Vallejo, Lima, 2018).

23. Cynthia Fiorella Carrillo Díaz; Alicia Noemí Montenegro Dávila, "La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos". (Tesis de grado. Universidad Señor de Sipán, Pimentel 2018).

los sistemas informáticos, por lo que se debe reformar el artículo 4. Los delitos informáticos son parte de los delitos ofensivos que dañan la propiedad, los sistemas informáticos y las actividades comerciales.

Sin embargo, es claro admitir que hay un gran desconocimiento de a donde recurrir en caso de vulnerabilidad de la seguridad informática lo que genera desconfianza de los contratos electrónicos dado que las normas actuales son muy generales y no garantizan la seguridad de celebración de los contratos electrónicos.

Blossiers[24] según su investigación, afirma que los avances en tecnología han creado nuevas causas del crimen, incluido el ciberdelito, mientras que el estado ha creado las siguientes nuevas formas de crimen: Pérdida por impacto económico para una empresa. Esto tiene un impacto social en la desconfianza de los clientes hacia las empresas bancarias y la inestabilidad legal que puede resultar de los procesos civiles y penales que pueden iniciar los clientes afectados.

Vilca[25], en su tesis titulada "La formación profesional en derecho informático y la persecución penal de delitos informáticos en el distrito fiscal de Huánuco-2017", enfatizó la importancia de la educación en derecho de la información digital para enfrentar los nuevos desafíos que la informática plantea a la sociedad. Especialmente si el abogado trabaja para una agencia como el Ministerio de Asuntos Públicos para manejar las acusaciones penales de delitos informáticos en el Perú.

Cabe señalar que los estudios revisados no identificaron deficiencias regulatorias y no proporcionaron alternativas para abordar las deficiencias regulatorias. Por lo tanto, el propósito de este estudio es analizar las capacidades regulatorias de los delitos informáticos para proteger los contratos electrónicos.

Perfil del ciberdelincuente (sujeto activo)

Esta forma de delincuencia el ciberdelincuente (sujeto activo) debe tener habilidades especializadas y conocimientos detallados en el campo de la gestión de sistemas informáticos. Por estas características, los sujetos activos se clasifican como delincuentes de cuello blanco con las siguientes características: (Villavicencio)[26]

a) Tener conocimientos avanzados de informática.

b) Ocupa un lugar estratégicamente importante en el lugar de trabajo donde se procesa información sensible (esto se denomina delito laboral porque se comete por la propiedad y acceso del sistema que el sujeto posee).

24. Juan José Blossiers Mazzini, "El delito informático y su incidencia en la empresa bancaria", (Tesis posgrado, Universidad Nacional Federico Villarreal, Lima 2018).

25. Leonardo Edgard Vilca Morales, "La formación profesional en derecho informático y la persecución penal de delitos informáticos en el Distrito Judicial de Huánuco-2017". (Tesis posgrado, Universidad Nacional Hermilio Valdizán, Huánuco. 2018).

26. F. Villavicencio Terreros, "Delitos informáticos". *Revista IUS et VERITAS*, 24(49), (2014): 284-304. Obtenido de http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Según Artega (citado por Mori)[27], los delitos informáticos están involucrados de alguna manera en los negocios, incluidos los empleados de confianza, programadores y personas de todo tipo que generalmente tienen acceso material a las instalaciones de procesamiento de datos. Suelen ser empleados de confianza por el tiempo que pasan en la empresa y el tipo de trabajo que realizan allí, y son conscientes de las debilidades del sistema. Aparte de lo anterior, la Internet actual permite que los delincuentes remotos participen como sujetos activos de delitos informáticos que pueden atacar los sistemas de procesamiento de información desde cualquier parte del mundo. La contribución de la criminología al flujo del estructuralismo por parte del sociólogo estadounidense Sutherland muestra la relación entre clase social y crimen en términos de estatus social, comisiones criminales y características de reacción social.

Los sujetos agraviados (sujeto pasivo)

Las víctimas de estos delitos suelen ser personas o entes jurídicas: bancos, compañías de seguros, empresas públicas y privadas, con o sin salvaguardias técnicas. Estas asociaciones no suelen denunciar delitos por miedo a perder su imagen corporativa al descubrir el comportamiento ilegal que están experimentando. No quieren perder su imagen de seriedad, solvencia y seguridad, por lo que prefieren solucionar problemas con medidas internas como despidos y mayor seguridad antes de aceptar sus debilidades. Por supuesto, tal actitud beneficia solo al criminal que continúa sus acciones con la máxima inmunidad, (Magliona, citado por Mori)[28].

Técnicas de ciberdelincuencias

A pesar de la gran cantidad de tecnologías utilizadas por los ciberdelincuentes y el surgimiento continuo de nuevas formas de piratear y eludir las medidas de seguridad del sistema, el analizarlas todas conduciría a la producción de un documento mucho más grande. Se hace una descripción general de los métodos más comunes de la actualidad:

Botnet: Se trata de un conjunto de dispositivos conectados a Internet que el atacante había infectado previamente con *software,* controlando remotamente el dispositivo contra todo tipo de ataques distribuidos de denegación de servicio, sensible o robo de información sensible, etc. Robando cuentas bancarias, datos personales e incluso ciclos de CPU para extraer (minar) criptomonedas[29]. Las *botnets* se han convertido en una de las principales preocupaciones de seguridad en las redes de datos actuales y futuras. Según el reciente "Informe de inteligencia sobre amenazas de Nokia", las *botnets* de

27. F. Mori Quiroz, "Los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, Periodo 2008 al 2012". (Perú: Universidad Nacional Federico Villarreal, 2019). Obtenido de http://repositorio.unfv.edu.pe/handle/UNFV/3519

28. Ibídem.

29. L. Maino Fernández, (2019). *Detección de bonets y ransomware en redes de datos mediante técnicas de aprendizaje automático*. Perú: Universidad de Murcia. Obtenido de http://hdl.handle.net/10201/73765

IoT (Internet of Things) representaron el 78% de los ataques de malware detectados y el 16% de los dispositivos de IoT infectados en 2018[30].

Ransomware: Un malware especialmente problemático que consiste en infectar a uno de los dispositivos de una red gracias a una vulnerabilidad o fallo humano, y llegar al resto de dispositivos por medio de una propagación horizontal basada habitualmente en vulnerabilidades del sistema, tras lo cual cifra todos los datos que contienen sus discos duros y carpetas compartidas y exige una cantidad de dinero para proporcionar la clave de descifrado[31]. Para apreciar el peligro potencial que supone el ransomware, baste mencionar los ataques sufridos por los hospitales del servicio de salud de Reino Unido en 2017, que llegaron a tener que cerrar servicios enteros, enviar pacientes a otros hospitales e incluso posponer intervenciones quirúrgicas[32].

Spoofing: El término Spoofing (robo de información personal) se refiere al uso de técnicas de robo de información personal para interceptar, modificar o ajustar la composición de los mensajes que puedan darse entre diversos sujetos. Puede distinguir entre los siguientes tipos de spoofing sin entrar en detalles:

- *IP Spoofing:* El identificador falso en este caso es en realidad la dirección IP de la tercera entidad que es el origen o destino del paquete. Este método se puede utilizar para obtener acceso no autorizado a los recursos de la red o para controlar su computadora.

