

Lima, 11 de febrero de 2020

OFICIO N° 008-2020-GTU.DU.006-2020:007-2020/CR

Señor Congresista

PEDRO OLAECHEA ÁLVAREZ - CALDERÓN

Presidente de la Comisión Permanente del Congreso de la República

Presente.-

109 folios
CONGRESO DE LA REPÚBLICA
Área de Trámite y Digitalización de Documentos

17 FEB 2020

RECIBIDO

Firma Hora 5:19

Referencia: Oficio N° 198-2019-2020-ADP-CP/CR.

De mi especial consideración:

Es grato dirigirme a usted a fin saludarlo cordialmente y remitirle el Informe Final del Grupo de Trabajo de la Comisión Permanente encargado del examen del **Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento**, que fuera aprobado por unanimidad, en la Primera Sesión del respectivo Grupo de Trabajo; así como el expediente, conteniendo la documentación en folios.

Habiendo concluido con el encargo de la Comisión Permanente, señalado en el Oficio N° 198-2019-2020-ADP-CP/CR, solicito a usted tenga a bien agendar su debate y votación del presente informe en la sesión del Pleno de la Comisión Permanente.

Hago propicia la ocasión para expresarle los sentimientos de mi mayor consideración y alta estima.

Atentamente,



ÁNGEL NEYRA OLAYCHEA
Congresista de la República
COORDINADOR

Grupo de Trabajo que examina
Decretos de Urgencia 006-2020 y 007-2020

GRUPO DE TRABAJO DECRETO DE URGENCIA 007-2020

SEÑOR PRESIDENTE:

Se ha dado cuenta para examen e informe correspondiente el **Decreto de Urgencia 007-2020**, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

El presente informe ha sido aprobado por **UNANIMIDAD** de los congresistas presentes, en la Primera Sesión del Grupo de Trabajo, celebrada el 10 de febrero de 2020, en la Sala María Elena Moyano, Palacio Legislativo, del Congreso de la República. Votaron a favor los señores congresistas **José Marvin Palma Mendoza** (C21) y **Ángel Neyra Olaychea** (FP).

El Informe del Grupo de Trabajo consta de cinco secciones: (i) La primera sección se desarrolla los antecedentes que motivaron la dación del Decreto de Urgencia 007-2020; (ii) la segunda sección está dedicada a describir el marco constitucional que sustenta el examen del Decreto de Urgencia 007-2020; (iii) en la tercera sección se resume el contenido del Decreto de Urgencia 007-2020; (iv) en la cuarta sección se examina en detalle el Decreto de Urgencia 007-2020; (v) en la quinta sección se detallan las conclusiones; y, finalmente, en la (vi) sexta sección se plantean las recomendaciones del Grupo de Trabajo.



1. ANTECEDENTES

1.1. Antecedentes generales

El 30 de setiembre de 2019, mediante el Decreto Supremo N° 165-2019-PCM, el Presidente de la República, disolvió el Congreso de la República, considerando que existía una “negación fáctica” a la cuestión de confianza solicitada por el Presidente del Consejo de Ministros; asimismo, convocó a elecciones para un nuevo Congreso, para completar el Período Parlamentario del Congreso disuelto.

Con fecha 10 de octubre de 2019, el señor Pedro Olaechea Álvarez Calderón, en su condición de Presidente de la Comisión Permanente del Congreso de la República, presentó demanda competencial contra el Poder Ejecutivo ante el Tribunal Constitucional, la que fue admitida a trámite el 29 de octubre de 2019. El Tribunal Constitucional en su sesión del 14 de enero de 2020, declara infundada dicha demanda competencial.

De acuerdo al artículo 134 de la Constitución Política *“Disuelto el Congreso, se mantiene en funciones la Comisión Permanente, la cual no puede ser disuelta”*. Asimismo, la Constitución Política en su artículo 135, señala que: *“En este interregno, el Poder*

Ejecutivo legisla mediante decretos de urgencia, de los que da cuenta a la Comisión Permanente para que los examine y los eleve al Congreso, una vez que éste se instale”.

El presente informe se circunscribe a la descripción de hechos que antecedieron a la disolución del Congreso, a fin de poner en contexto las circunstancias en la que se delega al presente Grupo de Trabajo elaborar el Informe del Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

1.2. Antecedentes procedimentales

El 9 de enero de 2020 el Poder Ejecutivo publicó en el Diario Oficial El Peruano el **Decreto de Urgencia 007-2020**, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

El 10 de enero de 2020, mediante Oficio N° 007-2020-PR, ingresó al Área de Trámite Documentario del Congreso de la República el Decreto de Urgencia 007-2020 y fue remitida a la Comisión Permanente.

En la sesión de la Comisión Permanente, de fecha 16 de enero de 2020, se acordó designar como coordinador para la elaboración el Informe sobre el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, al congresista **Ángel Neyra Olaychea** (FP), con la participación del señor congresista **Marvin Palma Mendoza** (C21).

El Grupo de Trabajo se instaló el 22 de enero de 2020, en Sala “María Elena Moyano”, Palacio Legislativo, con la asistencia de los señores congresistas Ángel Neyra Olaychea (FP) y Marvin Palma Mendoza (C21).

