PROYECTO DE LEY No _____
SEGURIDAD INFORMÁTICA Y REPRESIÓN DE LOS DELITOS INFORMÁTICOS

La Congresista de la República que suscribe **ROBERTINA SANTILLANA PAREDES** por medio del Grupo Parlamentario de Alianza para el Progreso, en ejercicio de los derechos constitucionales establecidos en los artículos 102° inciso 1) y 107° de la Constitución Política del Perú, y los contenidos en el artículo 76° del Reglamento del Congreso de la República, presenta el siguiente proyecto de ley:

FORMULA LEGAL

El Congreso de la República ha dado la siguiente ley:

LEY DE SEGURIDAD INFORMÁTICA Y REPRESIÓN DE LOS DELITOS INFORMÁTICOS

CAPITULO I
CUESTIONES GENERALES

ARTÍCULO 1.- OBJETO DE LA LEY

El objeto de la presente ley es:

1.1 Establecer reglas de seguridad informática de aplicación en el Estado Peruano.

1.2 Impulsar el Comercio electrónico y proteger al consumidor del mismo, y.

1.3 Dar cumplimiento a la obligación de adecuar la Ley de Delitos Informáticos a lo dispuesto por el Convenio sobre la Ciberdelincuencia adoptado en Budapest, el 23 de noviembre del año 2001, aprobado con reservas por el Estado Peruano mediante la Resolución Legislativa Nº 30913, publicada el 13 de febrero de 2019, en el diario oficial.

CAPITULO II
ESTANDARES DE SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

Artículo 2.- SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

2.1 La Presidencia del Consejo de Ministros a propuesta de la Secretaría de Gobierno Digital establece el plazo en el que de manera obligatoria, todas las entidades del

Poder Ejecutivo, Legislativo, Judicial, Organismos Autónomos, Gobiernos Regionales y Locales deben haber obtenido las certificaciones ISO 17799 y 27001 sobre seguridad informática y seguridad de la información. Así como las disposiciones necesarias y herramientas para comprobar en forma periódica su vulnerabilidad. El plazo considera el criterio de progresividad.

2.2 Los Organismos Públicos y al Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado -FONAFE, harán lo propio, respecto de las personas bajo el ámbito de su competencia.

Artículo 3.- DETERMINACIÓN DE ESTANDAR MÍNIMO DE SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACION QUE SERÁ EXIGIBLE A LAS PERSONAS NATURALES Y JURÍDICAS QUE CONTRATEN CON EL ESTADO

La Presidencia del Consejo de Ministros a propuesta de la Secretaría de Gobierno Digital establece el plazo en el que es exigible de manera obligatoria, a quienes contraten con el Estado, contar con las certificaciones ISO 17799 y 27001 sobre seguridad informática y seguridad de la información.

Artículo 4.- CONVENIOS MULTILATERALES

El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados en materia de prevención, protección al consumidor, investigación y sanción de los delitos informáticos.

CAPITULO III
PROTECCION DEL CONSUMIDOR EN EL COMERCIO ELECTRÓNICO

Artículo 5.- REGLA GENERAL

5.1 Toda transacción comercial realizada a través de un sistema informático, la red o cualquier otra tecnología, debe garantizar la idoneidad del bien o servicio, el cumplimiento de la normatividad vigente y una protección transparente y efectiva al Consumidor.

5.2 La protección que otorga esta Ley es la protección mínima que se brinda al Consumidor, la práctica comercial puede incluir mayores mecanismos de protección.

5.3 El Código de Protección al Consumidor, aprobado por la Ley No. 29571 es aplicable en todo lo no regulado por la presente norma.

Artículo 6.- INFORMACIÓN SOBRE EL BIEN O SERVICIO OFERTADO

Los términos y condiciones que deben ser explicitas en el sistema informático, la red o la tecnología empleada, para la realización de las transacciones comerciales, son cuando menos lo siguiente:

6.1 Información completa del proveedor, el Registro Único de Contribuyentes – RUC el número telefónico y todos los medios de contacto que emplee, una dirección física y horario de atención.

6.2 Información sobre el procedimiento para la adquisición del bien, producto o servicio, señalando las características y las restricciones de los mismos.

6.3 Información sobre los derechos del consumidor previstos en las disposiciones jurídicas aplicables.

6.4 Información sobre los mecanismos de notificación con el consumidor para remitirle el comprobante de pago.

6.5 Información sobre las garantías, el plazo y condiciones para hacerlas efectivas.

6.6 Información sobre los mecanismos de devolución o cambio de los bienes, productos, servicios o en su caso, reembolso, si procede.

6.7 Información sobre los mecanismos de solución para las reclamaciones o aclaraciones, incluyendo los días y horarios de atención, así como el plazo para su resolución.

6.8 Advertencias en las que el consumidor manifieste que cuenta con la mayoría de edad establecida por la legislación nacional.

6.9 Condiciones de pago y facturación.

6.10 Mecanismo para que el consumidor acepte los términos y condiciones. Esta aceptación será distinta a aquélla que pudiera requerirse para el tratamiento de los Datos personales, conforme a la normatividad de la materia.

6.11 Mecanismo para que el consumidor verifique la información resumida sobre el bien, producto o servicio que va a adquirir, así como cualquier información de entrega, precios y costo de envío, antes de aceptar la transacción.

6.12 Mecanismos de seguimiento del cumplimiento de la entrega del bien o prestación del servicio pactado.

Artículo 7.- PROTECCIÓN DE INFORMACIÓN DEL CONSUMIDOR

7.1 El sistema informático, la red o la tecnología empleada, debe contar con mecanismos de seguridad acordes con estándares internacionales que resulten equivalentes a la regulación en materia de seguridad de datos para la Industria de tarjeta de pago (Payment Card Industry Data Security Standard), para los datos de pago que en su caso se traten o almacenen.

7.2 Los métodos de pago, no deben almacenarse, por ende una vez que finalice la transacción comercial, deberá suprimir los datos financieros que no sean necesarios para el propósito para el cual se recabaron, y conservar los mínimos necesarios para la aplicación de cargos y/o reembolsos futuros, según disponga la normatividad aplicable.

Artículo 8.- EXPERIENCIA DEL CONSUMIDOR

El sistema informático, la red o la tecnología empleada, debe contar con mecanismos para que el consumidor consigne sus opiniones y experiencia con el proveedor, el proceso de compra, la entrega, la solución de disputas, etc.

Estos testimonios deberán mantenerse en forma visible en el sistema informático, la red o la tecnología empleada para que el consumidor tome una decisión informada.

CAPITULO IV
PROCEDIMIENTOS DE INVESTIGACIÓN CRIMINAL DE LOS DELITOS INFORMÁTICOS

Artículo 9.- DISPOSICIONES GENERALES

9.1 Se pueden adoptar técnicas especiales de investigación siempre que resulten idóneas, necesarias e indispensables para el esclarecimiento de los hechos materia de investigación. Su aplicación se decide caso por caso y se dictan cuando la naturaleza de la medida lo exija, siempre que existan suficientes elementos de convicción acerca de la comisión de uno o más delitos previstos en esta ley.

Las mismas deben respetar, escrupulosamente y en todos los casos, los principios de necesidad, razonabilidad y proporcionalidad.

9.2 El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

9.3 La ejecución de las técnicas especiales de investigación previstas en este capítulo, así como el requerimiento mediante el que se solicita su ejecución, según sea el caso, deben estar debida y suficientemente motivados, bajo sanción de nulidad, sin perjuicio de los demás requisitos exigidos por la ley. Asimismo, deben señalar la forma de ejecución de la diligencia, así como su alcance y duración.

9.4 Salvo en el caso del levantamiento del secreto bancario, reserva tributaria y bursátil, en el que será necesaria la autorización judicial previa. El fiscal está en la obligación de dar cuenta al Juez de la ejecución de las técnicas especiales, dentro de las veinticuatro horas de ejecutadas.

Artículo 10.- INTERVENCIÓN DE LAS COMUNICACIONES.

10.1 El fiscal, puede ordenar la intervención de las comunicaciones y la correspondencia informática vinculada al delito objeto de investigación procurando, en la medida de lo posible, no afectar a terceros no involucrados, siguiendo el procedimiento previsto en la Ley No. 27697, Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.

10.2 Las empresas de telecomunicaciones, atienden con prioridad las facilidades que sean necesarias para esta intervención, y la celeridad de la información de los datos que sean solicitados.

10.3 Toda comunicación o correspondencia electrónica que no tenga relación con los hechos investigados es mantenida en reserva, siempre y cuando no revelen la presunta comisión de otros hechos punibles, en cuyo caso el fiscal procede conforme al inciso 11 del artículo 2 de la precitada Ley.