- *ARP Spoofing:* El objetivo en este caso es modificar la tabla ARP, es decir, la relación entre la dirección de red (IP) y la dirección física (MAC) del dispositivo de enrutamiento de red para que los paquetes destinados a la víctima puedan ser interceptados. Posteriormente los analiza para otros fines[33].

- *DNS Spoofing:* Se trata de una modificación o manipulación de una o más entradas en la tabla de resolución de nombres del servidor de resolución de nombres (DNS) de dominio-IP. (Rios, 2020)

- *Web Spoofing:* Consiste en destruir parte o la totalidad del sitio web con el fin de interceptar y recopilar la información proporcionada por los usuarios durante la navegación. A diferencia del phishing, este método permite la comunicación entre la víctima y el sitio real. Esto significa que

30. NOKIA, *Nokia Threat Intelligence Report 2019*. Obtenido de https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html

31. L. Maino Fernández, op. cit

32. G. Mohney, (15 de mayo de 2017). *Hospitals remain key targets as ransomware attacks expected to increase.* Obtenido de abc News: https://abcnews.go.com/Health/hospitals-remain-key-targets-ransomware-attacks-expected-increase/story?id=47416989"

33. Ríos Agudelo, C. A. "Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing". (Tesis de maestría. Perú: Instituto Tecnológico Metropolitano, 2020).
Obtenido de http://hdl.handle.net/20.500.12622/4456

los usuarios pueden acceder a su perfil y cuenta mientras el sitio web falso recopila y almacena la información ingresada durante el envío al sitio real.

- *Mail Spoofing:* Se utiliza principalmente en el caso de fraude como un medio para eludir los servicios de seguridad al enviar spam. Este es un método de correo electrónico que simula la confiabilidad requerida para los servicios de seguridad y los destinatarios de correo electrónico, respectivamente. Consiste en alterar algunas o todas las direcciones.

- *GPS Spoofing:* Esta técnica consiste en modificar las señales de satélites oficiales y enviar señales a los receptores GPS, asumiendo que la información proviene de uno de los satélites GPS reales y localiza el dispositivo. Un modo común de operación para este método es cambiar gradualmente la información de ubicación real del sistema y finalmente redirigir a la ubicación deseada.

Ataques Brute Force: suelen estar destinados a la superación de sistemas criptográficos o protegidos por contraseñas. Este ataque consiste en probar todas las posibles llaves (claves/contraseñas); lo cual como es de suponerse en una máquina regular con un único procesador se convierte en una tarea si bien no imposible si poco viable debido al tiempo requerido para obtener resultados[34].

Ataques JavaScript: Algunos de los inconvenientes de las secuencias de comandos entre sitios (XSS para evitar la confusión con las hojas de estilo en cascada) son que un atacante puede usar una aplicación web para entregar código malicioso, generalmente en forma de secuencia de comandos, a otros usuarios. Ocurre durante la transmisión. Esta vulnerabilidad es tan común que es el resultado de una validación o filtrado incorrectos de los datos recuperados de un atacante y transmitidos a un tercero. Específicamente, el lenguaje utilizado para el ataque en este caso es JS (JavaScript)[35].

SQL Injection: El procedimiento de ataque principal es el siguiente. Primero, los datos se ingresan en la aplicación que transfiere los datos de la base de datos, y luego se realiza la intrusión utilizando el comando malicioso presentado en la consulta SQL. Un atacante puede obtener derechos de autenticación sobre la base de datos atacada si acepta la entrada de la aplicación como legítima[36].

Rootkits: El nombre proviene de la aparición de malware en sistemas similares a UNIX donde un atacante obtiene acceso a un usuario privilegiado llamado "root". Este tipo de malware oculta objetos. Por lo tanto, no es completamente peligroso ya que se usa para ocultar evidencia de la presencia de otro

34. Gallegos Chamba, M. J. "Implementación de controles a una aplicación web mediante la metodología owasp para el aseguramiento de su seguridad". (Ecuador: Universidad Técnica de Machala, 2019). Obtenido de http://repositorio.utmachala.edu.ec/handle/48000/13604

35. Briones Pincay, G. H., & Hernández Peñaherrera, E. B. (2018). "Auditoria de Seguridad del Servidor Web de la Empresa PUBLYNEXT S.A. Utilizando Mecanismos Basados en OWASP". Ecuador: Universidad de Guayaquil. Obtenido de http://repositorio.ug.edu.ec/handle/redug/26837

36. Segundo, C. J. (2020). "Hacking web (Análisis de ataques SQL Inyección, XSS)". Colombia: Universidad Nacional Abierta y a Distancia. Obtenido de https://repository.unad.edu.co/handle/10596/31471

malware, como sistemas infectados. Los rootkits utilizan funciones del sistema para actuar como parte del sistema y evitar su detección. Como resultado, el sistema está bajo el control de un atacante y podría ayudar a otros programas maliciosos[37].

Cryptojacking: También llamada Cryptojacking, consiste en la utilización d los sitios web para la realización de la computación necesaria en algoritmos como el PoW (Proof of Work) de forma ilegal y no autorizada. El tipo más común es la minería en el navegador, que utiliza la potencia computacional de los usuarios para resolver los cálculos necesarios. Afectando a las aplicaciones y usuarios[38].

Según la firma de seguridad Eset, el 25,1% de los ataques de ransomware de 2017 se detectaron en Perú. Este es el porcentaje más alto de América Latina. ¿Y cuál es el mayor impacto en los usuarios y empresas peruanas? El consultor ha aprobado los siguientes métodos como los más usados: ransomware, phishing y cryptojacking. El ciberdelito también aprovecha las vulnerabilidades y, en Perú, un tipo de amenaza es EternalBlue. Utilizado para difundir Wannacry en 2017, ha dañado a 12 empresas peruanas en 150 países y ha afectado a más de 200.000 sistemas. Según el National Cyber Security Index de la Fundación e-Governance Academy de Estonia, nuestro país está en el tercer lugar del ranking de América Latina en cuanto a preparación en ciberseguridad (Agencia Peruana de Noticias Andina)[39].

IV. EVOLUCIÓN DE LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS

La posmodernidad trae muchas innovaciones que representan el progreso constante de la humanidad en casi todos los aspectos de las relaciones sociales. El desarrollo constante de la tecnología, la ciencia y la búsqueda constante de nuevos conocimientos de las personas conduce a la creación de una sociedad, un mundo de nuevas relaciones y una nueva sociedad del conocimiento, que son los únicos límites para alcanzar el conocimiento infinito. Siempre que a alguien se le ocurre una invención que transmite sus beneficios o usos, es importante entender que es necesario tomarse un tiempo para ponderar los riesgos y efectos adversos que la invención puede plantear. Frente a la ignorancia natural del descubrimiento, debe haber sabiduría y espacio para la preocupación.

En principio, ha de considerarse que tanto las empresas que conforman el sistema financiero, así como los usuarios, tienen obligaciones que deben cumplir para proteger la contratación electrónica.

