4237; 4344; 4352/2018-CR

- DEFENSA NACIONAL

CONGRESO DE LA REPÚBLICA
ÁREA DE TRAMITE DOCUMENTARIO
11 SEP 2019
RECIBIDO
Firma ..... Hora 9:06am

"Año de la lucha contra la corrupción y la impunidad"
"Decenio de la Igualdad de oportunidades para mujeres y hombres"

OFICIO Nº 244 -2019 –PR

Lima, 11 de setiembre de 2019

Señor
PEDRO OLAECHEA ÁLVAREZ CALDERÓN
Presidente del Congreso de la República
Presente.-

Tenemos el agrado de dirigirnos a usted, con relación a la Ley de ciberseguridad. Al respecto, estimamos conveniente observar la misma por lo siguiente:

1. En principio, la Autógrafa de Ley, establece en su artículo 3 que la Seguridad Digital es: *"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".*

   Al respecto, la referida definición ya está contenida en el Decreto Supremo 050-2018-PCM, mediante la cual se aprueba la "Definición de Seguridad Digital en el ámbito nacional", la misma que sirve de sustento para su integración como componente del concepto de Gobierno Digital y su correspondiente organización e institucionalización mediante el Marco de Seguridad Digital del Estado Peruano, ambos conceptos descritos en el Decreto Legislativo N° 1412, Ley de Gobierno Digital.

   Con lo anterior queda evidenciado que el espíritu de La Autógrafa, conforme lo señalado en el artículo 1 y 3, es regular un ámbito que ya viene siendo dirigido, supervisado y gestionado por la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital, de manera mucho más amplia y extensa a través de un arreglo institucional establecido para dicha finalidad por el Poder Ejecutivo contando con un marco legislativo vigente a la fecha.

2. En esa misma línea, el artículo 4 de la Autógrafa de Ley hace referencia a los "Principios de Ciberseguridad". Sobre ello, las propuestas de principios se abordan más como "disposiciones" de la parte sustantiva de una Ley que Principios orientadores. Por otro lado, conforme lo señalado en párrafos anteriores, su desarrollo es competencia de la Presidencia del Consejo de Ministros (ente rector de Gobierno Digital). Cabe indicar que en el artículo 5 del Decreto Legislativo N° 1412 ya se establecen principios vinculados con la "Seguridad Digital".

3. Consistente con lo anterior, el referido artículo 4 de la Autógrafa de Ley, específicamente en su numeral 4.2, define la "comunicación de incidentes" como un principio, en los términos siguientes: "*Se deberá crear mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental. Dichos mecanismos de comunicación de incidentes deberán mantener la reserva de los casos indicados, en los casos que pudiera su revelación afectar a las instituciones o a la sociedad, pero también deberá evaluarse los casos para divulgar dicha información a otros actores y a la sociedad. Tanto al compartimentaje como la diseminación de la información a los organismos pertinentes no debe afectar la Defensa o la Seguridad Nacional. En el caso que los incidentes impliquen violación a datos personales deberá informarse al funcionario público responsable de transparencia y acceso a la información pública y a la protección de datos personales, de dicha afectación. De igual manera los incidentes deberán ser reportados antes las autoridades competentes de acuerdo a la naturaleza de la entidad*

1

41530 ATD

vulnerada y de los individuos y entidades afectadas, para que respondan a dicha afectación en la medida de sus funciones".

Sobre el particular, consideramos que tal como está redactado el referido principio desarrolla disposiciones y procedimientos sobre la atención de incidentes, debiendo estar integrados en el Marco de Seguridad Digital del Estado Peruano o formar parte de disposiciones prescriptivas o procedimentales de La Autógrafa de Ley.

Por otro lado, corresponde a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en el marco de sus competencias y, sobre todo, en su calidad de ente rector en materia de Seguridad Digital, el establecimiento de los protocolos de comunicación, recepción, escalamiento, coordinación, reporte, intercambio y activación de incidentes de seguridad digital, conforme lo establece el artículo 13 de la Ley N° 30999, Ley de Ciberdefensa.