10.4 La grabación mediante la cual se registre la intervención de las comunicaciones es custodiada debidamente por el fiscal, quien debe disponerla transcripción de las partes pertinentes y útiles para la investigación.

Artículo 11. LEVANTAMIENTO DEL SECRETO BANCARIO, RESERVA TRIBUTARIA Y BURSÁTIL

11.1 El juez, a solicitud del fiscal, puede ordenar, de forma reservada y de forma inmediata, el levantamiento del secreto bancario o de la reserva tributaria, conforme a lo establecido por el Código Procesal Penal aprobado por Decreto Legislativo 957. La información obtenida solo puede ser utilizada en relación con la investigación de los hechos que la motivaron.

11.2 El juez, previa solicitud del fiscal, puede ordenar que se remita información sobre cualquier tipo de movimiento u operación bursátil, relacionados a acciones, bonos, fondos, cuotas de participación u otros valores, incluyendo la información relacionada a un emisor o sus negocios según lo establecido en los artículos 40 y 45 del Decreto Legislativo 861, Ley del Mercado de Valores, en la medida en que pudiera resultar útil para la investigación.

11.3 Asimismo, la autoridad fiscal o judicial puede solicitar cualquier información sobre los compradores o vendedores de los valores negociados en el sistema bursátil, de conformidad con lo establecido en el inciso a) del artículo 47 del Decreto Legislativo 861.

Artículo 12. INCAUTACIÓN DE BIENES MATERIA DE DELITO

12.1 En todas las investigaciones y procesos penales por delitos informáticos, el fiscal puede autorizar a la Policía Nacional del Perú para la incautación de los objetos, instrumentos, efectos o ganancias del delito o cualquier otro bien proveniente del delito.

12.2 Cuando se trate de una intervención en flagrante delito o peligro inminente de su perpetración, la Policía Nacional del Perú procede de acuerdo a sus competencias, debiendo dar cuenta inmediata de su ejecución al fiscal.

12.3 La administración y custodia de los bienes de carácter delictivo, es determinada por el fiscal de conformidad con las normas y los reglamentos que garantizan la seguridad, conservación, seguimiento y control de la cadena de custodia de los bienes señalados.

12.4 Para los efectos de recepción, registro, calificación, conservación, administración y disposición de los bienes, asume competencia la Comisión Nacional de Bienes Incautados (CONABI), de conformidad con lo dispuesto por el Decreto Legislativo 1104, siempre que dichos bienes provengan de los delitos en agravio del patrimonio del Estado.

Artículo 13.- BLOQUEO DE DOMINIO

13.1 En todas las investigaciones y procesos penales por delitos informáticos, el fiscal puede autorizar el bloqueo del DNS ('Domain Name Service'), a través de la introducción de algoritmos que bloqueen automáticamente todos los posibles dominios asociados a estas redes, así como los vinculados a los enlaces de descarga, o empleando cualquier otro medio que garantice permanencia del bloqueo; igualmente puede disponer el corte del servicio de internet asociado a los delitos informáticos.

13.2 Para el efecto el fiscal ordenará que la empresa de telecomunicaciones, cumpla con este mandato, debiendo velar la Policía Nacional del Perú por su ejecución.

Artículo 14.- AUDIENCIA JUDICIAL DE REEXAMEN

Ejecutadas las técnicas especiales de investigación previstas en los artículos anteriores, el afectado puede instar la realización de la audiencia judicial de reexamen prevista en el artículo 228 y en los incisos 3 y 4 del artículo 231 del Código Procesal Penal aprobado por Decreto Legislativo 957

Artículo 15.- COLABORACIÓN EFICAZ

Cualquier persona que aporte información útil y corroborable que permita:

15.1 Evitar la continuidad, permanencia o consumación del delito informático, o disminuir sustancialmente las consecuencias que resultarían de su ejecución.

15.2 Conocer las circunstancias en las que se planificó o ejecutó, o que se viene planificando o ejecutando el delito informático.

15.3 Identificar a los autores o participes de un delito informático cometido o por cometer, y

15.4 Entregar los instrumentos, efectos, ganancias y bienes delictivos relacionados a los autores del delito informático.

Podrá acogerse a un procedimiento de colaboración eficaz y de ser el caso alcanzar los beneficios que corresponda. El procedimiento de colaboración se rige por las normas del nuevo Código Procesal Penal.

CAPITULO V
RESPONSABILIDAD ADMINISTRATIVA

Artículo 16.- RESPONSABILIDAD ADMINISTRATIVA DE LAS PERSONAS JURÍDICAS

16.1 La persona jurídica, sea o no proveedor de servicio, es responsable administrativamente por los delitos informáticos previstos en esta ley, y en el Código Penal, cuando estos hayan sido cometidos en su nombre y/o por cuenta de ellas y/o en su beneficio, directo o indirecto, por:

16.1.1 Sus administradores de hecho o derecho, representantes legales, contractuales y órganos colegiados, siempre que actúen en el ejercicio de las funciones propias de su cargo.

16.1.2 Las personas naturales que prestan cualquier tipo de servicio a la persona jurídica, con independencia de su naturaleza, del régimen jurídico en que se encuentren o de si media relación contractual y que, estando sometidas a la autoridad y control de los gestores y órganos mencionados en el literal anterior, actúan por orden o autorización de estos últimos.

16.1.3 Las personas naturales señaladas en el literal precedente cuando, en atención a la situación concreta del caso, no se ejerza sobre ellas el debido control y vigilancia por parte de los administradores de hecho o derecho, representantes legales, contractuales u órganos colegiados de la persona jurídica.

16.2 La responsabilidad administrativa prevista en este artículo es independiente de la responsabilidad penal que corresponda a las indicadas personas naturales.

16.3 Procederá la exención de responsabilidad administrativa de la persona jurídica, prevista en el presente artículo, en caso que:

16.3.1 Las personas naturales, señaladas en los numerales anteriores, hayan obrado en beneficio propio, o a favor de un tercero distinto a la persona jurídica.

16.3.2 La persona jurídica haya adoptado e implementado en su organización y con anterioridad a la comisión del delito, un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características, consistente en medidas de vigilancia y control idóneas para prevenir los delitos antes mencionados o para reducir significativamente el riesgo de su comisión.

16.4 Las sanciones aplicables como consecuencia de la responsabilidad administrativa son las previstas en la Ley No. 30424.

CAPITULO VI
DELITOS INFORMÁTICOS

Artículo 17.- INTRUSISMO INFORMÁTICO

17.1 El que sin contar con autorización o haciendo uso indebido de ella, accede o facilita a otro el acceso al conjunto o una parte de un sistema informático, o se mantiene en el mismo, con la intención de obtener información, datos informáticos, o con cualquier otra intención delictiva, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con treinta a noventa días-multa.

17.2 La pena privativa de libertad será no menor de seis ni mayor de diez, cuando el intrusismo es cometido abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema informático en razón del ejercicio de un cargo o función, o tiene por fin la obtención de un beneficio económico para sí o para tercero.

17.3 La pena privativa de libertad será no menor de ocho ni mayor de quince cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.

Artículo 18.-PERTURBACIÓN INFORMÁTICA

18.1 El que deliberadamente, valiéndose de cualquier medio, daña, borra, deteriora, altera, suprime, entorpece, hace inaccesible o imposibilita el funcionamiento de un sistema, una red, un programa o datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

18.2 La pena privativa de la libertad será no menor de seis ni mayor de diez cuando el delito tiene por fin el sabotaje comercial o industrial, es cometido abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema informático, en razón del ejercicio de un cargo o función; o tiene por fin la obtención de un beneficio económico para sí o para tercero.

18.3 La pena privativa de libertad será no menor de ocho ni mayor de quince cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.

Artículo 19.- INTERCEPTACIÓN DE DATOS INFORMÁTICOS

19.1 El que deliberada e ilegalmente intercepta datos informáticos de terceros, en transmisiones no públicas, dirigidos, originados o efectuados dentro de un sistema informático, incluidas las emisiones electromagnéticas que transporten dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

19.2 La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información información personal, comercial o industrial, secreta, reservada o confidencial

19.3 La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.

19.4 Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Artículo 20.- SUPLANTACIÓN DE IDENTIDAD

20.1 Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años, el que empleando un sistema informático o la red, se hace pasar por otra persona suplantando su identidad, con el fin de:

20.1.1 Obtener un beneficio económico para sí o para tercero,
20.1.2 Generar algún perjuicio, material o moral a otra persona natural o jurídica,
20.1.3 Difundir mensajes que agravien el honor o la reputación de otra persona.
20.1.4 Incitar o ejercer violencia material o psicológica por razones de opinión, política, cultura, sexo, raza, origen o actividad.
20.1.5 Incitar al uso de la fuerza en contra de la autoridad

20.2 La pena La pena privativa de libertad será no menor de ocho ni mayor de doce cuando se haya suplantado a una institución del Estado Peruano u organismo extranjero acreditado en el país.