Con respecto a las empresas del sistema financiero, el Reglamento de Conducta de Mercado del Sistema Financiero, aprobado por Resolución SBS N°3274-2017, y sus modificatorias, el artículo 49

37. Sosa Fernández, J. T. "Metodología para la elección de software de seguridad informática". Perú: Universidad César Vallejo 2018). Obtenido de https://hdl.handle.net/20.500.12692/31944

38. Luque Lodeiro, R. Blockchain, *Estado del arte, tendencias y retos.* (España: Universidad de Oviedo, 2020). Obtenido de http://hdl.handle.net/10651/56337

39. *Agencia Peruana de Noticias Andina*, 2018. "¿Cuáles son los ciberataques más comunes en el Perú? Empresas peruanas pueden perder su información en 30 minutos". Recuperado el 22 de mayo de 2020, de Portal Andina: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

establece que los contratos realizados mediante mecanismos escritos, como los medios electrónicos, deben poder registrar el consentimiento del cliente. Es responsabilidad de la empresa implementar los mecanismos adecuados para garantizar la seguridad en todas las etapas del contrato, lo que incide en la necesidad de mitigar los riesgos que puedan surgir. Además, la compañía restringe severamente el envío de correos electrónicos a los usuarios para evitar que los atacantes usen correos electrónicos para correos electrónicos falsos. El mecanismo de protección anterior es inadecuado por las siguientes razones:

- **Se enfocan en prevenir la suplantación de identidad**. En efecto, la norma actualmente busca garantizar que el contratante no sea suplantado por un tercero para lo cual exige mecanismos de autenticación de la identidad. Empero, ese no es el único tipo de delito informático que puede afectar la contratación electrónica. Los criminales también suplantan el sitio web de las entidades para robar información de acceso a las cuentas bancarias (phishing) o realizan ataques para robar la información de tarjetas de créditos de los clientes (acceso ilícito a sistemas informáticos).

- **Son meramente preventivos.** Inciden en el ex ante más no en el ex post, cuando la evidencia recogida revela que a menudo estos mecanismos de protección son quebrantados por el accionar delictivo.

El primer antecedente normativo que regula los delitos informáticos en el Perú se encuentra asentada en la Ley N° 27309; esta norma jurídica (Congreso del Perú, 2000) modificó el Título V del Libro Segundo del Código Penal vigente, incorporando el Artículo 207-A que tipifica la siguiente conducta ilícita "El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privada de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos [sic] a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de dos años y con prestación de servicios comunitarios no menor de ciento cuatro jornadas".

El supuesto contemplado en el artículo 207-A citado previamente, se focaliza en la actividad ilegal consistente en ataques a sistemas de información, pero con una descripción limitada en cuanto a sus variantes; en efecto, en los últimos años la ciberdelincuencia ha ampliado su accionar y la finalidad de dicho accionar. La norma descrita alude al siguiente accionar: "interferir", "interceptar", "acceder" o "copiar" información; hoy, en cambio, el delincuente, además de eso, "modifica", "destruye", "inserta" e "impide" el uso de datos en los sistemas de información.

En el año 2013 se publicó en nuestro país la Ley Nº 30096, "Ley de Delitos Informáticos" (Congreso del Perú, 2013), tuvo como objetivo prevenir y sancionar los sistemas y datos informáticos, la compensación y la libertad sexual, la privacidad y confidencialidad de los mensajes, la propiedad y la confianza pública, y la actividad ilegal que afecte a los delincuentes que utilizan la última tecnología

y hacer un acto tan ilegal. Dicha norma, aunque tuvo como referencia el Convenio de Budapest, recibió muchas críticas porque su tenor ambiguo podía derivar en el perjuicio a ciudadanos que no incurrían en un accionar delictivo, especialmente porque los supuestos que numeraba no precisaban la intencionalidad del agente.

La norma fue modificada por la Ley Nº 30171, en el año 2014. Según esta ley, el acceso no autorizado (artículo 2), los ataques a la integridad de los datos y los sistemas informáticos (artículos 3 y 4), la interceptación de datos informáticos (artículo 7) y el fraude informático (artículo 8), etc. Además, el uso indebido de maquinaria y equipo informático (artículo 10) confirma la frase "intencionalmente y viola la ley", confirma que se ha cometido un delito y constituye un intercambio de datos fraudulento. Se canceló el artículo 6 de tráfico ilegal de datos.

Asimismo, las proposiciones a niños, niñas y adolescentes con fines sexuales que busquen y reciban material pornográfico y mantengan relaciones sexuales utilizándolos, tendrá una pena de entre 4 y 8 años. Será castigado en virtud del artículo 36, artículos 1, 2 y 4 del Código Penal. Si la víctima tiene de 14 a 18 años, la pena es de 3 a 6 años y será impuesta en virtud del artículo 36, en sus numerales 1, 2 y 4 del Código Penal. Por ello, los legisladores han incluido en su reglamento acciones que se refieren a engañar a menores para los denominados propósitos de cortejo-sexual.

Además, si el delito está dentro del alcance de la Ley 27806- Ley de Transparencia y Acceso a la Información Pública, es decir si se da una manipulación, modificación, introducción, etc. de la información clasificada como confidencial, reservada o confidencial, está sujeta a una pena de prisión de 5 a 8 años. Si el delito pone en peligro la defensa, la seguridad o la soberanía nacionales, la pena es de entre 8 y 10 años. Además, para las bandas criminales, las multas son un tercio más altas que los límites legales previstos en casos anteriores.

Con el fraude informático consiste en dañar intencional e ilegalmente a un tercero mediante el desarrollo, introducción, modificación, eliminación, eliminación, duplicación o destrucción o manipulación de datos informáticos. El fraude informático mediante sistemas informáticos puede resultar en una pena de prisión de 3 a 8 años y una multa de 60 a 120 días. Las sanciones incluyen de 5 a 10 años de prisión, 80 a 140 días multas si la propiedad pública asignada a un programa de seguridad o asistencia sociales se ve afectada.

Finalmente, el artículo 10 de la ley se sancionará el fabricar, diseñar, desarrollar, vender, publicitar, distribuir, importar o fabricar una o más máquinas, programas informáticos, dispositivos, contraseñas, códigos de acceso u otros datos informáticos diseñados específicamente para violar las normas y artículos establecidos en las leyes ya mencionadas. Igualmente se sancionará a la persona que adquiera, ofrezca o preste algún servicio que pueda llegar a contribuir a dichos actos ilícitos, con una pena de prisión no menor de 1 año ni mayor a 4 años y de 30 a 90 días-multa.

Díaz[40] menciona cuáles serían las acciones más urgentes por tomar para que el usuario sea consciente de los peligros en internet y que los proveedores de aplicaciones aseguren mejor los canales de atención digital:

- "Concientizar a los altos directivos públicos y privados sobre la importancia de aplicar medidas de ciberseguridad."
- "Capacitar a ingenieros en seguridad tecnológica, protocolos, criptografía, desarrollo seguro, infraestructura segura con perfiles definidos y especializados."
- "Concientizar al ciudadano sobre los riesgos de navegar por internet."
- "Capacitar a las áreas de auditoría y darles herramientas para evaluar de forma técnica la efectividad de las medidas de seguridad."
- "Desarrollar o adquirir tecnologías de seguridad adecuadas al nivel de riesgo de cada organización."
- "Definir e implementar estrategias de ciberseguridad en las organizaciones, para responder ante ataques más sofisticados como Advanced Persistent Threats (APT)."
- "Otorgar los recursos necesarios a los oficiales de seguridad para implementar controles."
- "Contratar proveedores especializados para investigar los intentos de ataque *Threat Hunting* y realizar evaluaciones de seguridad *Ethical Hacking*."