4. La Autógrafa de Ley en su Título II, "De la Ciberseguridad", Capítulo I, "Ciberseguridad en el Ámbito del Sector Público", artículo 5, crea el Comité de Ciberseguridad del Estado Peruano, el cual "(...) *deberá contar en su conformación con participantes del sector privado, sociedad civil, academia, comunidad técnica de Internet y sector gubernamental. Este comité estará adscrito a la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital será la secretaría técnica, quien coordinará con el secretario técnico del Consejo de Seguridad y Defensa Nacional (COSEDENA). El Comité tendrá como función formular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de CSIRT en el sector privado, gestionar el Fondo de Seguridad Digital, fomentar la cultura de Ciberseguridad, coadyuvar al fomento de currículos de educación superior en materia de Ciberseguridad y otras que las pudieran establecer la COSEDENA.*"

   Al respecto, de acuerdo a lo establecido en el artículo 29 del Decreto Supremo N° 054-2018-PCM, que aprueba los Lineamientos de Organización del Estado, los Comités son "*29.1 (...) un tipo de órgano colegiado sin personería jurídica ni administración propia que se crean para tomar decisiones sobre materias específicas. Sus miembros actúan en representación del órgano o entidad a la cual representan y sus decisiones tienen efectos vinculantes para éstos, así como para terceros, de ser el caso. 29.2 Los Comités se disuelven automáticamente cumplido su objeto y periodo de vigencia, de ser el caso.*"

   En ese sentido, en cumplimiento con la Ley N° 29158 Ley Orgánica del Poder Ejecutivo, el Comité de Ciberseguridad no puede formular la Política de Ciberseguridad por cuanto es materia exclusiva del Poder Ejecutivo. De igual manera, el referido Comité no puede gestionar el Fondo de Seguridad Digital que se constituye con fondos públicos.

   Más aún, el referido Comité de Ciberseguridad se superpone con el Comité de Alto Nivel por un Perú Digital Innovador y Competitivo, creado mediante Decreto Supremo Nº 118-2018-PCM, dado que este último tiene por objetivo promover políticas, iniciativas y programas para el desarrollo de la innovación, la competitividad, la transformación digital de procesos y servicios públicos, las competencias digitales, la inclusión digital y el desarrollo de aplicaciones para la economía digital, acciones que contemplan como componente transversal la Seguridad Digital.

   Asimismo, el referido Decreto Supremo señala en el numeral 3.3 del artículo 3 que *"El Presidente del Comité podrá invitar a participar en sus sesiones a titulares de otras entidades públicas o privadas cada vez que en éstas se traten objetivos que tengan relación con su competencia"*, con lo cual está habilitado para incorporar a actores del sector privado, la sociedad civil y la academia a fin de evaluar necesidades objetivas en materia de Seguridad Digital y tomar decisiones en dicho ámbito al más alto nivel en el país, conforme la definición del Decreto Supremo N° 050-2018-PCM.

2

5. Por otra parte, el artículo 7 de la Autógrafa de Ley busca crear un Equipo de Respuesta frente a Incidentes de Seguridad Informática, denominado CSIRT del Perú (Pe-CSIRT), en el ámbito de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, quien deberá establecer los estándares mínimos para que cualquier entidad pública, privada, sociedad civil, academia o comunidad técnica participe en el CSIRT del Perú.