El 30 de enero de 2020 el Grupo de Trabajo realizó su primera sesión¹, en la Sala “María Elena Moyano”, Palacio Legislativo, del Congreso de la República, con la asistencia del señor congresista Ángel Neyra Olaychea (FP). En esta sesión sustentaron los fundamentos del contenido del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, así como respondieron a las preguntas formuladas por los señores congresistas, los siguientes representantes del Poder Ejecutivo:

- Señora **Marushka Chocobar Reyes**, Directora de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.
- Señor **Eduardo Salcedo Guillen**, representante del Gabinete de Asesores del Ministerio de Justicia y Derechos Humanos.
- Señor **Eduardo Luna Cervantes**, Director de la Autoridad de Protección de Datos, del Ministerio de Justicia y Derechos Humanos.

¹ Por falta de quórum dicha sesión se desarrolló una sesión informativa.

- Señora **Wendy Ledesma Orbegozo**, Directora de la Autoridad Nacional de Protección del Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – Indecopi.

Con la información recibida y los lineamientos generales presentados por el congresista Ángel Neyra Olaychea (FP), Coordinador, el tema de estudio quedó expedito para emitir el informe y someterlo a debate en la siguiente sesión del grupo de trabajo, la misma que se realizó el 10 de febrero de 2020.

2. MARCO CONSTITUCIONAL

Este Grupo de Trabajo, a quien se le ha delegado el examen del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, debe establecer el marco constitucional y legal básico que le permita delimitar los alcances del decreto de urgencia para su estudio y control, conjuntamente con el Congreso de la República, respecto a la facultada legislativa extraordinaria del Poder Ejecutivo, en el interregno parlamentario.

Para el desarrollo del presente informe de estudio y análisis del Decreto de Urgencia 007-2020, el marco constitucional y legal, principalmente aplicable, lo constituyen el artículo 135 de la Constitución Política, así como los artículos 118, inciso 19, y 123, inciso 3. Asimismo, el Reglamento del Congreso de la República en su artículo 91, y la costumbre y los precedentes parlamentarios, en tanto fuentes del derecho.

Asimismo, la Comisión Permanente, en su sesión del 18 de diciembre de 2019, una de las conclusiones que arribó², en consonancia con el marco constitucional, en relación a la facultad legislativa “extraordinaria” del Poder Ejecutivo determinó que:

“El Poder Ejecutivo emite decretos de urgencia de forma extraordinaria en dos momentos (artículos 118 y 135 de la Constitución Política del Perú). Ambos instrumentos coinciden en su denominación, pero tienen naturaleza, presupuestos habilitantes, materia legible, límites y procedimiento de control (político y jurídico) diferentes. La indicada facultad legislativa extraordinaria del artículo 135 no debería entenderse como absoluta.

*El Ejecutivo solo debe recurrir a la facultad legislativa extraordinaria en el periodo de interregno parlamentario ante la necesidad de **normas urgentes**, respetando los **principios de razonabilidad y proporcionalidad**, de tal manera que, no pueda afectar el sistema democrático y el estado de derecho constitucional. [Lo resaltado en negrita es nuestro].*

² Durante el debate de aprobación del Informe Final del Grupo de Trabajo encargado de examinar el Decreto de Urgencia 002-2019, Decreto de Urgencia que aprueba medidas para la realización de elecciones para un nuevo Congreso.

Existen materias durante el interregno que son incompatibles con la facultad legislativa extraordinaria del Poder Ejecutivo: reforma constitucional, normas que forman parte del bloque constitucional, reserva de ley orgánica, limitación de derechos fundamentales, tratados o convenios internacionales, autorización de viaje del Presidente de la República, nombramiento, ratificación o remoción de altos funcionarios, reglamento del Congreso, normas que requieren votación calificada e ingreso de tropas al país con armas". [Lo resaltado en negrita es nuestro].

Por lo tanto, el Grupo de Trabajo examinará si la dación del Decreto de Urgencia 007-2020, de conformidad con el marco normativo establecido, **corresponden a normas urgentes** y si se respetó los **principios de razonabilidad y proporcionalidad**, sin afectar el sistema democrático y el estado de derecho constitucional. Asimismo, se examinará si la dación del Decreto de Urgencia 007-2020 son incompatibles con la facultad legislativa extraordinaria del Poder Ejecutivo, respecto a la **reserva de Ley de Presupuesto y sobre modificaciones presupuestales**.

2.1 Sobre la urgencia de los Decretos



El examen que debería realizar la Comisión Permanente del Congreso de la República, sobre la necesidad de la urgencia, implica analizar que los Decretos de Urgencia deben dictar medidas extraordinarias, en el sentido señalado por la Constitución Política y el Reglamento del Congreso, esto es, *"que su expedición responda a circunstancias anormales e imprevistas que demanden una acción inmediata. (...) [y, que], la expedición de los Decretos de Urgencia se sustenta en situaciones anormales e imprevisibles que por el mismo hecho de no poder evitarse su ocurrencia, toman al Estado por sorpresa, debiendo éste adoptar las medidas extraordinarias y urgentes que permitan paliar los efectos de dichas situaciones. En tal sentido, toda vez que se justifican por la presencia de circunstancias imponderables y no susceptibles de ser afrontadas a través de los mecanismos y procedimientos ordinarios y/o normales"*³.