En el entorno supranacional, es importante mencionar que, como iniciativa de la lucha contra la ciberdelincuencia para lograr la seguridad digital de los ciudadanos y empresas en el Perú, el Congreso de la República aprobó la propuesta del Poder Ejecutivo para garantizar la adhesión del Perú al Convenio contra la Ciberdelincuencia o Convenio de Budapest. La suscripción se aprobó el 30 de febrero del 2019 (Presidencia del consejo de ministros, 2019)[41]. El convenio de Budapest (2001) fue el primer acuerdo sobre delitos cometidos a través de Internet y otros sistemas informáticos, en el que se buscó adoptar herramientas de derecho penal y judicial para proteger al público del ciberdelito, así como la cooperación internacional en el campo de la justicia.

El Convenio mencionado tiene por objeto optimizar la regulación interna en materia de ciberseguridad, con mayor énfasis en materia penal, de tal manera que sus organismos correspondientes puedan tener mayor capacidad para poder perseguir este tipo de delitos, tales como el fraude informático,

40. R. Díaz, *El crecimiento de la ciberdelincuencia*, op.cit.

41. Presidencia del Consejo de Ministros. Perú se adhiere al Convenio de Budapest para luchar contra la ciberdelincuencia. Disponible en:
http://www.pcm.gob.pe/2019/02/peru-se-adhiere-al-convenio-de-budapest-para-luchar-contra-la-ciberdelincuencia/

la interceptación ilícita y otros; siendo la tarea entonces, diseñar un enfoque de regulación predecible, proporcionado y basado en riesgos. Es decir, los Estados deben asumir y resolver el reto que implica tener un marco regulatorio específico y predecible que garantice la estabilidad y la protección de los intereses de los usuarios; así como tener un marco regulatorio abierto y flexible, que promueva la innovación y la inclusión financiera.

En el contexto del Convenio de Budapest, el Poder Judicial peruano sugiere invertir mayor presupuesto y dotar de mejores instrumentos y equipos de alta tecnología a las instituciones vinculadas al servicio de administración de justicia – Policía Nacional del Perú, Ministerio Público y Poder Judicial, con el fin de continuar con los trabajos de apoyo y coordinación entre ellas, buscando el desarrollo de aquellas actividades preparatorias de trabajo y coordinación conjunta, que lleve a fortalecer y afianzar las relaciones administrativas, investigativas y judiciales debidamente planificadas y organizadas (Poder Judicial).

En esa línea, mediante Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN, se creó la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, la cual, aunque a la fecha tiene recursos limitados – está a cargo de un (01) Fiscal Superior y el apoyo de dos (02) Fiscales Adjuntos Superiores-, tiene por objeto conformar la "Red de fiscales en ciberdelincuencia a nivel nacional", brindando una viabilidad efectiva al Convenio de Budapest o Convenio sobre la Ciberdelincuencia.

En base a lo expuesto, se presenta el análisis sobre la capacidad de la regulación contra los delitos informáticos en aras de proteger la contratación electrónica; la cual ha sido obtenida mediante revisión bibliográfica y de análisis documental; asimismo, se ha comparado la regulación de países como España, Estados Unidos, Chile y Colombia; considerando que dichos países suscribieron el convenio de Budapest con anterioridad a Perú.

V. LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO

Argentina

"Legislación: Código Penal, Ley 26.388 (2008), Ley 25.326 (2000). A partir de junio de 2008, la Ley 26.388 conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388."

Bolivia

"Legislación: Código Penal, Ley 1.768 (1997), Ley 3325 (2006). La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de DELITOS INFORMÁTICOS. Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos."

Brasil

"Legislación: Ley 12.737 (2012), Ley 11.829 (2008). La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet."

Chile

"Legislación: Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002). La Ley 19.223 es una ley "Relativa a Delitos Informáticos" de acuerdo con su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación."

Colombia

"Legislación: Ley 1.273 (2009), Ley 1366 (2009). La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos"."

Costa Rica

"Legislación: Ley 9.048 (2012). La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la

Ley Nº 4573. Por otro lado, adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo Delitos informáticos y conexos, donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231)."

Cuba

"Legislación: Resolución 204/96, Resolución 6/96, Decreto Ley 199/99, Ley de Soberanía Nacional. En este país se ha podido acceder a la Resolución 204/96, la cual dispone el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, junto a la Resolución 6/96 que pone en vigor el Reglamento sobre la Seguridad informática, con medidas establecidas para la protección y seguridad del Secreto Estatal. Por otro lado, el Decreto Ley 199/99 define como objetivo fundamental establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial. Si bien no existe legislación específica para delitos informáticos, se han encontrado distintas posturas en la doctrina. Por un lado, se opina sobre la necesidad de regulación especial en la materia, y por otro se considera que por la forma en que están redactados algunos delitos y por la filosofía del Código cubano de sancionar por los valores atacados y por los medios empleados, los tipos penales ya existentes son aplicables."

Ecuador

"Legislación: Ley Nº 67/2002 (2002). La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado DE LAS INFRACCIONES INFORMÁTICAS, el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos."

El Salvador

"Legislación: Decreto 1030 / 1997 (1997). No se ha encontrado legislación específica en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos, se pueden mencionar los artículos siguientes: 172, 185, 186, 190, 208 No.2, 216, 222 No. 2, 228, 230, 231 y 302 del Código Penal de El Salvador."

Honduras

"Legislación: Código Penal; Decreto 144/83. Si bien no se ha encontrado legislación especial en la materia, si posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del art. 149 y sus incisos al Código Penal."

México

"Legislación: Reforma 75 del Código Penal Federal (1999). Mediante reformas se crearon en el Código Penal Federal, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo."

Panamá

"Legislación: Código Penal y sus reformas; Ley 51 (2008). No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cual se regula penalmente sobre la falsificación de documentos."

Paraguay

"Legislación: Código Penal – Ley 1.160 (1997), Ley 2.861. No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249."

Perú

"Legislación: Ley 27.309 (2000), Ley 28.251 (2004). La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además, Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo, en la misma no incluye ningún tipo de sanción penal."

Puerto Rico

"Legislación: Ley 146/2012 (Código Penal), Ley de Espionaje Cibernético 1165 (2008). No se ha encontrado legislación especial al respecto. Sin embargo, Puerto Rico ha optado por la modificación de los tipos penales clásicos, a fin de adaptarlos para su comisión a través de las nuevas tecnologías. Por otro lado, a través de la Ley de Espionaje Cibernético Nº 1165/2008 si se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje."

República Dominicana

"Legislación: Ley Nº 53-07 (2007). Posee una Ley Especial contra Crímenes y Delitos de Alta Tecnología. Dicha norma regula una parte general, conteniendo algunos principios y conceptos, y posteriormente tipifica los delitos informáticos según el bien jurídico afectado. Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos."

Uruguay

"Legislación: Ley 18.600 (2009), Ley 17.520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009). Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales, permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación."

Venezuela

"Legislación: Gaceta Oficial Nº 37.313 (2001). Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico"

VI. PROTECCIÓN AL CONSUMIDOR

En el Perú la regulación de una normativa exclusiva para el Comercio Electrónico a un no es una realidad, a diferencia de la Ley electrónica de España, Chile y Ecuador que sí cuentan con una legislación para la protección del Consumidor. En Perú, el Comercio Electrónico aún se encuentra en desarrollo y da índices de un crecimiento potencial año a año. Además, los dos grandes problemas que obstaculizan el desarrollo y crecimiento del comercio electrónico son (i) la falta de difusión de sus ventajas y (ii) la falta de confianza en este tipo de transacciones.