   Sobre el particular, actualmente nuestro país ya cuenta con la Coordinadora de Respuesta de Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (PE-CERT), creada mediante Resolución Ministerial N° 360-2009-PCM, en el ámbito de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros. Cabe señalar que el Pe-CERT tiene entre sus objetivos:

   "(...)
   a. *Promover la coordinación entre las entidades de la administración de redes informáticas de la Administración Pública Nacional, para la prevención, detección, manejo, recopilación de información y desarrollo de soluciones para los incidentes de seguridad. (...)*
   e. *Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas de la Administración Pública Nacional y facilitar el intercambio de información para afrontarlos.*
   (...)
   h. *Interactuar con coordinaciones de similar naturaleza."*

   Conforme lo anterior, se realizan coordinaciones sectoriales con los oficiales de Seguridad de la Información de la Administración Pública para la atención de incidentes críticos, actividades de prevención y capacitación en seguridad de la información; asimismo, promueve acciones para fortalecer la cooperación y colaboración con instituciones del sector privado, academia, sociedad civil, organismos internacionales y países a nivel mundial en el intercambio de experiencias, investigaciones, entre otros.

   En esa línea, el artículo 7 de La Autógrafa de Ley duplica funciones, competencias e instancias que ya se encuentran a cargo de la Presidencia del Consejo de Ministros.

6. El artículo 8 de La Autógrafa de Ley señala que el Comité de Ciberseguridad del Estado Peruano establecerá los lineamientos para el establecimiento de CSIRTs en el sector privado, academia, sociedad civil y comunidad técnica; asimismo, fomentará instrumentos de cooperación público – privado en materia de ciberseguridad.

   Al respecto, la Presidencia del Consejo de Ministros ya tiene entre sus competencias la emisión de normas en materia de Seguridad Digital y atención de emergencias en redes teleinformáticas, que comprende el diseño y aprobación de lineamientos en materia de CSIRT, Unidades de Seguridad de la Información, Coordinadoras de Respuestas a Emergencias en Redes Teleinformáticas, responsabilidades y competencias del Oficial de Seguridad de la Información, ciberseguridad, entre otros, conforme lo establece su Reglamento de Organización y Funciones de la PCM, el Decreto Legislativo N° 1412, el Decreto Legislativo N° 604, Decreto Supremo N° 050-2018-PCM y la Resolución Ministerial N° 360-2009-PCM.

   Asimismo, la PE-CERT promueve la cooperación y colaboración con instituciones del sector privado, academia, sociedad civil, organismos internacionales y países a nivel mundial en el intercambio de experiencias, investigaciones, entre otros en dicho ámbito, conforme al Marco de Seguridad Digital del Estado Peruano, el cual se sustenta en la articulación con actores del sector público, sector privado y otros interesados. En esa línea, La Autógrafa duplica funciones y competencias asignadas a la Presidencia del Consejo de Ministros en el marco de su rectoría.

7. Además, la Tercera Disposición Complementaria Final de la Autógrafa de Ley ya ha sido recogida en la Tercera Disposición Complementaria Final de la Ley N° 30999, Ley de Ciberdefensa, por lo tanto ya existe un reconocimiento a las entidades que gestionen recursos críticos de Internet (nombres de dominio, números IP y protocolos) como entidades vinculadas a la ciberdefensa; por lo tanto ya son actores dentro del marco de seguridad digital.

8. En lo que respecta a la Cuarta Disposición Complementaria Final de la Autógrafa de Ley, referida al desarrollo del currículo de educación superior en dicha materia, resulta inviable evaluar la pertinencia del desarrollo de contenidos curriculares de las universidades y/o contenidos curriculares especializados, como el caso de los de educación superior tecnológica, toda vez que ello afectaría la autonomía que la Constitución Política del Perú y la Ley Universitaria le reconocen a las universidades, en particular respecto a la autonomía académica; así como lo señalado en la Ley N° 30512, Ley de Institutos y Escuelas de Educación Superior y de la Carrera Pública de sus Docentes, sobre la autonomía académica otorgada a los Institutos y Escuelas de Educación Superior para el desarrollo de sus programas de estudios.