20.3 Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Artículo 21.- CREACIÓN DE FALSA IDENTIDAD

21.1 Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años, el que empleando un sistema informático, o la red, crea una identidad inexistente, con el objeto de:

21.1.1 Obtener un beneficio económico para sí o para tercero,

21.1.2 Generar algún perjuicio, material o moral a otra persona natural o jurídica,

21.1.3 Difundir mensajes que agravien el honor o la reputación de otra persona.

21.1.4 Incitar o ejercer violencia material o psicológica por razones de opinión, política, cultura, sexo, raza, origen o actividad.

21.1.5 Incitar al uso de la fuerza en contra de la autoridad

21.2 Si el agente comete el delito como integrante de una organización criminal, o su actividad ilícita ha sido financiada o auspiciada por una institución o funcionario del Estado, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Artículo 22.- PORNOGRAFIA INFANTIL

22.1 El que a través de la red u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de seis ni mayor de diez años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.

22.2 Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.

22.3 Si el agente produce, financia, ofrece, comercializa, publica, facilita, divulga o distribuye por cualquier medio, o se encuentra en su poder, con fines inequívocos de distribución o comercialización, material pornográfico obtenido en la forma descrita en los párrafos anteriores, la pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.

22.4 La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

Artículo 23.- FRAUDE INFORMÁTICO

23.1 Será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa, el que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante:

23.1.1 El diseño, introducción, alteración, borrado, supresión, extracción o clonación de datos informáticos de un registro o tarjeta, así como cualquier interferencia o manipulación en el funcionamiento de un sistema informático,

23.1.2 La formulación de ofertas engañosas, mediante alegaciones falsas respecto de cualquier elemento de dicha oferta, de modo que resulte un perjuicio económico.

23.1.3 La no entrega de productos adquiridos electrónicamente, por los que se ha recibido el valor convenido.

23.1.4 La obtención indebida de bienes o servicios sin erogar o asumir el compromiso de pago de la contraprestación debida.

23.2 La pena será privativa de libertad no menor de seis ni mayor de doce años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio de personas jurídicas dedicadas a obras de bienestar social, fondos destinados a programas asistenciales, o instituciones del Estado dedicadas a fines asistenciales.

Artículo 24. ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.**"**

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Reglamentación

El Poder Ejecutivo en un plazo máximo de 60 días hábiles emite las normas reglamentarias de la presente ley. En el mismo plazo, mediante decreto supremo refrendado por el Ministro del Interior adecúa las disposiciones del Plan Nacional de

Seguridad Ciudadana 2019-2023, aprobado mediante Decreto Supremo Nº 013-2019-IN.

SEGUNDA. Creación de Fiscalías Especializadas en Delitos Informáticos

El Ministerio Público en un plazo máximo de treinta (30) días, emitirá la norma que disponga la creación de la Fiscalía Especializada en Delitos Informáticos, así como la forma, modo y oportunidad en que empezarán a funcionar.

TERCERA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP

La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

CUARTA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente.**"**

DISPOSICIÓN DEROGATORIA FINAL

PRIMERA.- Derogase la Ley N° Ley N° 30096 y su modificación efectuada por Ley N°30171 y toda norma que se oponga a lo dispuesto en la presente Ley.

FIRMA DIGITAL
Firmado digitalmente por: COMBINA SALVATIERRA CESAR AUGUSTO FIR 44709978 hard
Motivo: En señal de conformidad
Fecha: 25/06/2020 11:11:47-0500

FIRMA DIGITAL
Firmado digitalmente por: SANTILLANA PAREDES ROBERTINA FIR 01115525 hard
Motivo: Soy el autor del documento
Fecha: 25/06/2020 11:13:10-0500

:RTINA SANTILLANA PAREDES
CONGRESISTA DE LA REPÚBLICA

FIRMA DIGITAL
Firmado digitalmente por: ACATE CORONEL EDUARDO GEOVANNI FIR 18151793 hard
Motivo: En señal de conformidad
Fecha: 25/06/2020 10:44:59-0500

FIRMA DIGITAL
Firmado digitalmente por: CARCAUSTO HUANCA Irene FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 25/06/2020 11:18:48-0500

FIRMA DIGITAL
Firmado digitalmente por: BENAVIDES GAVIDIA Walter FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 25/06/2020 11:34:20-0500

FIRMA DIGITAL
Firmado digitalmente por: PEREZ MIMBELA Jhosept Amado FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 25/06/2020 11:48:00-0500

FIRMA DIGITAL
Firmado digitalmente por: QUISPE SUAREZ Mario Javier FIR 02881152 hard
Motivo: En señal de conformidad
Fecha: 25/06/2020 13:08:09-0500

FIRMA DIGITAL
Firmado digitalmente por: MERINO LOPEZ Omar FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 25/06/2020 12:07:40-0500

FIRMA DIGITAL
Firmado digitalmente por: GONZALEZ CRUZ Moises FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 25/06/2020 14:04:19-0500

FIRMA DIGITAL
Firmado digitalmente por: GONZALEZ CRUZ Moises FAU 20161749126 soft
Motivo: VOCERO ALTERNO
Fecha: 25/06/2020 14:05:23-0500

EXPOSICIÓN DE MOTIVOS

I. FUNDAMENTOS

1. La Seguridad Informática

La Cuarta Revolución Industrial ha traído consigo el uso intensivo de herramientas tecnológicas como el big data o el Internet de las Cosas que ha cambiado la manera de hacer gestión pública y la vida ciudadana. Esta irrupción tecnológica debe ser preocupación de los gobiernos, por los cambios que implica:

"El Gobierno, los gobiernos, están en el centro de esta revolución. De entrada, porque serán responsables de que el acceso a la tecnología cree más ciudadanos incluidos en la sociedad global y sus beneficios. Asimismo, deberán ser conscientes del conflicto que siempre surge entre el favorecer el avance tecnológico o limitarlo y de las consecuencias que en todos los campos va a tener para el desarrollo normal de la acción de Gobierno. Todo ello combinado con la realidad de la facilidad que tiene la deslocalización de actividades y de presencia virtual del individuo –a través de las VPN-, con lo que supone de limitación en su actividad de supervisión y el efecto negativo sobre la recaudación fiscal"[1]

Y la preocupación debe estar centrada, en que conjuntamente con las inconmensurables ventajas del internet y del intercambio de información global en tiempo real, se ha desarrollado una fuerza oscura de cibercrimenes, que van más allá de las fronteras físicas, tan es así que la Escuela Clark de la Universidad de Maryland, en un estudio realizado, resalta que cada 39 segundos hay un ciberataque en el mundo, como promedio.

La respuesta a esta situación ha sido la seguridad informática y la creación de estándares internacionales de protección de datos, implementación de medidas, obligación de auditorías de ciberseguridad, protección de firmas digitales y transacciones electrónicas, responsabilidad y compromiso de los proveedores de servicios de Internet, entre otros aspectos.

Se ha avanzado mucho en la materia, sin embargo pandemias como el COVID-19 se han convertido en un gatillador de la cibercriminalidad, como consecuencia del teletrabajo, la educación a distancia, las compras "on line", el uso de las redes sociales y tantas otras actividades que se realizan a través del internet y que constituyen potenciales amenazas.

[1] GONZALES, J. (2017). CUARTA REVOLUCIÓN INDUSTRIAL Y DESAFÍOS DEL GOBIERNO . *Revista Catalana de Derecho Público*.

"El delito cibernético es una forma emergente de la delincuencia transnacional y uno de los de más rápido crecimiento. A medida que Internet se ha convertido en una parte casi esencial de nuestras vidas, suministrando información y comunicación en todo el mundo, los delincuentes le han sacado aprovecho. Con unos dos mil millones de usuarios en todo el mundo, el ciberespacio es el lugar ideal para los delincuentes, ya que pueden permanecer en el anonimato y tener acceso a todo tipo de información personal que, a sabiendas o inconscientemente, guardamos en línea. Las amenazas a la seguridad en Internet se han disparado de forma espectacular en los últimos años, y el delito cibernético afecta ahora a más de 431 millones de víctimas adultas a nivel mundial".[2]

Se calcula que la delincuencia cibernética es un negocio que puede superar los tres billones de dólares al año, por los que sin una normativa adecuada y capacidad de gestión, estamos ante una pelea disímil porque los delincuentes cibernéticos se esconden dentro de vacíos legales y la posibilidad de cometer sus fechorías en cualquier lugar de la tierra.