Empero, este crecimiento se acelera día a día con los avances tecnológicos, y existe una necesidad urgente de regular las normas de protección al consumidor electrónico, las reglas de los contratos electrónicos, los requisitos de integridad de los contratos y, sobre todo, las obligaciones de los proveedores. De hecho, si bien, no existen leyes; lo cierto es que se cuenta con la Ley N° 29571 "Ley de protección y protección de los derechos del consumidor" que, aunque regula los derechos, principios y obligaciones básicos de los consumidores peruanos, también, exige reglas especiales aún no adoptadas. A diferencia

de las leyes electrónicas chilenas y ecuatorianas que se aplican a los países de América Latina, estas han logrado grandes avances en la regulación del comercio electrónico a través de leyes para proteger los contratos electrónicos y han ayudado a la economía. Ha crecido exponencialmente. Asimismo, la Ley N° 27269 "Ley de Certificados y Firmas Digitales", no regula necesariamente la protección de los consumidores electrónicos, sino regula las reglas de autenticación de documentos virtuales.

Un claro ejemplo es lo sucedido hoy en día; pues en el contexto de la pandemia, el coronavirus ha dejado en evidencia la vulnerabilidad de la sociedad. No es casualidad que los gobernantes más proteccionistas hayan merecido el aplauso popular. Ello refuerza la necesidad de proteger la contratación digital en el Perú, dado que ofrece ventajas para realizar pagos y transferencias, sin perjuicio de un esfuerzo educativo para que más personas conozcan los riesgos asociados a la tecnología, lo que conllevaría a, entre otros, no prestar atención a correos ni mensajes sospechosos y/o corroborar la veracidad de los mensajes recibidos con la entidad a través de sus canales oficiales. De febrero a marzo del 2020, se detectó un aumento del 117% en este tipo de estafa en el Perú. El crecimiento está directamente relacionado con los numerosos mensajes maliciosos que circulan en WhatsApp aprovechando el interés del público sobre la pandemia del coronavirus (Covid-19). Los cibercriminales van adaptando sus estafas diariamente y envían mensajes muy convincentes. (Diario Gestión, 2020)

El estado debe garantizar la protección al consumidor dado que el mismo protege la salud y seguridad de los consumidores a través de una normativa apropiada y actualizada (las diferentes leyes ya mencionadas), fomentando la participación de todos los estamentos públicos o privados. Para tal efecto, promueve el establecimiento de las normas reglamentarias para la producción y comercialización de productos y servicios y fiscaliza su cumplimiento a través de los organismos competentes. En esa línea, en el año 2021 el Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual ha presentado el documento "Propuestas para la protección del consumidor en el comercio electrónico y la seguridad de producto" (Indecopi, 2021), el cual, busca establecer un estándar mínimo de cumplimiento en las transacciones realizadas a través de canales digitales y su ejecución, así como garantizar la seguridad de los consumidores mediante el fortalecimiento de las instituciones y las medidas a adoptar frente al posible ingreso al mercado de productos de consumo que pueden representar un riesgo para los consumidores y reformular aspectos relacionados con el reconocimiento y allanamiento de las pretensiones a fin de incentivar la solución de controversias sin la necesidad de que se inicie un procedimiento administrativo sancionador.

VII. CONCLUSIONES

- No queda duda que actualmente, es posible acceder a los servicios financieros por canales virtuales, los cuales abren un abanico de ventajas tales como: permitir la contratación fácil y rápida; abaratar los costos; y, facilitar la inclusión financiera; tampoco queda duda de que urge mecanismos para hacer frente a los retos que plantea poseer un ecosistema digital. Siendo una de las medidas adoptadas, mediante (Congreso de la República, 2019) de fecha 13 de febrero, la aprobación del Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001.

- De la bibliografía revisada, actualmente, si bien existe cierta regulación del ciberdelito este no está cerca de ser completamente eficaz para poder proteger a los usuarios que tengan contratos electrónicos, resaltando que el Perú apenas pasa la media superior de los países que tienen más desarrollo digital e implementación de ciberseguridad, ocupando el lugar 78 de 160, agregando que tenemos una brecha negativa del 5.83 entre el desarrollo digital peruano y ciberseguridad nacional. Ver anexo*. (Tabla 1).

- Los estudios revisados no representan ni precisan una carencia ni alternativa a las deficiencias de las actuales normativas legales lo que supone un breve estancamiento momentáneo al desarrollo del comercio electrónico, específicamente en el ámbito de las contrataciones electrónicas, puesto que las regulaciones actuales no son suficientes.

- Las actuales regulaciones no están lo suficientemente precisadas como para ser de completa confianza para el público en general lo cual a largo y corto plazo genera desconfianza, una clara recomendación a este problema es el incentivar las propuestas de regulaciones legales que puedan presentarse teniendo en cuenta el futuro desarrollo que estas puedan traer a nuestro país.

- La ciberdelincuencia en el contexto actual de la pandemia está en auge; por ello, importa agilizar el desarrollo e implementación de sistemas de seguridad más fiables; lo que permitirá estar más actualizados frente a las amenazas más comunes de ataques informáticos, lo que redundará en la disminución de futuros brotes de ciberdelincuencia, impulsando así la confianza de los usuarios hacia las contrataciones electrónicas

- El público por lo general desconoce la protección ofrecida por los contratos electrónicos (independientemente del grado de protección que los mismos provean); el impulsar una cultura de desarrollo en informática para ampliar el limitado conocimiento de los clientes con respecto a la existencia de productos digitales, así como a sus ventajas, siendo de especial mención el hecho que el uso de canales y servicios financieros digitales haya resultado tan bueno en la coyuntura del Covid-19, al permitir la contratación de forma segura, rápida, evitando traslados y aglomeración de personas. A la par, también debe informárseles en torno a las consideraciones aquí descritas para atenuar riesgos en la contratación electrónica.

- Algunas prácticas adecuadas desde el punto de vista de las empresas financieras son: i) mecanismos de autenticación de clientes; y, ii) emplear sistemas de inteligencia que detecten amenazas de *malware y bots*; ahora bien, prácticas desde el punto de vista de los consumidores financieros son: i) verificar el URL de las páginas web en las que navega; ii) evitar interactuar en páginas y/o con documentos sospechosos; y, iii) tener máximo cuidado con instrucciones enviadas por correo electrónico. Al implementar estos de manera más recurrente es que se puede dar más confianza a las regulaciones contra la ciberdelincuencia.