Las daciones de los decretos de urgencia se justifican por la presencia de circunstancias imponderables y no susceptibles de ser afrontadas a través de mecanismos y procedimientos ordinarios; por lo tanto, los decretos de urgencia deben responder, a su vez, a un espacio temporal, debiendo ser lo suficientemente razonable como para superar la situación presentada o permitirle al Estado adoptar las medidas conducentes a tal fin (véase los pronunciamientos recaídos en los Expedientes N° 0008-2003-AI/TC, 17-2004-AI/TC y 708-2005-PA/TC).

Respecto a las situaciones imprevisibles, de emergencia o urgencia, César Landa Arroyo advierte que es un error común en la formulación de decretos de urgencia, que el Poder Ejecutivo confunda las situaciones extremas o preocupantes (que requieren una actuación previsible y permanente) con temas urgentes, de necesidad o urgencia, de

³ "El control parlamentario de los decretos legislativos y los decretos de urgencia en el Perú", Javier Bedoya de Vivanco.

crisis, de “carácter desesperado” o imprevisibles (...)”⁴. Entonces, sobre la materia es menester indicar que el criterio de excepcionalidad establece que el decreto de urgencia debe estar orientado a **revertir situaciones extraordinarias⁵ e imprevisibles**.

2.2 Sobre el principio de razonabilidad

Los principios de razonabilidad y proporcionalidad fueron establecidos expresamente en la parte final del artículo 200 de la Constitución Política, a propósito de la no suspensión del hábeas corpus y del amparo en períodos de estado de excepción. Si bien los principios de razonabilidad y proporcionalidad son principios distintos y tienen significados lingüísticos y jurídicos diferentes, el Tribunal Constitucional ha hecho de los mismos en múltiples sentencias que ha emitido. Sin embargo, “a la luz de la jurisprudencia constitucional peruana, esta diferenciación de la proporcionalidad y la razonabilidad es difícil”⁶.

En la siguiente cita, el Tribunal Constitucional dio la mejor referencia para hallar el concepto de razonabilidad que usa en sus sentencias: *“El principio de razonabilidad implica encontrar justificación lógica en los hechos, conductas y circunstancias que motivan todo acto discrecional de los poderes públicos. este principio adquiere mayor relevancia en el caso de aquellos supuestos referidos a restringir derechos o, para fines del caso, despojar de las prerrogativas que actúan como garantías funcionales para determinados funcionarios públicos”*⁷.

Entonces, para Marcial Rubio, el principio de razonabilidad exige encontrar justificación lógica, y esta es la disciplina de lo que es racionalmente demostrable, en general, y dentro del uso común, se utiliza la expresión justificación lógica no solo para lo que es racionalmente demostrable, sino también para lo que, sin cumplir tal requisito, es aceptado generalmente y que se conoce como tópica. De esta manera, podemos decir que el principio de razonabilidad exige que las conductas o, en términos jurídicos, los actos, para dar el significado de contenido voluntario que los sujetos realizan frente a los hechos y circunstancias, deben cumplir el requisito de ser generalmente aceptados por la colectividad como adecuada respuesta a los retos que presenta la realidad frente al actuar humano jurídicamente relevante.

Un aspecto fundamental de la razonabilidad como principio constitucional es el rechazo a la arbitrariedad, lo dice el Tribunal Constitucional: “Por ello, el principio de razonabilidad, implícitamente derivado del principio de igualdad, y expresamente formulado en el artículo

⁴ LANDA ARROYO, César. Op. Cit. Pp. 144-146.

⁵ «[...] a revertir situaciones extraordinarias e imprevisibles, condiciones que deben ser evaluadas en atención al caso concreto y cuya existencia, desde luego, no depende de la «voluntad» de la norma misma, sino de datos fácticos previos a su promulgación y objetivamente identificables. Ello sin perjuicio de reconocer, tal como lo hiciera el Tribunal Constitucional español —criterio que este Colegiado sustancialmente comparte— que «en principio y con el razonable margen de discrecionalidad, es competencia de los órganos políticos determinar cuándo la situación, por consideraciones de extraordinaria y urgente necesidad, requiere el establecimiento de una norma» (STC N.º 29/1982, fs. N.º 3)». (Fundamento jurídico N.º 60).

⁶ La interpretación de la Constitución según el Tribunal Constitucional, Marcial Rubio Correa, p- 162.

⁷ Sentencia del Tribunal Constitucional emitida el 1 de diciembre de 2003 en el Exp_0006_2003_AI_TC, sobre acción de inconstitucionalidad interpuesta por 65 congresistas contra el inciso j, artículo 89 del Reglamento del Congreso de la República.

200° de la Constitución, no tolera ni protege que se realicen o expidan actos o normas arbitrarias. Razonabilidad, en su sentido mínimo, es lo opuesto a la arbitrariedad y a un elemental sentido de justicia⁸.