Es tan grave el tema que en la actualidad, la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) promueve el desarrollo de capacidad sostenible a largo plazo en la lucha contra el delito cibernético a través del apoyo a las estructuras y acción nacionales, en los sistemas de justicia penal desarrollo de capacidades, la prevención y la sensibilización, así como la recopilación de datos, la investigación y el análisis sobre la delincuencia cibernética.

2. Las normas ISO sobre Seguridad Informática y Seguridad de la Información en el Estado Peruano

En el mes de julio del 2004 se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 1ª Edición, la cual fue actualizada en el año 2007 por la NTP-ISO/IEC 17799:2007; aprobándose su uso obligatorio mediante la Resolución Ministerial No. 246-2007-PCM; siendo éstas últimas normas la base para la elaboración de la ISO 27001.

Posteriormente, teniendo como marco la Política Nacional de Gobierno Electrónico 2013 – 2017, la Presidencia del Consejo de Ministros, mediante Resolución Ministerial N° 004-2016-PCM de fecha 14 de enero del 2016, aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición", para todas las entidades integrantes del Sistema Nacional de Informática.

[2] https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

En cumplimiento de estas obligaciones, las entidades del Estado han aprobado sus propios documentos de gestión destinados a cumplir con estas Normas Técnicas peruanas. De ahí que la obtención de las normas ISO permitirán a las instituciones del Estado, tener un documento que avale y garantice la calidad de sus procesos, sus formas de trabajo y los controles de calidad para que no haya errores.

Recientemente el Estado Peruano mediante el Decreto de Urgencia No. 007-2020, aprobó el "Marco de Confianza Digital" en cuya exposición de motivos se lee lo siguiente:

"Mediante Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se estableció un 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;

El artículo 30 del precitado Decreto Legislativo define la Seguridad Digital como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas;

Que, asimismo, el artículo 33 del referido Decreto Legislativo, establece que la Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno";

Y en tal sentido define la Confianza Digital como "…el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital"

Está claro que exigir alcanzar los estándares ISO, abona en el propósito del Estado de alcanzar este resultado. El Instituto Nacional de la Calidad – INACAL cuenta con un registro de Organismos de Certificación de Sistemas de Gestión (OCSG) verifican que una entidad cumpla con todos los requerimientos de una norma técnica.

Considerando que el mercado peruano es aún muy pequeño para estas certificaciones, el costo es variado, por eso considerando las urgencias del Estado, se ha establecido una pauta de progresividad que deberá ser determinada por la administración teniendo en cuenta, entre otros dicho factor.

3. El Comercio Electrónico

"En la nueva era el comercio se trasforma con el avance de la tecnología y la ciencia, la aparición de los equipos de computación e internet, la globalizan del mundo en la medida que estos avanzan, siendo más dinámicos y sofisticados. El comercio entre personas, el comercio de empresas a empresas principalmente en los países con mayor desarrollo financiero, hacen uso de estos avances tecnológicos. El internet empieza a ser más accesible, como lo señala la Organización Mundial del Comercio (OMC). En forma simultánea aparece el fenómeno delictivo y se tiene que ir adecuando las normas legales a nuevos los tipos penales los delitos informáticos".[3]

El usuario de hoy realiza por internet compras, pagos de cuentas de servicios básicos, compras de pasajes o transferencias a terceros desde el portales bancarios, sin considerar usualmente las recomendaciones de seguridad básicas para la protección de su información sensible. Eso ha permitido el crecimiento del fraude informático, que generalmente emplea las modalidades de ingeniería social, "fishing", y el "pharming".

El primero de ellos consiste en obtener información de los usuarios a través de plataformas como Facebook y operar en base a engaños; el segundo, tiene que ver con el desarrollo de "espejos" de sitios bancarios o casas comerciales; y el último, con virus troyanos que invaden los computadores y envían información al hacker.

"La organización policial Europol alerta de que los delincuentes están aprovechando "rápidamente las oportunidades" para explotar la crisis del coronavirus "adaptando su modus operandi" en actividades como el cibercrimen, el fraude o las falsificaciones, según consta en un informe presentado este viernes.

El contexto de emergencia sanitaria y las medidas de confinamiento aplicadas por los países europeos a sus ciudadanos para contener la expansión de la pandemia, combinado con una alta demanda de equipos de protección y productos farmacéuticos,

[3] http://revista.cleu.edu.mx/new/descargas/1602/articulos/Articulo12_Criminalidad_y_Economia_Digital.pdf

la disminución de la movilidad dentro de la Unión Europea (UE) y el recurso al teletrabajo, han generado nuevos modelos de delincuencia"[4]

En un reportaje periodístico publicado en el Diario El Peruano [5], se cita al coronel PNP Orlando Mendieta, jefe de la División de Investigación de Alta Tecnología (Divindat), quien precisó que la mayor cantidad de denuncias se concentra en el delito contra el patrimonio. Los fraudes informáticos y sus subtipos alcanzaron 2,097 denuncias durante el 2019.

Del total, 1,641 denuncias se centran en transacciones no autorizadas vía internet. También hubo 431 casos de compras fraudulentas y 25 de clonación de tarjetas de crédito o débito. Le siguen las denuncias en las que los atacantes emplearon herramientas digitales como redes sociales, software y otras plataformas en línea. En esta categoría hubo 268 denuncias en el 2019, mientras que el año previo tuvo 362 registros.

4. Las recomendaciones de la OCDE

La Organización para la Cooperación y el Desarrollo Económicos (OCDE), emitió en el año 2016, un conjunto de recomendaciones, respecto del tema de la protección del consumidor del comercio electrónico, en la idea de que estas "buenas prácticas" sean recogidas por la legislación nacional, ante el crecimiento de las transacciones electrónicas.

En el Perú, el Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual – INDECOPI, que es titular de la competencia de defensa del consumidor, emite periódicamente recomendaciones a los consumidores respecto de los cuidados que debe tener al realizar transacciones por medios electrónicos. Pero también es cierto que hasta la fecha este tipo de conductas dañosas a los derechos del consumidor, no han sido incorporadas en la Ley 29571, Código de Protección al Consumidor.

La urgencia del tema se hace patente, cuando el propio INDECOPI revela que según reporte al día 72, durante el estado de emergencia, recibió 1027 reclamos y reportes de consumidores que realizaron compras online. Estos se registraron mediante los canales de atención virtuales y telefónicos que la institución mantiene al servicio de los ciudadanos.

[4] https://gestion.pe/tecnologia/europol-alerta-contra-fraude-cibercrimen-y-estafas-en-la-crisis-del-covid-19-noticia/
[5] http://www.elperuano.pe/noticia-estos-son-delitos-informaticos-mas-frecuentes-el-peru-88720.aspx

Entre las infracciones al Código de Protección y Defensa del Consumidor más recurrentes detectadas tras el análisis de la estadística, se encuentran las siguientes:

- El proveedor no entregó el producto
- Los productos se encontraban defectuosos
- Las empresas entregaron productos incompletos
- No atendieron el cambio del producto
- No les reembolsaron el dinero pagado
- Cancelación o anulación sin previo aviso

Resulta entonces necesario, establecer mecanismos legales que permitan una adecuada defensa del consumidor, pues la especialidad de estas conductas amerita reglas claras que se sumen a las existentes.

5. La suplantación y creación de identidades inexistentes para cometer delitos

Una situación que se presenta con especial relevancia, no solo en la actividad comercial, sino en los delitos relacionados con la pornografía infantil y en los delitos contra el honor, es la suplantación y creación de identidades inexistentes, a partir de las cuales el delincuente informático se esconde para cometer sus acciones.

La suplantación de identidad es una acción malintencionada para cometer algún tipo de fraude, obtener datos de manera ilegal, cometer ciberbullying o grooming (conseguir la confianza de un menor para poder abusar sexualmente de él). El ejemplo más típico de suplantación es crear un perfil falso en las redes sociales para poder comunicarse con otras personas haciéndose pasar por ella.