REFERENCIAS

- Agencia Peruana de Noticias Andina. "¿Cuáles son los ciberataques más comunes en el Perú?" Empresas peruanas pueden perder su información en 30 minutos. 2018. Recuperado el 22 de mayo de 2020, de Portal Andina: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

- Alliance for Financial Inclusion, 30 de setiembre de 2011. "El compromiso con la inclusión financiera por parte de la red de la AFI". Obtenido de Declaración Maya: https://www.afi-global.org/sites/default/files/publications/2017-04/Maya%20Declaration_SP.pdf

- Andina- Agencia Peruana de Noticias, 23 de enero de 2019. "Perú se suscribe a convenio de Budapest en materia de ciberseguridad y ciberdefensa". Obtenido de https://andina.pe/agencia/noticia-peru-suscribira-convenio-budapest-materia-ciberseguridad-y-ciberdefensa-740180.aspx

- Blossiers Mazzini, J. J. "El delito informático y su incidencia en la empresa bancaria". Tesis grado de Maestro. Universidad Nacional Federico Villarreal, Lima 2018. Obtenido de file:///C:/Users/Angely/Downloads/UNFV_BLOSSIERS_%20MAZZINI_%20JUAN%20_JOS%C3%89_MAESTRIA_2018.pdf

- Briones Pincay, G. H., & Hernández Peñaherrera, E. B. *Auditoria de Seguridad del Servidor Web de la Empresa PUBLYNEXT S.A. Utilizando Mecanismos Basados en OWASP.* Ecuador: Universidad de Guayaquil 2018 . Obtenido de http://repositorio.ug.edu.ec/handle/redug/26837

- Brunet, J. M. "La Fiscalía denuncia el "imparable" aumento de delitos informáticos". 7 de septiembre de 2020. Obtenido de *El País*: https://elpais.com/espana/2020-09-07/la-fiscalia-denuncia-el-imparable-aumento-de-delitos-informaticos.html

- Bustamante Gavilano, J. J. "La función pública notarial en la contratación electrónica en Lima Metropolitana 2017". Perú: Tesis para optar el título profesional de Abogado. Universidad César Vallejo. Obtenido de http://repositorio.ucv.edu.pe/bitstream/handle/UCV/15116/Bustamante_GJJ.pdf?sequence=1&isAllowed=y

- Cabrejos Valdez, G. B., & Guerrero Ortiz, T. Y. (2018). "Perfeccionamiento del contrato electrónico en el Perú como medida de protección jurídica del consumidor". Tesis para optar título profesional. Universidad Señor de Sipán, Perú. Obtenido de https://hdl.handle.net/20.500.12802/4431

- Cancillería de Colombia, 25 de junio de 2018. Congreso de Colombia aprobó ley de adhesión a la Convención de Budapest (20-06-2018). La propuesta del gobierno pasó los cuatro debates y entrará a sanción presidencial. Colombia. Obtenido de https://www.cancilleria.gov.co/newsroom/news/congreso-colombia-aprobo-ley-adhesion-convencion-budapest-20-06-2018-propuesta

- Carranco, R. "Detenido por instalar un programa espía en el móvil de su expareja" (04 de junio de 2019). *El País.* (E. País, Ed.) Recuperado el 22 de julio de 2019, de https://elpais.com/ccaa/2019/06/04/catalunya/1559645979_609180.html

- Carrillo Díaz, C. F., & Montenegro Dávila, A. N. (2018). "La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos". Perú: Tesis para título de Abogado. Obtenido de http://repositorio.uss.edu.pe/bitstream/handle/uss/4514/Carrillo%20Diaz%20%26%20Montenegro%20Davila.pdf?sequence=1&isAllowed=y

- Congreso de la República, 28 de mayo de 2000. "Ley N° 27269: Ley de firmas y certificados digitales". Obtenido de *El Peruano:* https://cdn.www.gob.pe/uploads/document/file/356833/NORMA_1887_LEY_27269_Modificada_por_LEY_27310.pdf

- Congreso de la República, 27 de julio de 2017. "LEY Nº 30618". Obtenido de *El Peruano:* https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/

- Congreso de la República, 21 de agosto de 2017. "Resolución SBS Nº 3274-2017: Reglamento de gestión de conducta de mercado del Sistema Financiero". Obtenido de *El Peruano*: http://ima01.gestion.pe/doc/0/0/2/4/3/243991.pdf

- Congreso de la República, 13 de febrero de 2019. "Resolución Legislativo N°30913: Resolución Legislativa Que Aprueba El Convenio Sobre La Ciberdelincuencia". Obtenido de *El Peruano*: https://busquedas.elperuano.pe/normaslegales/resolucion-legislativa-que-aprueba-el-convenio-sobre-la-cibe-resolucion-legislativa-n-30913-1740637-2/

- Congreso de la República. (s.f.). "Política Nacional de ciberseguridad". Obtenido de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf

- Congreso del Perú, 17 de julio de 2000. "Ley N° 27309: Ley que incorpora los delitos informáticos al código penal". Obtenido de *El Peruano:* https://cdn.www.gob.pe/uploads/document/file/356824/NORMA_1887_Ley_27309.pdf

- Congreso del Perú, 22 de octubre de 2013. "Ley N° 30096: Ley de delitos informáticos". Obtenido de *El Peruano:* https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/
- Congreso del Perú, 10 de marzo de 2014. "Ley N°30171 : Ley que modifica la Ley N° 30096, Ley de delitos informáticos". Obtenido de *El Peruano:* http://www.mef.gob.pe/contenidos/servicios_web/conectamef_quechua/pdf/normas_legales_2012/NL20140310.pdf
- Criminal Defense Issues, 2018. "Computer Fraud and Abuse Act (CFAA)". Obtenido de https://www.nacdl.org/cfaa/
- Daccach, J. C. , 2019. "Ley de los delitos informáticos en Colombia". Obtenido de *Delta Asesores*: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/
- "Defraudadores tienen en la mira a 76,000 clientes del sistema financiero", 28 de junio de 2017. Obtenido de *Diario Gestión:* https://gestion.pe/economia/defraudadores-mira-76-000-clientes-sistema-financiero-138258
- "Ciberataques a dispositivos móviles en Perú se duplicaron en marzo", 9 de abril de 2020. Obtenido de *Diario Gestión:* https://gestion.pe/peru/ciberataques-a-dispositivos-moviles-en-peru-se-duplicaron-en-marzo-noticia/
- "Ciberataques: cinco claves para evitar ser una víctima en época de cuarentena", 21 de abril de 2020. Obtenido de *Diario Gestión:* https://gestion.pe/tendencias/ciberataques-cinco-claves-para-evitar-ser-una-victima-en-epoca-de-cuarentena-noticia/
- "Coronavirus: capturan a banda que obtuvo $25 000 tras robar bonos de S/380 por internet", 26 de marzo de 2020. Obtenido de *Diario La República:* https://larepublica.pe/sociedad/2020/03/26/coronavirus-en-peru-capturan-a-banda-que-obtuvo-25-000-dolares-tras-robar-bono-de-s380-por-internet-video/
- Díaz, R. *El crecimiento de la ciberdelincuencia*, 2019. Recuperado el 22 de mayo de 2020, de Conexión ESAN: https://www.esan.edu.pe/conexion/actualidad/2019/10/03/el-crecimiento-de-la-ciberdelincuencia/
- Fernández Maimó, L. *Detección de bonets y ransomware en redes de datos mediante técnicas de aprendizaje automático*. 2019. Universidad de Murcia. Obtenido de http://hdl.handle.net/10201/73765