En síntesis, la definición que podemos dar del principio de razonabilidad a partir de la jurisprudencia del Tribunal Constitucional es la siguiente: el principio de razonabilidad exige que los actos que los sujetos realizan frente a los hechos y circunstancias cumplan el requisito de ser generalmente aceptados por la colectividad como una respuesta adecuada a los retos que presenta la realidad frente al actuar humano jurídicamente relevante. dichos actos deben estar sostenidos en argumentos de razonamiento objetivos y no subjetivos, en valores y principios aceptados. debe hacerse un tratamiento imparcial de las personas y, cuando sea pertinente, se debe aplicar la regla de que «donde hay la misma razón, hay el mismo derecho». (Rubio, 2010).

2.3 Sobre el principio de proporcionalidad

Los principios de razonabilidad y proporcionalidad fueron establecidos expresamente en la parte final del artículo 200 de la Constitución Política, a propósito de la no suspensión del hábeas corpus y del amparo en periodos de estado de excepción. Si bien los principios de razonabilidad y proporcionalidad son principios distintos y tienen significados lingüísticos y jurídicos diferentes, el Tribunal Constitucional ha hecho de los mismos en múltiples sentencias que ha emitido. Sin embargo, "a la luz de la jurisprudencia constitucional peruana, esta diferenciación de la proporcionalidad y la razonabilidad es difícil"⁹.

A diferencia de lo que sucede con el principio de razonabilidad, en el caso del de proporcionalidad el Tribunal Constitucional no ha intentado elaborar una definición, al menos hasta donde hemos podido ubicar las referencias a él en las sentencias de dicha entidad. Ante esta situación Marcial Rubio ensaya la siguiente definición: "el principio de proporcionalidad mide la calidad o la cantidad de dos elementos jurídicos (o de elementos con relevancia jurídica) comparativamente entre sí, de manera que no haya un exceso de volumen, de significación o de cuantía entre uno y otro a partir de las consideraciones que se hacen en relación con cada tiempo y lugar".

Además, Rubio señala que, aunque el Tribunal Constitucional no se haya referido a una definición similar, la proporcionalidad no depende de criterios absolutos sino de criterios relativos al tiempo y al lugar en que se resuelve el problema jurídico. en otras palabras, depende de las ideas predominantes en la sociedad o en el grupo social de que se trate, sobre las proporciones aproximadas que es necesario aplicar en dicha situación. esto vincula al principio de proporcionalidad con el de razonabilidad, en la medida en que las ideas predominantes, el sentido común y la apreciación grupal forman parte de la definición de la razonabilidad.

⁸ Sentencia del Tribunal Constitucional emitida el 5 de julio de 2004 en el Exp_0090-2004-AA/TC sobre acción de amparo interpuesta por don Juan Carlos Callegari Herazo contra el Ministerio de Defensa.

⁹ La interpretación de la Constitución según el Tribunal Constitucional, Marcial Rubio Correa, p- 162.

Entonces, La diferencia está en que, mientras la razonabilidad consiste en expresar buenas razones para la conducta frente a las ocurrencias de la realidad, la proporcionalidad busca encontrar una adecuada relación de volumen, significación o cuantía entre dos elementos jurídicos (o de relevancia jurídica) entre si.

2.4 Sobre materias incompatibles: Ley de presupuesto y sobre modificaciones presupuestales

El Poder Ejecutivo ha reconocido que existen materias que inexorablemente son o serían incompatibles con la facultad extraordinaria del Poder Ejecutivo durante el interregno parlamentario, reconocimiento expresado en el Informe Legal N° 389-2019-JUS/DGDNCR¹⁰. Entre estas materias se encuentran: (i) reforma constitucional; (ii) normas que forman parte del bloque constitucional; (iii) reserva de ley orgánica; (iv) limitación de derechos fundamentales; (v) tratados o convenios internacionales; (vi) autorización de viaje del Presidente de la República; (vii) materia tributaria; (viii) nombramiento, ratificación o remoción de altos funcionarios; (ix) Reglamento del Congreso; (x) normas que requieren votación calificada; e, (xi) ingreso de tropas al país con armas.

Al respecto, en el análisis realizado por el Poder Ejecutivo no hace mención al procedimiento de la Ley de Presupuesto y sobre modificaciones presupuestales, es necesario precisar que, la Constitución Política en sus artículos 80 (tercer párrafo) y 101 numeral 3, establece que **los créditos suplementarios, habilitaciones y transferencias de partidas se tramitan ante el Congreso de la República** tal como la "Ley de Presupuesto", y que le corresponde tal atribución a la Comisión Permanente durante el receso parlamentario. **Sobre la materia, parte de la doctrina señala que lo anterior no puede tener excepción alguna**¹¹.

Entonces, según Edgar Carpio: *"han de considerarse excluidas de la regulación de los decretos de urgencia todas aquellas materias que se hallen sujetas a reservas de ley cualificadas, como es el caso de las materias que solo se puedan regular mediante leyes orgánicas, o aquellas otras para las cuales la Constitución exige que medie un consenso especial entre los representantes de la voluntad general, como puede ser el establecimiento de tratamientos tributarios especiales a los que se refiere el último párrafo del artículo 79 de la Constitución"*.