Por lo general se suele tender a pensar que las únicas personas a las que se suplanta su identidad son personas famosas como por ejemplo políticos o "celebrities". Esta es una idea incorrecta ya que cualquier identidad de un usuario anónimo corre el riesgo de ser suplantada. El número de personas que han denunciado una suplantación de identidad ha crecido exponencialmente en los últimos años. La suplantación de identidades es un vehículo para la comisión de los delitos"[6]

La creación de identidades inexistentes se emplea, no solo como mecanismo, para cometer delitos, tal como ocurre con la suplantación de identidad, sino también para incitar a la violencia o dañar la reputación de una persona u organización. El ejemplo más claro de esta figura son los denominados "troll" a los que se puede describir como una persona que administra una o varias cuentas en forma manual sin revelar su verdadera identidad, que opera en coordinación con cientos o miles de bots, que son

[6] https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

cuentas que funcionan de forma automatizada, para replicar y masificar un mensaje determinado.

Luciano Galup, consultor en comunicación y analista de redes, señala que estos "troll"

"Gracias a sofisticadas herramientas de "escucha activa", creadas originalmente para que las marcas puedan evaluar qué pensaban sus clientes sobre ellas, se puede detectar rápidamente cuando alguien habla de un tema determinado. Una vez definido el objetivo, los trolls pueden atacar con altos niveles de agresividad, respaldados en el anonimato

En la misma línea, Galup subraya que el hostigamiento es una forma de incentivar la autocensura. "Se nota mucho cuando hay un periodista que dice algo diferente a la audiencia que tiene construida históricamente. Se produce entre sus seguidores ciertos niveles de indignación", afirma. Si bien medir la autocensura es casi imposible, se puede especular que el miedo a los ataques podría tener cierto peso a la hora de intervenir en la discusión pública".[7]

Debe quedar claro que lo que se pretende sancionar, son conductas en las que el uso de la tecnología traspasa lo legal y se cometen delitos a través de medios informáticos, en ningún caso se pretende sancionar la libertad de opinión.

6. El Convenio de Budapest y la ley peruana

El Convenio de Budapest sobre ciberdelincuencia es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes.

Fue elaborado por el Consejo de Europa en Estrasburgo, y aprobado por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en Budapest y en el caso peruano, el mismo fue aprobado con reservas por el Estado Peruano mediante la Resolución Legislativa Nº 30913, publicada el 13 de febrero de 2019, en el diario oficial.

Cabe señalar que para cuando el país aprobó el citado Convenio, ya estaba vigente la Ley de Delitos Informáticos, Ley N° 30096 y su modificación efectuada por Ley N°30171. La aprobación del convenio a través de la Resolución Legislativa Nº 30913, nos obliga a adaptar nuestra legislación interna a lo dispuesto en el referido tratado, considerando, por cierto las declaraciones y reservas efectuadas.

[7] https://www.infobae.com/politica/2017/11/20/mitos-y-verdades-de-los-trolls-en-la-politica/

El propósito de este proyecto es cumplir con esa adecuación, además de los propósitos ya señalados de dotar al país de un marco de seguridad informática e incorporar medidas de protección al consumidor para proteger el comercio electrónico.

7. **La incorporación de nuevas facultades para el proceso de investigación criminal**.

En el desarrollo de la adecuación de la legislación nacional al Convenio de Budapest, se han incorporado las más recientes facultades que la ley peruana ha concedido a los órganos de justicia para el combate de la criminalidad organizada, haciendo las modificaciones pertinentes para su adecuación a las figuras delictivas a perseguir.

En este escenario, se conceden amplias facultades y herramientas al Ministerio Público y a la Policía Nacional del Perú, bajo el control del Poder Judicial, entendiendo que siendo delitos que se cometen empleando herramientas tecnológicas, es necesario que se cuente con todos los medios para una lucha eficaz contra los mismos.

8. La fiscalía especializada

El artículo 80-B de la Ley Orgánica del Ministerio Público (Decreto Legislativo Nº 052) establece que "el Fiscal de la Nación, previa aprobación de la Junta de Fiscales Supremos, podrá designar fiscales para que intervengan, según su categoría, en la investigación y juzgamiento de todos aquellos hechos delictivos vinculados entre sí o que presentan características similares y que requieran de una intervención especializada del Ministerio Público". El mismo artículo señala que el reglamento de funcionamiento de estas fijará la competencia territorial, organización, funcionamiento y los mecanismos de coordinación y supervisión que correspondan a estos Órganos Especializados.[8]

Es así como a la fecha existen Fiscalías Especializadas en Delitos de Corrupción de Funcionarios Fiscalías Especializadas en Criminalidad Organizada. Fiscalías Especializadas en Delitos de Lavado de Activos y Pérdida de Dominio Fiscalías Especializadas en Materia Ambiental (FEMA). Fiscalías Especializadas en Tráfico Ilícito de Drogas. Fiscalías Especializadas en Delitos de Trata de Personas. Fiscalías Especializadas en Delitos Tributarios. Fiscalías Especializadas en Delitos Aduaneros y contra la Propiedad Intelectual.[9]

Con esta experiencia, se deja a criterio del Ministerio Público la emisión de un resolutivo que determine cuando van a entrar en funcionamiento estas fiscalías, lo que obedecerá

[8] https://www.mpfn.gob.pe/fiscalias_especializadas/
[9] ídem

a la disponibilidad presupuestaria para cumplir esta función, pudiendo incluso convertir alguna de las actuales fiscalías especializadas en mixta o exclusiva para este nuevo tipo de criminalidad.

II. PROPUESTA

La propuesta normativa tiene por finalidad dotar al país de un marco de seguridad informática, incorporar medidas de protección al consumidor para proteger el comercio electrónico a tono con las recomendaciones de la OCDE y cumplir con la adecuación, de la normatividad nacional a los preceptuado por el Convenio de Budapest aprobado con reservas por el Estado Peruano mediante la Resolución Legislativa Nº 30913, publicada el 13 de febrero de 2019, en el diario oficial.

La propuesta normativa, consta de seis capítulos, veinticuatro artículos, cuatro disposiciones complementarias finales y una disposición derogatoria final.

Se incorpora además la responsabilidad administrativa de la persona jurídica en la que preste servicios, labore o tenga relación el autor material de los delitos informáticos, con lo cual se impulsa que las empresas establezcan medidas de gobierno corporativo y de prevención.

Contiene normas que son de aplicación en todo el Estado Peruano, normas que serán de aplicación por el Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual- INDECOPI, y normas que serán de aplicación por la autoridad policial y los operadores de justicia del país.

III. ANALISIS COSTO BENEFICIO

Se cumple la finalidad señalada en el numeral 3.1 del Artículo 3º del Reglamento de la Ley Nº 26889, Ley Marco para la Producción y Sistematización Legislativa, aprobado por Decreto Supremo Nº 008-2006- JUS, ya que el costo de no regular con eficiencia devendrá en perjuicios mayores al país considerando las cifras mundiales alrededor de la tecnología que nos revelan que diariamente se realizan treinta (30) billones de tratos económicos, y, sobre todo, que la proyección del impacto económico de los delitos informáticos al año 2022 se estima en ocho (8) trillones de dólares.

IV. ANÁLISIS DE IMPACTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

El impacto de la presente propuesta legislativa sobre la legislación nacional implica la dación de un cuerpo normativo innovativo que regula la seguridad informática y la protección del consumidor en las operaciones de comercio electrónico; asimismo, la

derogatoria de la Ley 30096, Ley de Delitos Informáticos y sus normas modificatorias, planteando un nueva regulación sobre los mismos conforme a los lineamientos establecidos en el Convenio de Budapest.