9. Por otra parte, la propuesta de la Autógrafa de Ley de crear el Equipo de Respuesta frente a Incidentes de Seguridad Informática – CSIRT en el ámbito de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (artículo 7); al crear el Comité de Ciberseguridad del Estado Peruano, adscrito a la Presidencia del Consejo de Ministros (artículo 5), quien gestionará el Fondo de Seguridad Digital; y, al disponer el desarrollo de currículos especializados por parte del Ministerio de Educación (Cuarta Disposición Complementaria Final), conllevan la disposición de recursos públicos, generando gasto público.

   En este sentido, al generarse gasto público, resulta necesario especificar sobre el financiamiento de dicho gasto, y contar, como requisito para el inicio del trámite de la Autógrafa, con una evaluación presupuestal que demuestre la disponibilidad de los créditos presupuestarios que pueden ser destinados a su aplicación, así como el impacto de dicha aplicación en el Presupuesto del Sector Público para el Año Fiscal 2019, y un análisis costo beneficio en términos cuantitativos y cualitativos, conforme a lo dispuesto en los numerales 3 y 4 del numeral 2.2 del artículo 2 de la Ley de Equilibrio Financiero del Sector Público para el Año Fiscal 2019 (Ley N° 30880).

   Dicha exigencia se aplica, igualmente, a los gastos que supondría la implementación de las disposiciones de la Autógrafa, en los años fiscales subsiguientes, en cuyo caso, como se ha mencionado, afectaría la Caja Fiscal, contraviniendo el artículo 79 de la Constitución Política del Perú, y lo dispuesto en el inciso 1 del numeral 2.1 del artículo 2 del Decreto Legislativo del Sistema Nacional de Presupuesto Público (Decreto Legislativo N° 1440).

10. Finalmente, la Autógrafa de Ley atenta contra las recomendaciones de la OCDE en materia de gestión de riesgos de seguridad digital y pone en riesgo la incorporación del Perú a la OCDE. Pues, el Perú ya tiene un arreglo institucional que permite regular, dirigir, orientar y supervisar la Seguridad Digital en el país, el cual es gestionado por la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital, tal como se establece en el Decreto Supremo N° 022-2017-PCM, Decreto Legislativo N° 1412 y Ley N° 30999.

    Es así que, en la Cuarta Disposición Complementaria, la Autógrafa de Ley establece que el Ministerio del Interior es el ente rector de la Seguridad Digital en el Estado Peruano vulnerando lo establecido en el Decreto Legislativo N° 604 - que crea el Sistema Nacional de Informática, el Decreto Legislativo N° 1412 - que Aprueba la Ley de Gobierno Digital y, lo que dispone la reciente Ley 30999 - Ley de Ciberdefensa y la regulación digital establecida en el país que establecen que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en seguridad digital en el Perú.

En esa línea, el Estudio de Gobernanza Pública de la OCDE, publicado el año 2016, considera como recomendación fundamental "establecer el gobierno digital en el centro de la reforma del sector público", obligando al país a fortalecer la rectoría de gobierno digital en el centro de gobierno, esto es la Presidencia del Consejo de Ministros. Sumado a ello, recomiendan *"asegurar el liderazgo para una gobernanza, gestión y planificación más sólidas"* con lo cual, es la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, la que concentra la rectoría en materia digital y, en particular, la seguridad digital, conforme al Decreto Legislativo N° 1412 y a la Ley N° 30999, dando cumplimiento a los lineamientos de OCDE.

Además, el fortalecimiento de la gobernanza digital en el Perú fue reconocido en el Estudio de Gobierno Digital en el Perú de la OCDE 2019, la cual está sustentada en la rectoría integral de gobierno digital en la Presidencia del Consejo de Ministros y la Ley de Gobierno Digital.

Por consiguiente, la Autógrafa resulta entonces contraria a los avances en gobernanza digital reconocidos por OCDE ocasionando un serio incumplimiento de las recomendaciones en materia digital al fraccionar la rectoría en seguridad digital, desconociendo lo establecido en la regulación vigente y poniendo en riesgo el cumplimiento de las recomendaciones para el ingreso del Perú a la OCDE.