¹⁰ Elaborado por la Dirección General de Desarrollo Normativo y Calidad Regulatoria del Ministerio de Justicia y Derechos Humanos, de fecha 7 de octubre de 2019.

¹¹ "Los créditos suplementarios, habilitaciones y transferencias de partidas son diversas modificaciones que se van haciendo al Presupuesto, conforme avanza su ejecución. Como se trata de aprobación de ingresos y egresos debe ser hecha también por el Congreso. Por eso dice la Constitución que se tramitan ante el Congreso como la Ley de Presupuesto y en el receso ante la Comisión Permanente, la que para aprobarlos requiere tres quintos del número legal de sus miembros". RUBIO CORREA, Marcial (1999). Estudio de la Constitución Política de 1993 (Vol. III) Lima: PUCP, p. 459:

"En síntesis, hemos podido apreciar que el requisito de legislar respecto a materias económicas o financieras no puede dejar de lado el contenido expreso de la Constitución. Así, es evidente que lo establecido en el párrafo tercero del artículo 80 de la Constitución es, asimismo, pauta de análisis para dilucidar qué materia económica o financiera puede ser regulada mediante un Decreto de Urgencia. Por ello, bien puede afirmarse que la materia presupuestaria, en general, no está vedada para la legislación de urgencia, pero sí, en específico, el otorgamiento de créditos suplementarios, transferencias de partidas y habilitaciones". BEDOYA DE VIVANCO, Javier. Op. Cit. P. 1340.

Por lo tanto, las facultades legislativas extraordinarias del Poder Ejecutivo para legislar mediante decretos de urgencia tampoco alcanza a aquellas materias cuya regulación solo se pueda realizar mediante actos legislativos propios al Congreso de la República (por ejemplo, modificaciones al reglamento parlamentario), para aprobar reformas constitucionales o solicitar créditos suplementarios, habilitaciones y transferencias de partidas presupuestales, *“pues durante el interregno parlamentario la competencia que la Constitución confiere al Poder Ejecutivo solo lo es para “legislar” y no para transformarse en un poder constituyente derivado, como la doctrina suele denominar al poder de reforma constitucional”* (Carpio). Este es el caso para lo relacionado a la **Ley de Presupuesto y sobre modificaciones presupuestales**.

3. CONTENIDO DEL DECRETO DE URGENCIA 007-2020

El Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, tiene por objeto fortalecer la confianza de las personas, entidades y sociedad en general, en su interacción con los servicios que prestan las entidades públicas y organizaciones privadas, a través de la implementación de medidas en materia de confianza y seguridad digital.

Para tal efecto, el texto normativo establece el “Marco de Confianza Digital”, el cual está constituido por el “conjunto de principios, modelos, políticas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital”. Asimismo, establece que tiene tres ámbitos; (i) Protección de datos personales a cargo del Ministerio de Justicia y Derechos Humanos; (ii) Protección del Consumidor a cargo del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual; y, (iii) Seguridad Digital a cargo de la Presidencia del Consejo de Ministros (PCM), a través de la Secretaria de Gobierno Digital, la que a su vez se constituye en ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos.

Respecto de lo establecido, corresponde a la Secretaria de Gobierno Digital: formular, dirigir y supervisar el cumplimiento de la estrategia de Confianza Digital a nivel nacional, emitiendo lineamientos y directivas, articulando acciones y medidas; así como mantener informado al Presidente del Consejo de Ministros sobre los resultados e incidentes de seguridad digital que hayan sido notificados en el Centro Nacional de Seguridad Digital cuando corresponda.

En tal sentido, con fines de implementación, se crea el **Centro Nacional de Seguridad Digital**, a cargo de la secretaria de Gobierno Digital de la PCM en calidad de plataforma encargada de gestionar la respuesta y recuperación ante incidentes de seguridad digital. Asimismo, se crea el **Registro Nacional de Incidentes de Seguridad Digital** a fin de *“recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución”*.

Un aspecto importante es la obligación que se establece, para los proveedores de servicios digitales, (i) para notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital e (ii) implementar medidas y controles para garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.

Respecto del “uso ético de las tecnologías digitales y de los datos”, la norma crea el **Centro Nacional de Datos**, a cargo de la Secretaría de Gobierno Digital de la PCM, como una plataforma digital que gestiona, y supervisa la operación, educación, promoción, colaboración y cooperación de datos a nivel nacional.

Con relación a las disposiciones complementarias finales, se precisa que el Reglamento correspondiente será aprobado en noventa (90) días y que la Secretaría de Gobierno Digital se encargará de impulsar y gestionar la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE) a las que se refiere la Ley 29904, debiendo encargarse cada entidad de la Administración Pública de la contratación de los servicios necesarios para su conectividad de conformidad con lo dispuesto en el artículo 19 de dicha Ley. Respecto de las disposiciones transitorias finales, se establece que en noventa (90) días, la Secretaría de Gobierno Digital implementará el Registro Nacional de Incidentes de Seguridad Digital citado líneas arriba, y aprobará los lineamientos necesarios para su adecuado funcionamiento.