Ley 30096	Propuesta	Comentario
Artículo 1. Objeto de la Ley La presente Ley tiene por objeto prevenir y sancionar 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, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.	**ARTÍCULO 1.- OBJETO DE LA LEY** El objeto de la presente ley establecer es: 1.1 Establecer reglas de seguridad informática de aplicación en el Estado Peruano. 1.2 Impulsar el Comercio electrónico y proteger al consumidor del mismo, y. 1.3 Dar cumplimiento a la obligación de adecuar la Ley de Delitos Informáticos a lo dispuesto por el Convenio sobre la Ciberdelincuencia adoptado en Budapest, el 23 de noviembre del año 2001, aprobado con reservas por el Estado Peruano mediante la Resolución Legislativa Nº 30913, publicada el 13 de febrero de 2019, en el diario oficial.	El Proyecto tiene una finalidad más amplia, pues resume en un solo documento tres necesidades: a. Mejorar las reglas de seguridad en el Estado Peruano. b. Establecer un estándar mínimo de protección para el consumidor de bienes y servicios por medios electrónicos. c. Cumplir con adecuar la legislación nacional a lo preceptuado por el Convenio de Budapest que ya es norma legal en el Perú
	Artículo 2.- INCORPORACIÓN DE LA SEGURIDAD INFORMATICA Y LA REPRESION DE DELITOS INFORMATICOS EN EL PLAN NACIONAL DE SEGURIDAD CIUDADANA 2019-2023 Dispóngase la modificación del Plan Nacional de Seguridad Ciudadana 2019-2023 aprobado mediante Decreto Supremo No. 013-2019-IN, con la finalidad de incorporar los temas que son materia de la presente ley.	Es un tema nuevo, ni el Plan Nacional de Seguridad Ciudadana anterior ni el vigente disgregan los delitos informáticos, a pesar de ser un tema creciente. La idea del Plan Nacional es que en el CONASEC se identifiquen los problemas y su origen a partir de lo cual se propongan las estrategias de acción.
	Artículo 3.- SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN 3.1 La Presidencia del Consejo de Ministros a propuesta de la Secretaría de	Ya el Estado Peruano está caminando hacia la seguridad y confianza digital, por lo que la certificación ISO establece un sistema de medición y retroalimentación para mantener en el tiempo los

	Gobierno Digital establece el plazo en el que de manera obligatoria, todas las entidades del Poder Ejecutivo, Legislativo, Judicial, Organismos Autónomos, Gobiernos Regionales y Locales deben haber obtenido las certificaciones ISO 17799 y 27001 sobre seguridad informática y seguridad de la información. Así como las disposiciones necesarias y herramientas para comprobar en forma periódica su vulnerabilidad. El plazo considera el criterio de progresividad. 3.2 Los Organismos Públicos y al Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado - FONAFE, harán lo propio, respecto de las personas bajo el ámbito de su competencia.	estándares que determina la organización.
	Artículo 4.- DETERMINACIÓN DE ESTANDAR MÍNIMO DE SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACION QUE SERÁ EXIGIBLE A LAS PERSONAS NATURALES Y JURÍDICAS QUE CONTRATEN CON EL ESTADO La Presidencia del Consejo de Ministros a propuesta de la Secretaría de Gobierno Digital establece el plazo en el que es exigible de manera obligatoria, a quienes contraten con el Estado, contar con las certificaciones ISO 17799 y 27001 sobre seguridad informática y seguridad de la información.	Es un tema nuevo, la idea es masificar el uso de los mecanismos de seguridad de la información y seguridad informática. Luego, siendo el Estado el primer demandante de bienes y servicios una forma de hacerlo es exigir en el plazo en que se determine, el cumplimiento de las normas ISO
OCTAVA. Convenios multilaterales El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos	Artículo 5.- CONVENIOS MULTILATERALES El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados en materia de prevención, protección al	En la Ley 30096 esta es una disposición final, sitio indebido para una regulación, en la propuesta forma parte del articulado.

	consumidor, investigación y sanción de los delitos informáticos.	
	Artículo 6.- REGLA GENERAL 6.1 Toda transacción comercial realizada a través de un sistema informático, la red o cualquier otra tecnología, debe garantizar la idoneidad del bien o servicio, el cumplimiento de la normatividad vigente y una protección transparente y efectiva al Consumidor. 6.2 La protección que otorga esta Ley es la protección mínima que se brinda al Consumidor, la práctica comercial puede incluir mayores mecanismos de protección. 6.3 El Código de Protección al Consumidor, aprobado por la Ley No. 29571 es aplicable en todo lo no regulado por la presente norma. Artículo 7.- INFORMACIÓN SOBRE EL BIEN O SERVICIO OFERTADO Los términos y condiciones que deben ser explicitas en el sistema informático, la red o la tecnología empleada, para la realización de las transacciones comerciales, son cuando menos lo siguiente: 7.1 Información completa del proveedor, el Registro Único de Contribuyentes – RUC el número telefónico y todos los medios de contacto que emplee, una dirección física y horario de atención. 7.2 Información sobre el procedimiento para la adquisición del bien, producto o servicio, señalando las características y las restricciones de los mismos. 7.3 Información sobre los derechos del consumidor	Estas normas no tienen precedentes en la legislación nacional, son una propuesta nueva.

	previstos en las disposiciones jurídicas aplicables. 7.4 Información sobre los mecanismos de notificación con el consumidor para remitirle el comprobante de pago. 7.5 Información sobre las garantías, el plazo y condiciones para hacerlas efectivas. 7.6 Información sobre los mecanismos de devolución o cambio de los bienes, productos, servicios o en su caso, reembolso, si procede. 7.7 Información sobre los mecanismos de solución para las reclamaciones o aclaraciones, incluyendo los días y horarios de atención, así como el plazo para su resolución. 7.8 Advertencias en las que el consumidor manifieste que cuenta con la mayoría de edad establecida por la legislación nacional. 7.9 Condiciones de pago y facturación. 7.10 Mecanismo para que el consumidor acepte los términos y condiciones. Esta aceptación será distinta a aquélla que pudiera requerirse para el tratamiento de los Datos personales, conforme a la normatividad de la materia. 7.11 Mecanismo para que el consumidor verifique la información resumida sobre el bien, producto o servicio que va a adquirir, así como cualquier información de entrega, precios y costo de envío, antes de aceptar la transacción. 7.12 Mecanismos de seguimiento del cumplimiento de la entrega del bien o prestación del servicio pactado. Artículo 8.- PROTECCIÓN DE INFORMACIÓN DEL CONSUMIDOR	

	8.1 El sistema informático, la red o la tecnología empleada, debe contar con mecanismos de seguridad acordes con estándares internacionales que resulten equivalentes a la regulación en materia de seguridad de datos para la Industria de tarjeta de pago (Payment Card Industry Data Security Standard), para los datos de pago que en su caso se traten o almacenen. 8.2 Los métodos de pago, no deben almacenarse, por ende una vez que finalice la transacción comercial, deberá suprimir los datos financieros que no sean necesarios para el propósito para el cual se recabaron, y conservar los mínimos necesarios para la aplicación de cargos y/o reembolsos futuros, según disponga la normatividad aplicable. Artículo 9.- EXPERIENCIA DEL CONSUMIDOR El sistema informático, la red o la tecnología empleada, debe contar con mecanismos para que el consumidor consigne sus opiniones y experiencia con el proveedor, el proceso de compra, la entrega, la solución de disputas, etc. Estos testimonios deberán mantenerse en forma visible en el sistema informático, la red o la tecnología empleada para que el consumidor tome una decisión informada.	
SEGUNDA. Agente encubierto en delitos informáticos El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la	Artículo 10.- DISPOSICIONES GENERALES 10.1 Se pueden adoptar técnicas especiales de investigación siempre que resulten idóneas, necesarias e indispensables para el esclarecimiento de los hechos materia de investigación. Su	Las normas de carácter procesal están en la Ley vigente como Disposiciones Finales, y las modificaciones efectuadas permitían varias de estas técnicas especializadas de investigación cuando se trata de crimen organizado, no de acciones individuales de los

presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957. PRIMERA. Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional Modifícase el artículo 1 de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por el Decreto Legislativo 991 y por Ley 30077,	aplicación se decide caso por caso y se dictan cuando la naturaleza de la medida lo exija, siempre que existan suficientes elementos de convicción acerca de la comisión de uno o más delitos previstos en esta ley. Las mismas deben respetar, escrupulosamente y en todos los casos, los principios de necesidad, razonabilidad y proporcionalidad. 10.3 El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957. 10.4 La ejecución de las técnicas especiales de investigación previstas en este capítulo, así como el requerimiento mediante el que se solicita su ejecución, según sea el caso, deben estar debida y suficientemente motivados, bajo sanción de nulidad, sin perjuicio de los demás requisitos exigidos por la ley. Asimismo, deben señalar la forma de ejecución de la diligencia, así como su alcance y duración. 10.5 Salvo en el caso del levantamiento del secreto bancario, reserva tributaria y bursátil, en el que será necesaria la autorización judicial previa. El fiscal está en la obligación de dar	delincuentes informáticos, por lo que se amplía la competencia policial en la materia. El fiscal se convierte en el titular de la investigación a tono con las normas del nuevo Código procesal Penal

	cuenta al Juez de la ejecución de las técnicas especiales, dentro de las veinticuatro horas de ejecutadas.	
Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación (...) 4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular. Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de	Artículo 11.- INTERVENCIÓN DE LAS COMUNICACIONES. 11.1 El fiscal, puede ordenar la intervención de las comunicaciones y la correspondencia informática vinculada al delito objeto de investigación procurando, en la medida de lo posible, no afectar a terceros no involucrados, siguiendo el procedimiento previsto en la Ley No. 27697, Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional. 11.2 Las empresas de telecomunicaciones, atienden con prioridad las facilidades que sean necesarias para esta intervención, y la celeridad de la información de los datos que sean solicitados. 11.3 Toda comunicación o correspondencia electrónica que no tenga relación con los hechos investigados es mantenida en reserva, siempre y cuando no revelen la presunta comisión de otros hechos punibles, en cuyo caso el fiscal procede conforme al inciso 11 del artículo 2 de la precitada Ley. 11.4 La grabación mediante la cual se registre la intervención de las comunicaciones es custodiada debidamente por el fiscal, quien debe disponerla transcripción de las partes pertinentes y útiles para la investigación.	El tema se incorporó como una modificación al código procesal penal. Lo que se ha hecho es reducir el plazo de 30 días que tenían las empresas operadoras Se precisa que esta intervención se hace en el marco y con el procedimiento previsto en la Ley 27697.

innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú		
Artículo 235. Levantamiento del secreto bancario (...) 5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.	Artículo 12. LEVANTAMIENTO DEL SECRETO BANCARIO, RESERVA TRIBUTARIA Y BURSÁTIL 12.1 El juez, a solicitud del fiscal, puede ordenar, de forma reservada y de forma inmediata, el levantamiento del secreto bancario o de la reserva tributaria, conforme a lo establecido por el Código Procesal Penal aprobado por Decreto Legislativo 957. La información obtenida solo puede ser utilizada en relación con la investigación de los hechos que la motivaron. 12.2 El juez, previa solicitud del fiscal, puede ordenar que se remita información sobre cualquier tipo de movimiento u operación bursátil, relacionados a acciones, bonos, fondos, cuotas de participación u otros valores, incluyendo la información relacionada a un emisor o sus negocios según lo establecido en los artículos 40 y 45 del Decreto Legislativo 861, Ley del Mercado de Valores, en la medida en que pudiera resultar útil para la investigación. 12.3 Asimismo, la autoridad fiscal o judicial puede solicitar cualquier información sobre los compradores o vendedores de los valores negociados en el sistema bursátil, de conformidad con lo establecido en el inciso a) del artículo 47 del Decreto Legislativo 861.	Se le ha dado un mejor tratamiento y mayor rapidez a la solicitud de levantamiento del secreto bancario.

	Artículo 13. INCAUTACIÓN DE BIENES MATERIA DE DELITO 13.1 En todas las investigaciones y procesos penales por delitos informáticos, el fiscal puede autorizar a la Policía Nacional del Perú para la incautación de los objetos, instrumentos, efectos o ganancias del delito o cualquier otro bien proveniente del delito. 13.2 Cuando se trate de una intervención en flagrante delito o peligro inminente de su perpetración, la Policía Nacional del Perú procede de acuerdo a sus competencias, debiendo dar cuenta inmediata de su ejecución al fiscal. 13.3 La administración y custodia de los bienes de carácter delictivo, es determinada por el fiscal de conformidad con las normas y los reglamentos que garantizan la seguridad, conservación, seguimiento y control de la cadena de custodia de los bienes señalados. 13.4 Para los efectos de recepción, registro, calificación, conservación, administración y disposición de los bienes, asume competencia la Comisión Nacional de Bienes Incautados (CONABI), de conformidad con lo dispuesto por el Decreto Legislativo 1104, siempre que dichos bienes provengan de los delitos en agravio del patrimonio del Estado.	Tema nuevo tomado de las normas del crimen organizado.
	Artículo 14.- BLOQUEO DE DOMINIO 14.1 En todas las investigaciones y procesos penales por delitos informáticos, el fiscal puede autorizar el bloqueo del DNS ('Domain Name Service'), a través de la introducción de	Tema nuevo, se busca evitar la continuación del delito a través de medidas inmediatas que atienden al uso de las herramientas tecnológicas. Esta forma de actuar se recoge en la legislación española.

	algoritmos que bloqueen automáticamente todos los posibles dominios asociados a estas redes, así como los vinculados a los enlaces de descarga, o empleando cualquier otro medio que garantice permanencia del bloqueo; igualmente puede disponer el corte del servicio de internet asociado a los delitos informáticos. 14.2 Para el efecto el fiscal ordenará que la empresa de telecomunicaciones, cumpla con este mandato, debiendo velar la Policía Nacional del Perú por su ejecución.	
	Artículo 15.- AUDIENCIA JUDICIAL DE REEXAMEN Ejecutadas las técnicas especiales de investigación previstas en los artículos anteriores, el afectado puede instar la realización de la audiencia judicial de reexamen prevista en el artículo 228 y en los incisos 3 y 4 del artículo 231 del Código Procesal Penal aprobado por Decreto Legislativo 957	Al darle más facultades al Ministerio Público se ha consignado esta medida de control por parte del Poder Judicial.
	Artículo 16.- COLABORACIÓN EFICAZ Cualquier persona que aporte información útil y corroborable que permita: 16.1 Evitar la continuidad, permanencia o consumación del delito informático, o disminuir sustancialmente las consecuencias que resultarían de su ejecución. 16.2 Conocer las circunstancias en las que se planificó o ejecutó, o que se viene planificando o ejecutando el delito informático. 16.3 Identificar a los autores o participes de un delito informático cometido o por cometer, y	Se incorpora la colaboración eficaz, la norma vigente no la contempla.

	16.4 Entregar los instrumentos, efectos, ganancias y bienes delictivos relacionados a los autores del delito informático. Podrá acogerse a un procedimiento de colaboración eficaz y de ser el caso alcanzar los beneficios que corresponda. El procedimiento de colaboración se rige por las normas del nuevo Código Procesal Penal.	
	Artículo 17.- RESPONSABILIDAD ADMINISTRATIVA DE LAS PERSONAS JURÍDICAS 17.1 La persona jurídica, sea o no proveedor de servicio, es responsable administrativamente por los delitos informáticos previstos en esta ley, y en el Código Penal, cuando estos hayan sido cometidos en su nombre y/o por cuenta de ellas y/o en su beneficio, directo o indirecto, por: 17.1.1 Sus administradores de hecho o derecho, representantes legales, contractuales y órganos colegiados, siempre que actúen en el ejercicio de las funciones propias de su cargo. 17.1.2 Las personas naturales que prestan cualquier tipo de servicio a la persona jurídica, con independencia de su naturaleza, del régimen jurídico en que se encuentren o de si media relación contractual y que, estando sometidas a la autoridad y control de los gestores y órganos mencionados en el literal anterior, actúan por orden o autorización de estos últimos. 17.1.3 Las personas naturales señaladas en el literal precedente cuando, en atención a la situación concreta del caso,	Tema nuevo. Se hace responsable a la persona jurídica por los delitos que se cometan en nombre suyo o sin que haya cumplido con observar el deber de cuidado. La intención de esta norma es que a través de mecanismos de prevención, la empresa pueda lograr resultar indemne, si prueba que actuó diligentemente y que el autor del delito burló sus controles. Las sanciones a imponer son las previstas en la ley 30424.

	no se ejerza sobre ellas el debido control y vigilancia por parte de los administradores de hecho o derecho, representantes legales, contractuales u órganos colegiados de la persona jurídica. 17.2 La responsabilidad administrativa prevista en este artículo es independiente de la responsabilidad penal que corresponda a las indicadas personas naturales. 17.3 Procederá la exención de responsabilidad administrativa de la persona jurídica, prevista en el presente artículo, en caso que: 17.3.1 Las personas naturales, señaladas en los numerales anteriores, hayan obrado en beneficio propio, o a favor de un tercero distinto a la persona jurídica. 17.3.2 La persona jurídica haya adoptado e implementado en su organización y con anterioridad a la comisión del delito, un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características, consistente en medidas de vigilancia y control idóneas para prevenir los delitos antes mencionados o para reducir significativamente el riesgo de su comisión. 17.4 Las sanciones aplicables como consecuencia de la responsabilidad administrativa son las previstas en la Ley No. 30424.	
Artículo 2. Acceso ilícito El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo,	**Artículo 18.- INTRUSISMO INFORMÁTICO** 18.1 El que sin contar con autorización o haciendo uso indebido de ella, accede o facilita a otro el acceso al conjunto o una parte de un sistema	Como se observa se ha desarrollado la figura penal de manera más específica. De otro lado se emplea el término de intrusismo en lugar de acceso ilícito, ya que es un delito se comete cuando una persona con ciertos

será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.**"**	informático, o se mantiene en el mismo, con la intención de obtener información, datos informáticos, o con cualquier otra intención delictiva, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con treinta a noventa días-multa. 18.2 La pena privativa de libertad será no menor de seis ni mayor de diez, cuando el intrusismo es cometido abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema informático en razón del ejercicio de un cargo o función, o tiene por fin la obtención de un beneficio económico para sí o para tercero. 18.3 La pena privativa de libertad será no menor de ocho ni mayor de quince cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.	conocimientos y habilidades informáticas viola las medidas de seguridad de un sistema utilizando su experiencia y conocimientos informáticos
Artículo 3. Atentado a la integridad de datos informáticos El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa. Artículo 4. Atentado a la integridad de sistemas informáticos	Artículo 19.-PERTURBACIÓN INFORMÁTICA 19.1 El que deliberadamente, valiéndose de cualquier medio, daña, borra, deteriora, altera, suprime, entorpece, hace inaccesible o imposibilita el funcionamiento de un sistema, una red, un programa o datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	Se ha desarrollado la figura, para incluir en la misma, no solo la afectación a los datos informáticos, sino a los sistemas, redes y programas, conjugando en un solo artículo lo dispuesto en los artículos 3 y 4 de la ley.