- Gallegos Chamba, M. J." Implementación de controles a una aplicación web mediante la metodología owasp para el aseguramiento de su seguridad", 2019. *Ecuador: Universidad Técnica de Machala*. Obtenido de http://repositorio.utmachala.edu.ec/handle/48000/13604
- Gartner research, 2017. *Seize the digital ecosystem opportunity.* Disponible en: https://www.gartner.com/imagesrv/cio/pdf/Gartner_CIO_Agenda_2017.pdf
- Indecopi, 2021. *Propuestas para la protección del consumidor en el comercio electrónico y la seguridad de productos*. Disponible en: https://www.gob.pe/institucion/indecopi/informes-publicaciones/1783379-propuestas-para-la-proteccion-del-consumidor-en-el-comercio-electronico-y-la-seguridad-de-productos
- Koch, T. ,05 de 04 de 2019. "Aumenta el consumo legal "on line" de cultura, según un informe de la industria". *El País.* Recuperado el 22 de julio de 2019.
- "Asbanc confirma que ataque financiero mundial afectó al Perú", 17 de agosto de 2018. Obtenido de *La República:* https://larepublica.pe/economia/1300366-asbanc-bancos-peru-sufrieron-ataques-ciberneticos/
- Luque Lodeiro, R. *Blockchain: Estado del arte, tendencias y retos*. España: Universidad de Oviedo, 2020. Obtenido de http://hdl.handle.net/10651/56337
- Mars, A. "El ciberataque que exhibió la fragilidad de Estados Unidos", 16 de mayo de 2021. Obtenido de *El País:* https://elpais.com/internacional/2021-05-15/el-ciberataque-que-exhibio-la-fragilidad-de-estados-unidos.html
- Mendoza Riofrío, M. "Fortinet: Se eleva la incidencia de ataques a bancos en Perú", 31 de julio de 2018, *El Comercio*. Recuperado el 22 de julio de 2019, de https://elcomercio.pe/economia/negocios/fortinet-eleva-incidencia-ataques-bancos-peru-noticia-540432
- Mohney, G. *Hospitals remain key targets as ransomware attacks expected to increase*, 15 de mayo de 2017. Obtenido de abc News: https://abcnews.go.com/Health/hospitals-remain-key-targets-ransomware-attacks-expected-increase/story?id=47416989
- Mori Quiroz, F. "Los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, Periodo 2008 Al 2012". Perú: Tesis de maestria. Universidad Nacional Federico Villarreal, 2019. Obtenido de http://repositorio.unfv.edu.pe/handle/UNFV/3519
- NOKIA. *Nokia Threat Intelligence Report 2019*. Obtenido de https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html
- Notaria Rodríguez Velarde. *La contratación electrónica.* 5 de agosto de 2018. Obtenido de: https://rodriguezvelarde.com.pe/2018/08/05/la-contratacion-electronica/

- Peña Jiménez, Y. J. *Comercio electrónico ventajas y desventajas.* Bogotá, Colombia: Universidad Cooperativa de Colombia, 2019. Obtenido de http://hdl.handle.net/20.500.12494/16999

- Poder Judicial, marzo de 2019. *Tratamiento judicial del ciberdelito*. Obtenido de Oficina de las Naciones Unidas contra la Droga y el Delito: http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Peru_2.pdf

- Presidencia del consejo de ministros, 01 de febrero de 2019. *Perú se adhiere al Convenio de Budapest para luchar contra la ciberdelincuencia*. Obtenido de http://www.pcm.gob.pe/2019/02/peru-se-adhiere-al-convenio-de-budapest-para-luchar-contra-la-ciberdelincuencia/

- Rios Agudelo, C. A. "Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing". Tesis de maestría. Instituto Tecnológico Metropolitano, Colombia 2020. Obtenido de http://hdl.handle.net/20.500.12622/4456

- Rodríguez, R. "Unos hackers tienen secuestrada una ciudad entera de EEUU desde hace dos semanas". Obtenido de *El Confidencial* 23 de mayo de 2019: https://www.elconfidencial.com/tecnologia/2019-05-23/baltimore-secuestro-hackers-ransomware-robinhood_2018306/

- Segundo, C. J. "Hacking web (Análisis de ataques SQL Inyección, XSS)". Colombia: Universidad Nacional Abierta y a Distancia, 2020. Obtenido de https://repository.unad.edu.co/handle/10596/31471

- Sosa Fernández, J. T. "Metodología para la elección de software de seguridad informática". Tesis para optar el titulo profesional. Universidad César Vallejo, Perú, 2018. Obtenido de https://hdl.handle.net/20.500.12692/31944

- Soto Coaguila, C. "La contratación electrónica: los supuestos «contratos informáticos» y los contratos celebrados a través de medios electrónicos". *Derecho PUCP,* 55, (2002): 181-221. https://doi.org/10.18800/derechopucp.200201.009

- Superintendencia de Banca, Seguros y AFP de Perú. *Encuesta de medición de capacidades financieras de perú* 19 de Julio de 2019. Obtenido de Superintendencia de Banca, Seguros y AFP de Perú: https://www.sbs.gob.pe/inclusion-financiera/cifras/encuestas

- Valderrama Chevarría, J. G. "¿Se puede legislar la contratación electrónica y ser tutelada a través de la función notarial?: una nueva necesidad a raíz de la COVID 19". 7 de mayo de 2020. Obtenido de *La Ley*: https://laley.pe/art/9678/se-puede-legislar-la-contratacion-electronica-y-ser-tutelada-a-traves-de-la-funcion-notarial-una-nueva-necesidad-a-raiz-de-la-covid-19

- Vilca Morales, L. E. "La formación profesional en derecho informático y la persecución penal de delitos informáticos en el Distrtito Judicial de Huánuco-2017". Tesis para optar el título de Abogado. Universidad Nacional Hermilio Valdizán, Perú, 2018. Obtenido de http://repositorio.unheval.edu.pe/bitstream/handle/UNHEVAL/3908/TD00114V65.pdf?sequence=1&isAllowed=y

- Villavicencio Terreros, F. "Delitos imformáticos". *Revista IUS et VERITAS*, 24,49, (2014): 284-304. Obtenido de http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

- Ydrogo Gavidia, R. N., 2018. *El derecho a la información del consumidor en la contratación electrónica en el Perú 2016-2017*. Obtenido de file:///C:/Users/Angely/Downloads/Ydrogo_GRN.pdf

RECIBIDO: 03/08/2021

APROBADO: 20/10/2021

ANEXO

- * De la bibliografía revisada, actualmente, si bien existe cierta regulación del ciberdelito este no está cerca de ser completamente eficaz para poder proteger a los usuarios que tengan contratos electrónicos (Ver tabla 1).

Tabla n°. 1: Índice de Nivel de protección en delitos informáticos en el mundo

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1	Greece	96.1	63.75	32.35
2	Czech Republic	92.21	68.96	23.25
3	Estonia	90.91	75.86	15.05
4	Portugal	89.61	67.85	21.76
5	Lithuania	88.31	68.3	20.01
6	Spain	88.31	72.61	15.7
7	Poland	87.01	65.35	21.66
8	Belgium	85.71	74.39	11.32
9	Finland	85.71	79.48	6.23
10	France	84.42	77.79	6.63
11	Denmark	84.42	84.64	-0.22
12	Saudi Arabia	83.12	62.34	20.78
13	Croatia	83.12	64.17	18.95
14	Slovakia	83.12	65.69	17.43
15	Netherlands	81.82	83.14	-1.32
16	Germany	80.52	80.69	-0.17
17	Malaysia	79.22	62.61	16.61
18	United States	79.22	80.36	-1.14
19	Serbia	77.92	59.53	18.39
20	United Kingdom	77.92	81.39	-3.47
21	Italy	76.62	67.04	9.58
22	Switzerland	76.62	83.91	-7.29
23	Ukraine	75.32	52.81	22.51
24	Bulgaria	74.03	61.81	12.22
25	Romania	71.43	59.48	11.95
26	Latvia	71.43	66.54	4.89
27	Singapore	71.43	80.94	-9.51
28	Austria	68.83	76.56	-7.73