El decreto de urgencia también estipula que el ámbito de aplicación abarca a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionan a partir de la entrada en vigencia de la misma.

Finalmente, la implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

4. EXAMEN DEL DECRETO DE URGENCIA 007-2020

Es relevante precisar que el Tribunal Constitucional ha señalado¹² que corresponde al Parlamento realizar el control de constitucionalidad de los decretos de urgencia, pero que dicho control de constitucionalidad no es el mismo que realiza el Tribunal Constitucional, sino que, por la propia naturaleza del órgano que lo realiza y de la composición plural de quienes lo integran, es siempre un control de naturaleza política.

En ese sentido, como se ha mencionado, el presente Grupo de Trabajo examinará si la dación del Decreto de Urgencia 007-2020, corresponde a una **norma urgente** y si se

¹² Sentencia 0004-2011-PI/TC del 22 de setiembre de 2011.

respetó los **principios de razonabilidad y proporcionalidad**, sin afectar el sistema democrático y el estado de derecho constitucional. Asimismo, se examinará si la dación de los Decretos de Urgencia 007-2020 es incompatible con la facultad legislativa extraordinaria del Poder Ejecutivo, respecto a lo referido a la **Ley de Presupuesto y sobre modificaciones presupuestales**, específicamente a materias cuya regulación solo se pueda realizar mediante actos legislativos propios al Congreso de la República.

Entonces, el presente Grupo de Trabajo inicia el examen del Decreto de Urgencia 007-2020, evaluando si hubo necesidad y urgencia de la dación de decreto de urgencia.

4.1 Sobre la necesidad y urgencia del Decreto de Urgencia 007-2020

El examen que realiza el Grupo de Trabajo, sobre la necesidad y de la urgencia, implica analizar que el Decreto de Urgencia 007-2020 dicta medidas extraordinarias, en el sentido señalado por la Constitución Política y el Reglamento del Congreso, esto es, *“que su expedición responda a circunstancias anormales e imprevistas que demanden una acción inmediata. (...) [y, que], la expedición de los Decretos de Urgencia se sustenta en situaciones anormales e imprevisibles que por el mismo hecho de no poder evitarse su ocurrencia, toman al Estado por sorpresa, debiendo éste adoptar las medidas extraordinarias y urgentes que permitan paliar los efectos de dichas situaciones”*¹³.

Respecto a las situaciones imprevisibles, de emergencia o urgencia, César Landa Arroyo advierte que es un error común en la formulación de decretos de urgencia, que el Poder Ejecutivo confunda las situaciones extremas o preocupantes (que requieren una actuación previsible y permanente) con temas urgentes, de necesidad o urgencia, de crisis, de “carácter desesperado” o imprevisibles (...)”¹⁴. Entonces, sobre la materia es menester indicar que el criterio de excepcionalidad establece que el decreto de urgencia debe estar orientado a **revertir situaciones extraordinarias e imprevisibles**.

El Decreto de Urgencia 007-2020, en la Exposición de Motivos, fundamenta la necesidad y la urgencia de la dación de dicha norma en lo siguiente:

Sobre la NECESIDAD y URGENCIA:

- i. Se fundamenta como problema a resolver que: *“La confianza digital es un problema complejo que comprende diversos actores (público, privado, academia y sociedad civil) con diferentes intereses, pero un solo afectado que son las personas”*. En esa línea, la urgencia de establecer un Marco de Confianza responde a: (i) Vulneración de los derechos fundamentales del ciudadano en el entorno digital; (ii) Falta de una norma con rango de ley que establezca un marco de articulación entre actores públicos y privados para atender incidentes de seguridad digital a nivel nacional; (iii) No existe un registro unificado de los

¹³ “El control parlamentario de los decretos legislativos y los decretos de urgencia en el Perú”, Javier Bedoya de Vivanco.

¹⁴ LANDA ARROYO, César. Op. Cit. Pp. 144-146.

incidentes de seguridad digital en el Estado; (iv) Pérdidas económicas como resultado de los ciberataques; y, (v) No se tiene un Centro Nacional de Seguridad Digital que gestione la respuesta en el ámbito nacional, interactuando con actores públicos y privados. En ese sentido, señalan que: *"Consistente con lo analizado, la propuesta de Decreto de Urgencia responde a motivaciones de naturaleza estratégica, económica, social, política y técnica, con miras a promover la confianza digital de los ciudadanos en el entorno digital, asegurando su desenvolvimiento con las mismas garantías que en el entorno digital"*.