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	19.2 La pena privativa de la libertad será no menor de seis ni mayor de diez cuando el delito tiene por fin el sabotaje comercial o industrial, es cometido abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema informático, en razón del ejercicio de un cargo o función; o tiene por fin la obtención de un beneficio económico para sí o para tercero. 19.3 La pena privativa de libertad será no menor de ocho ni mayor de quince cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.	
"Artículo 7. Interceptación de datos informáticos El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa,	Artículo 20.- INTERCEPTACIÓN DE DATOS INFORMÁTICOS 20.1 El que deliberada e ilegalmente intercepta datos informáticos de terceros, en transmisiones no públicas, dirigidos, originados o efectuados dentro de un sistema informático, incluidas las emisiones electromagnéticas que transporten dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. 20.2 La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información información personal, comercial o industrial, secreta, reservada o confidencial 20.3 La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.	En todos los casos se ha incluido disposiciones destinadas a agravar la pena si se trata de afectaciones a la seguridad nacional o soberanía nacional, la administración de justicia o la función pública.

seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."	20.4 Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.	
Artículo 9. Suplantación de identidad El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.	Artículo 21.- SUPLANTACIÓN DE IDENTIDAD 21.1 Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años, el que empleando un sistema informático o la red, se hace pasar por otra persona suplantando su identidad, con el fin de: 16.1.1 Obtener un beneficio económico para sí o para tercero, 16.1.2 Generar algún perjuicio, material o moral a otra persona natural o jurídica, 16.1.3 Difundir mensajes que agravien el honor o la reputación de otra persona. 16.1.4 Incitar o ejercer violencia material o psicológica por razones de opinión, política, cultura, sexo, raza, origen o actividad. 16.1.5 Incitar al uso de la fuerza en contra de la autoridad 22.2 La pena La pena privativa de libertad será no menor de ocho ni mayor de doce cuando se haya suplantado a una institución del Estado Peruano u organismo extranjero acreditado en el país. 23.3 Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.	La suplantación de identidad no necesariamente tiene que derivar en un perjuicio para ser sancionada. La sola suplantación es delictiva, más aun el propósito podría no ser logrado y quedar impune. A través de esta suplantación se cometen otros delitos, es el delito medio y el delito fin puede ser de naturaleza comercial, personal o de favorecimiento de la pornografía infantil.

	Artículo 24.- CREACIÓN DE FALSA IDENTIDAD 24.1 Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años, el que empleando un sistema informático, o la red, crea una identidad inexistente, con el objeto de: 24.1.1 Obtener un beneficio económico para sí o para tercero, 24.1.2 Generar algún perjuicio, material o moral a otra persona natural o jurídica, 24.1.3 Difundir mensajes que agravien el honor o la reputación de otra persona. 24.1.4 Incitar o ejercer violencia material o psicológica por razones de opinión, política, cultura, sexo, raza, origen o actividad. 24.1.5 Incitar al uso de la fuerza en contra de la autoridad 24.2 Si el agente comete el delito como integrante de una organización criminal, o su actividad ilícita ha sido financiada o auspiciada por una institución o funcionario del Estado, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.	Esta figura es nueva y atiende a la necesidad de sancionar a quien crea identidad falsa para cometer similares delitos a los que se cometen con la suplantación.
Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4	Artículo 25.- PORNOGRAFIA INFANTIL 25.1 El que a través de la red u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de seis ni mayor de diez años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.	Se incluye en la figura penal la posesión de la pornografía con fines de comercialización.

y 9 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal".	25.2 Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal. 25.3 Si el agente produce, financia, ofrece, comercializa, publica, facilita, divulga o distribuye por cualquier medio, o se encuentra en su poder, con fines inequívocos de distribución o comercialización, material pornográfico obtenido en la forma descrita en los párrafos anteriores, la pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal. 25.4 La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.	
Artículo 8. Fraude informático El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.	Artículo 26.- FRAUDE INFORMÁTICO 26.1 Será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa, el que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante: 26.1.1 El diseño, introducción, alteración, borrado, supresión, extracción o clonación de datos informáticos de un registro o tarjeta, así como cualquier	Se han agravado las penas y se han precisado los tipos penales que puede incluir el fraude informático.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."	interferencia o manipulación en el funcionamiento de un sistema informático. 26.1.2 La formulación de ofertas engañosas, mediante alegaciones falsas respecto de cualquier elemento de dicha oferta, de modo que resulte un perjuicio económico. 26.1.3 La no entrega de productos adquiridos electrónicamente, por los que se ha recibido el valor convenido. 26.1.4 La obtención indebida de bienes o servicios sin erogar o asumir el compromiso de pago de la contraprestación debida. 26.2 La pena será privativa de libertad no menor de seis ni mayor de doce años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio de personas jurídicas dedicadas a obras de bienestar social, fondos destinados a programas asistenciales, o instituciones del Estado dedicadas a fines asistenciales.	
Artículo 10. Abuso de mecanismos y dispositivos informáticos El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de	Artículo 27. ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de	Esta figura se ha recogido de la ley actual.

cuatro años y con treinta a noventa días-multa."	cuatro años y con treinta a noventa días-multa."	
	SEGUNDA. Creación de Fiscalías Especializadas en Delitos Informáticos El Ministerio Público en un plazo máximo de treinta (30) días, emitirá la norma que disponga la creación de la Fiscalía Especializada en Delitos Informáticos, así como la forma, modo y oportunidad en que empezarán a funcionar.	En la exposición de motivos se desarrolla la necesidad de las fiscalías especializadas.

V. ALINEAMIENTO CON LAS POLITICAS NACIONALES

Debemos empezar por señalar que el presente proyecto se encuentra alineado con los Objetivos de Desarrollo Sostenible (ODS) contenidos en la Agenda 2030, ya que las Naciones Unidas reconocen a la tecnología es una herramienta para cumplir los procesos de implementación de los mismos, por ende las iniciativas que se orientan al uso ético de las mismas son positivas.

En el ámbito nacional, el Acuerdo Nacional define los lineamientos generales para lograr un desarrollo inclusivo, equitativo y sostenible, para afirmar la gobernabilidad democrática del país. Las políticas de Estado están agrupadas en cuatro grandes objetivos.

El Proyecto que presentamos se encuentra alineado con las políticas de Estado que pasamos a describir:

LINEAMIENTO	POLÍTICA DE ESTADO
DEMOCRACIA Y ESTADO DE DERECHO	9. Política de Seguridad Nacional
COMPETITIVIDAD DEL PAÍS	18. Búsqueda de la Competitividad, Productividad y Formalización de la Actividad Económica
	20. Desarrollo de la Ciencia y la Tecnología
ESTADO EFICIENTE, TRANSPARENTE Y DESCENTRALIZADO	26. Promoción de la ética, la transparencia y erradicación de la corrupción, el lavado de dinero, la evasión tributaria y el contrabando en todas sus formas
	35. Sociedad de la Información y Sociedad del Conocimiento.

Se alinea con todos los "Ejes Estratégicos" objetivos, lineamientos, prioridades y programas, que deben orientar las decisiones y acciones del Estado para alcanzar las metas de desarrollo al 2021, ya que el tema de la tecnología es transversal a los mismos.

Y finalmente con el Plan Nacional de Competitividad y Productividad, aprobado por Decreto Supremo N° 237-2019-EF en el Eje No. 03 de Innovación.