Por las razones expuestas, se observa la Autógrafa de Ley, en aplicación del artículo 108 de la Constitución Política del Perú, porque no cumple jurídicamente con el marco constitucional y es contradictoria con las disposiciones legales vigentes, lo que hará inviable su aplicación, sobre todo cuando colisiona con la política en dicha materia que ya se encuentra en marcha.

Atentamente,

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

SALVADOR DEL SOLAR LABARTHE
Presidente del Consejo de Ministros

4237;4344;4352/2018-CR

CONGRESO DE LA REPÚBLICA

Lima, 11 de setiembre de 2019

Pase a la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas, con cargo de dar cuenta de este procedimiento al Consejo Directivo.

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

LA COMISIÓN PERMANENTE DEL

CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE CIBERSEGURIDAD

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

La presente ley tiene por objeto establecer el marco normativo en materia de seguridad digital del Estado peruano.

Artículo 2. Ámbito de aplicación

La presente ley tiene alcance a todas las entidades del sector público de los niveles de gobierno. De igual manera tiene alcance sobre entidades del sector privado, academia y sociedad civil en lo que le aplique la presente ley.

Artículo 3. Definición

3.1 CSIRT.- Se define un CSIRT (equipo de respuesta frente a incidentes de seguridad informática) como un colectivo o una entidad dentro de un organismo que ofrece servicios y soporte a un grupo en particular (comunidad objetivo) con la finalidad de prevenir, gestionar y responder a incidentes de seguridad digital. Estos equipos deben estar conformados por especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de coadyuvar a mitigar el riesgo de los ataques cibernéticos.

3.2 Seguridad digital.- Es 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.

Artículo 4. Principios de la ciberseguridad

4.1 Respeto de los derechos humanos en el ejercicio de la ciberseguridad

Se deberán tomar en consideración en todo desarrollo normativo y de políticas en materia de ciberseguridad el respeto irrestricto a los derechos humanos, en concordancia con la Constitución Política del Perú y los acuerdos internacionales en la materia.

4.2 Comunicación de incidentes

Se deberá crear mecanismos de comunicación de incidentes entre la sociedad civil, el sector privado, la academia, la comunidad técnica y el sector gubernamental. Dichos mecanismos de comunicación de incidentes deberán mantener la reserva de los casos indicados, en los casos que pudiera su revelación afectar a las instituciones o a la sociedad, pero también deberá evaluarse los casos para divulgar dicha información a otros actores y a la sociedad. Tanto el compartimentaje como la diseminación de la información a los organismos pertinentes no debe afectar la defensa o la seguridad nacional.

En el caso de que los incidentes impliquen violación a datos personales deberá informarse al funcionario público responsable de transparencia y

acceso a la información pública y a la protección de datos personales, de dicha afectación.

De igual manera los incidentes deberán ser reportados ante las autoridades competentes de acuerdo a la naturaleza de la entidad vulnerada y de los individuos y entidades afectadas, para que respondan a dicha afectación en la medida de sus funciones.

TÍTULO II

DE LA CIBERSEGURIDAD

CAPÍTULO I

CIBERSEGURIDAD EN EL ÁMBITO DEL SECTOR PÚBLICO

Artículo 5. Comité de Ciberseguridad del Estado Peruano

Dispóngase la creación del Comité de Ciberseguridad del Estado Peruano, el mismo que deberá contar en su conformación con participación del sector privado, sociedad civil, academia, comunidad técnica de Internet y sector gubernamental. Este comité estará adscrito a la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital será la secretaría técnica, quien coordinará con el secretario técnico del Consejo de Seguridad y Defensa Nacional (COSEDENA).

El Comité tendrá como función formular la Política de Ciberseguridad del Estado Peruano, generar lineamientos en materia de CSIRT en el sector privado, gestionar el Fondo de Seguridad Digital, fomentar la cultura de ciberseguridad, coadyuvar al fomento de currículos de educación superior en materia de ciberseguridad y otras que les pudiera establecer la COSEDENA.