- ii. *"En el Perú se ha tomado la decisión de garantizar la transformación digital del Estado para el logro de los objetivos del país¹⁵ en el marco de la Política General de Gobierno cuyos pilares se centran en la integridad y lucha contra la corrupción; fortalecimiento institucional para la gobernabilidad; crecimiento económico equitativo, competitivo y sostenible; desarrollo social y bienestar para la población y descentralización efectiva para el desarrollo. **La transformación digital del país es fundamental para el logro de estos objetivos**"¹⁶. [El resaltado y subrayado es nuestro]*
- iii. *"(...) el Perú tomó la decisión de adherirse al Convenio de Budapest o Convenio contra la Ciberdelincuencia reconociendo la necesidad de fortalecer la regulación en materia de seguridad digital dado al avance de la digitalización y el crecimiento de los delitos cometidos en Internet. (...) **Dicha adhesión establece plazos perentorios para adecuar la regulación digital** en torno a los riesgos digitales y fortalecer la confianza digital de los ciudadanos"¹⁷. [El resaltado es nuestro]*
- iv. *"Durante el 2018 y 2019 el avance de las tecnologías digitales ha sido exponencial. En medio de este avance, se ha verificado el crecimiento de los ciberataques, el robo de datos, los delitos contra niños y adolescentes, suplantación, ingeniería social, entre otros delitos en Internet. Ello ha ocasionado pérdidas económicas tanto en el sector público como en el sector privado y, sobre todo, ha afectado a millones de ciudadanos. Esta situación que van en franco incremento, **nos brinda un pronóstico bastante negativo respecto al cual la normativa resulta insuficiente** y revela la necesidad de emitir una norma de rango legal para su resolución"¹⁸. [El resaltado es nuestro]*
- v. *El impacto de los ciberataques afecta la credibilidad y confianza en el país, impacta la competitividad, la productividad, las condiciones para hacer negocios en el país, la productividad en las regiones y la seguridad de las personas. De igual manera, los delincuentes comunes utilizan las redes y el Internet para facilitar sus delitos: acosas a sus víctimas por redes sociales, ingresan a cámaras*

¹⁵ Discurso Presidencial del 28 de julio de 2019.

¹⁶ Numeral 1.1, de la necesidad y urgencia, pág. 1 de la Exposición de Motivos.

¹⁷ Numeral 1.2, de la necesidad y urgencia, pág. 1 de la Exposición de Motivos.

¹⁸ Numeral 1.3, de la necesidad y urgencia, pág. 1 de la Exposición de Motivos.

de vigilancia y a cualquier dispositivo de los hogares, hacen seguimiento a las víctimas rastreando maliciosamente. Por ello, **existe la urgencia de establecer un marco regulatorio** con el fin primario de salvaguardar los **derechos fundamentales** de las personas y ciudadanos en el **entorno digital** (...). **Revertir esta situación es urgente**. Para ello debe garantizarse la articulación público privada y que el Estado emita lineamientos para los servicios y plataformas digitales públicas y privadas que se implementen para lograr estos objetivos”¹⁹. [El resaltado y subrayado es nuestro]

vi. “La Política General de Gobierno tiene metas definidas que deben ser cumplidos antes del 28 de julio de 2021. Es así que la lucha contra la corrupción y la generación de bienestar social; así como la competitividad y productividad tienen un componente, **la transformación digital, es un proceso fundamental para el logro de los objetivos de dicha Política en beneficio de los ciudadanos y empresas**. Por ello, la Política General de Gobierno y la adhesión del Perú al Convenio de Budapest se constituyen en un componente normativo que establece metas sobre la materia a ser cumplidas a corto plazo”²⁰. [El resaltado y subrayado es nuestro]

vii. “(...) el **Perú no dispone de una norma legal de alto nivel (Norma con rango de Ley) que establece un marco de articulación acorde con las necesidades y demandas de la transformación digital y uso de tecnologías digitales** (...) **este escenario debe ser revertido antes del referido plazo** (2021)”²¹. [El resaltado es nuestro]



Asimismo, en los considerandos del texto normativo se establece que “mediante Decreto Supremo N° 086-2015-PCM se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económico – OCDE, e implementación del Programa País” y que, en ese sentido, resulta de particular relevancia la necesidad de cumplir con las “Recomendación para la Gestión de Riesgos de Seguridad Digital realizadas por la OCDE”, entre las cuales se encuentra **“el establecimiento de Equipos de Respuestas a Incidentes de Seguridad Digital a nivel de los estados”**.

Asimismo, en el noveno considerando del decreto de urgencia se precisa que en el documento Gobierno Digital en el Perú “Trabajando con los ciudadanos”, la OCDE señala como recomendación, que el estado peruano debe “considerar establecer un Centro Nacional de Seguridad Digital” a fin de articular acciones para gestionar incidentes de seguridad digital y fortalecer la confianza. **En esa línea, queda establecido que las disposiciones del texto normativo, tienen como principal antecedente al “Programa País OCDE-Perú”, OCDE y el conjunto de documentos específicos que se han**

¹⁹ Literal b, numeral 1.3, de la necesidad y urgencia, pág. 1 de la Exposición de Motivos.

²⁰ Literal c, del numeral 1.3, de la necesidad y urgencia, pág. 2 de la Exposición de Motivos.

²¹ pág. 2 de la Exposición de Motivos.

venido desarrollando para brindar un enfoque integrado de la digitalización a nivel nacional. En tal sentido, y conforme a los criterios habilitantes establecidos por el Tribunal Constitucional para la emisión de los decretos de urgencia, es menester referir el criterio de excepcionalidad, por el cual el decreto de urgencia debe estar orientado a revertir situaciones extraordinarias e imprevisibles.