29	Korea (Republic of)	68.83	81.55	-12.72
30	Canada	66.23	76.31	-10.08
31	Australia	66.23	78.74	-12.51
32	Thailand	64.94	55.08	9.86
33	Russian Federation	64.94	62.46	2.48
34	Hungary	64.94	64.68	0.26
35	Israel	64.94	74.31	-9.37
36	Philippines	63.64	46.33	17.31
37	Japan	63.64	78.92	-15.28
38	Ireland	62.34	76.16	-13.82
39	Luxembourg	62.34	79.99	-17.65
40	Norway	62.34	82.04	-19.7
41	Bangladesh	59.74	30.66	29.08
42	India	59.74	35.94	23.8
43	Chile	59.74	59.88	-0.14
44	Paraguay	57.14	41.46	15.68
45	Slovenia	57.14	70.19	-13.05
46	Sweden	57.14	83.43	-26.29
47	North Macedonia	55.84	54.19	1.65
48	Qatar	55.84	66.18	-10.34
49	New Zealand	55.84	78.29	-22.45
50	Iceland	55.84	80.18	-24.34
51	Benin	54.55	25.83	28.72
52	Nigeria	54.55	28.22	26.33
53	Turkey	54.55	56.02	-1.47
54	Dominican Republic	53.25	45.44	7.81
55	Costa Rica	53.25	58.28	-5.03
56	Belarus	53.25	62.33	-9.08
57	Georgia	51.95	52.93	-0.98
58	Uganda	50.65	26.65	24
59	Moldova (Republic of)	50.65	55.79	-5.14
60	Malta	50.65	72.66	-22.01
61	Kenya	49.35	36.16	13.19
62	Bosnia and Herzegovina	49.35	47.81	1.54
63	Panama	48.05	46.92	1.13
64	Albania	48.05	47.81	0.24
65	Mauritius	48.05	54.31	-6.26
66	Argentina	48.05	59.13	-11.08
67	Uruguay	48.05	63.24	-15.19
68	Tunisia	46.75	44.75	2

69	Colombia	46.75	50.21	-3.46
70	Brazil	46.75	55.89	-9.14
71	Kazakhstan	45.45	59.64	-14.19
72	Pakistan	42.86	28.74	14.12
73	Sri Lanka	42.86	40.88	1.98
74	Zambia	41.56	27.97	13.59
75	Jamaica	41.56	47.88	-6.32
76	Brunei Darussalam	41.56	67.5	-25.94
77	Cyprus	41.56	69.19	-27.63
78	Peru	40.26	46.09	-5.83
79	United Arab Emirates	40.26	68.26	-28
80	Indonesia	38.96	45.01	-6.05
81	Mexico	37.66	50.64	-12.98
82	Azerbaijan	37.66	55.38	-17.72
83	Vietnam	36.36	46.99	-10.63
84	South Africa	36.36	47.43	-11.07
85	Egypt	35.06	44.43	-9.37
86	Ecuador	35.06	45.3	-10.24
87	China	35.06	57.22	-22.16
88	Rwanda	33.77	29.52	4.25
89	Algeria	33.77	40.93	-7.16
90	Trinidad and Tobago	33.77	52.01	-18.24
91	Montenegro	33.77	57.68	-23.91
92	Oman	33.77	59.81	-26.04
93	Ethiopia	32.47	19.99	12.48
94	Cameroon	32.47	26.83	5.64
95	Venezuela	32.47	43.14	-10.67
96	Côte d'Ivoire	31.17	31.31	-0.14
97	Ghana	31.17	38.74	-7.57
98	Bolivia	31.17	39.91	-8.74
99	Uzbekistan	31.17	49	-17.83
100	Armenia	31.17	54.76	-23.59
101	Nepal	28.57	30.31	-1.74
102	Guatemala	28.57	34.51	-5.94
103	Malawi	27.27	21.31	5.96
104	Bahrain	25.97	66.79	-40.82
105	Tonga	23.38	43.4	-20.02
106	Morocco	23.38	43.71	-20.33
107	Bahamas	23.38	65.1	-41.72

108	Nicaragua	22.08	32.7	-10.62
109	Botswana	22.08	41.42	-19.34
110	Papua New Guinea	22.08		
111	Chad	20.78	13.75	7.03
112	Liberia	19.48		
113	Mali	19.48	24.3	-4.82
114	El Salvador	19.48	37.76	-18.28
115	Kyrgyzstan	19.48	41.15	-21.67
116	Suriname	19.48	51.5	-32.02
117	Lao PDR	18.18	33.11	-14.93
118	Bhutan	18.18	36.9	-18.72
119	Mongolia	18.18	45.52	-27.34
120	Cuba	16.88	29.1	-12.22
121	Zimbabwe	15.58	27.49	-11.91
122	Senegal	15.58	31.75	-16.17
123	Syrian Arab Republic	15.58	33.4	-17.82
124	Cambodia	15.58	34.41	-18.83
125	Barbados	15.58	73.1	-57.52
126	Tajikistan	14.29	34.14	-19.85
127	Iran (Islamic Republic of)	14.29	49.86	-35.57
128	Jordan	14.29	53.75	-39.46
129	Grenada	14.29	58	-43.71
130	Madagascar	12.99	21.32	-8.33
131	Tanzania, United Republic of	12.99	26.01	-13.02
132	Mauritania	11.69	11.3	0.39
133	Afghanistan	11.69	19.5	-7.81
134	Sudan	11.69	25.5	-13.81
135	Namibia	11.69	37.51	-25.82
136	Antigua and Barbuda	11.69	57.1	-45.41
137	Haiti	10.39	26.46	-16.07
138	Vanuatu	10.39	28.1	-17.71
139	Samoa	10.39	33	-22.61
140	Myanmar	10.39	34.29	-23.9
141	Honduras	10.39	34.51	-24.12
142	Libya	10.39	41.1	-30.71
143	Guyana	10.39	42.91	-32.52
144	Seychelles	10.39	50.3	-39.91

145	Saint Kitts and Nevis	10.39	72.4	-62.01
146	Angola	9.09	20.18	-11.09
147	Mozambique	9.09	23.69	-14.6
148	Saint Lucia	9.09	46.3	-37.21
149	Saint Vincent and the Grenadines	9.09	55.4	-46.31
150	Yemen	7.79	18	-10.21
151	Kiribati	5.19	21.7	-16.51
152	Belize	5.19	37.1	-31.91
153	Dominica	3.9	56.9	-53
154	Sierra Leone	3.9		
155	Turkmenistan	3.9		
156	Congo (Democratic Republic of the)	2.6	16.05	-13.45
157	Burundi	2.6	18.71	-16.11
158	Solomon Islands	2.6	21.1	-18.5
159	Tuvalu	2.6		
160	South Sudan	1.3		

Belén en momento lluvioso. Óleo sobre lienzo 50 x 35 cm. 2020.
Cliver Flores Lanzo (Iquitos, Loreto, Perú , 1965).
Correo electrónico: maifloreslanza@yahoo.com
www.cliverpintoramazonico.blogspot.com