La conformación del Comité de Ciberseguridad del Estado Peruano será establecida en el reglamento de la presente ley.

9

<u>Artículo 6</u>. Marco de seguridad digital del sector gubernamental

Los principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la administración pública, serán establecidos por la Secretaría de Gobierno Digital.

<u>Artículo 7</u>. Establecimiento del Pe-CSIRT

Créase, en el ámbito de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, el CSIRT del Perú.

La Secretaría de Gobierno Digital establecerá los estándares mínimos que se deberá cumplir para participar en el CSIRT del Perú, por parte de cualquier entidad pública, privada, de la sociedad civil, de la academia o de la comunidad técnica.

CAPÍTULO II

CIBERSEGURIDAD EN EL ÁMBITO DEL SECTOR PRIVADO

<u>Artículo 8</u>. Lineamientos para el establecimiento de CSIRTs en sector privado

El Comité de Ciberseguridad del Estado Peruano establecerá los lineamientos para el establecimiento de CSIRTs en el sector privado, la academia, la sociedad civil y la comunidad técnica. De igual manera fomentará el desarrollo de instrumentos de cooperación público-privado en materia de ciberseguridad.

<u>Artículo 9</u>. Cooperación público-privada en materia de ciberseguridad

Las entidades públicas y privadas, así como de la academia, la sociedad civil y la comunidad técnica deberán tener como principio a la cooperación para el mantenimiento de la ciberseguridad a nivel del Estado peruano.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación del numeral 8) del artículo 2 del Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI

Modifíquese el numeral 8) del artículo 2 del Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, en los siguientes términos:

> *"**Artículo 2.- Definiciones***
>
> *Para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo, se entenderá por:*
>
> *[...]*
>
> *Seguridad Digital: Es 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."*

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación en materia de ciberseguridad

La Presidencia del Consejo de Ministros mediante decreto supremo aprueba el reglamento de la presente ley, en lo referido a ciberseguridad, en un plazo

máximo de noventa (90) días, contados a partir del día siguiente de su publicación en el diario oficial El Peruano.

SEGUNDA. Modificaciones a normas de la Policía Nacional del Perú en materia de ciberseguridad

El Ministerio del Interior, en un plazo de noventa (90) días, contados a partir de la fecha de entrada en vigencia de la presente ley, presentará las modificaciones, derogaciones e incorporaciones a las normas correspondientes a la Policía Nacional del Perú en materia de la presente ley.

TERCERA. Recursos críticos de Internet

Se reconoce a las entidades que gestionen recursos críticos de Internet (nombres de dominio, números IP y protocolos) en su naturaleza de entidades vinculadas a la seguridad digital debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad seguridad digital nacional.

CUARTA. Desarrollo del currículo de educación superior en materia de ciberseguridad

El Ministerio del Interior, en su calidad de ente rector en materia de seguridad digital, coordina con el Ministerio de Educación, la pertinencia del desarrollo de contenidos especializados en materia de seguridad digital, que incluye la ciberseguridad, en las instituciones de educación superior universitaria y tecnológica, a nivel de pre y postgrado. Para ello, establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

QUINTA. De la participación de los organismos reguladores del Estado

Para la conformación del Comité de Ciberseguridad del Estado Peruano, propuesto en el artículo 5 de la presente ley, se deberá considerar la

participación de los organismos reguladores de la inversión privada en los servicios públicos.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróguese la segunda disposición complementaria final de la Ley 30618, Ley que modifica el DL 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veinte días del mes de agosto de dos mil diecinueve.

PEDRO C. OLAECHEA ÁLVAREZ CALDERÓN

Presidente del Congreso de la República

KARINA JULIZA BETETA RUBÍN

Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE DE LA REPÚBLICA