Por otro lado, se justifican las disposiciones establecidas en el decreto de urgencia en el marco de nuestro proceso de “vinculación” lo que haría necesario “dictar medidas en materia de confianza y seguridad digital, estableciendo los mecanismos de colaboración y articulación con actores públicos, privados y sociedad civil en el entorno digital, a través de un enfoque sistémico e integral que asegure el fortalecimiento de la confianza en los servicios digitales por las personas, entidades y sociedad en general”. Respecto a la materia, César Landa Arroyo advierte que es un error común en la formulación de los decretos de urgencia que el Poder Ejecutivo confunda las situaciones extremas o preocupantes (que requieren una actuación previsible y permanente) con temas urgentes, de necesidad o de urgencia, de crisis, de “carácter desesperado” o imprevisibles.

En ese orden de ideas, y considerando que el texto normativo regula la activación de protocolos, la implementación de registros, centrales de riesgo, entre otros mecanismos técnicos y operacionales para mejorar la confianza digital, **éstos pudieron ser parte de la Política Nacional en materia de Gobierno Digital del Poder Ejecutivo**, y aprobarse mediante una ley ordinaria a fin de tener una regulación de carácter integral, como parte del ejercicio de la rectoría de la Secretaría de Gobierno Digital de la PCM.

Por lo tanto, el grupo de trabajo, considerando la situación actual, la urgencia y el estado de las cosas, expuesto en la Exposición de Motivos del Decreto de Urgencia 007-2020, concluye que estas **no corresponden a una situación de carácter imprevisible**; es decir, de una situación de urgencia, toda vez que la problemática expuesta es consecuencia de la inacción del Poder Ejecutivo, por no atender eficientemente las recomendaciones de la OCDE, emitidas el 2015, en el documento denominado “Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social”; y, por su no ratificación oportuna e implementación del “Convenio de Ciberdelincuencia” o “Convenio de Budapest”, suscrito en noviembre de 2001.

En ese sentido, considerando que la norma en evaluación “(...) responde a motivaciones de naturaleza estratégica, económica, social, política y técnica, con miras a promover la confianza digital de los ciudadanos en el entorno digital (...)”²², el **Grupo de Trabajo considera que la facultad legislativa extraordinaria del Poder Ejecutivo durante el interregno parlamentario no aplica para lo normado en el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone de medidas para su funcionamiento, toda vez que no se ha demostrado, ni justificado, el carácter de urgencia de dicha norma.**

²² Literal C. Problema. De los Fundamentos.

Sin perjuicio de la conclusión a la que llegó el presente grupo de trabajo no debe entenderse que estemos en contra de normar, implementar y fortalecer el “Marco de Confianza Digital”, que aborden la protección de datos personales, la transparencia, la seguridad digital y la seguridad de las personas en el entorno digital, sino, que, esta materia debería regularse solo mediante actos legislativos propios al Congreso de la República, es decir, a través de una ley, y no a través de un decreto de urgencia.

4.2 Sobre los principios de razonabilidad y proporcionalidad del Decreto de Urgencia 006-2020

En esta sección se examinará el principio de razonabilidad y proporcionalidad del Decreto de Urgencia 007-2020.

El Decreto de Urgencia 007-2020, señala de manera expresa que “El Marco de Confianza Digital se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles (...), tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital”; sin embargo, el decreto de urgencia no desarrolla ningún principio, modelo, política, proceso, rol o estándar mínimo para fortalecer la confianza digital; todo lo contrario, posterga la reglamentación de la norma en un plazo de 90 días hábiles, luego de publicado el Decreto de Urgencia.



Asimismo, el decreto de urgencia posterga la implementación del Registro Nacional de Incidentes de Seguridad Digital, la emisión de normas, lineamientos y directivas para su correcto funcionamiento, hasta un plazo de 90 días hábiles, luego de publicado el Decreto de Urgencia. Peor aún, el decreto de urgencia no establece plazo alguno para la implementación del Centro Nacional de Seguridad Digital y del Centro Nacional de Datos, plataformas digitales que gestionarán, dirigirán, articularán y supervisarán la operación, educación, promoción, colaboración y cooperación de la seguridad digital y la de datos, respectivamente, a nivel nacional, a fin de fortalecer la confianza digital y bienestar de las personas en el entorno digital.

Al respecto, es menester referir, que el criterio de conexidad, dentro del principio de razonabilidad, estable que: “... las medidas extraordinarias y los beneficios que su aplicación produzcan deben pues surgir del contenido mismo del decreto de urgencia y no de acciones diferidas en el tiempo, pues ello sería incongruente con una supuesta situación excepcionalmente delicada”²³.

Es decir, en el peor escenario, recién en mayo de 2020 sabremos cuáles serán los principios, modelos, políticas, procesos, roles o estándares mínimos para fortalecer la confianza digital, para su respectiva implementación del “Marco de Confianza Digital”, de la implementación del Registro Nacional de Incidentes de Seguridad Digital, la emisión de normas, lineamientos y directivas para su correcto funcionamiento; y, sin fecha de implementación del Centro Nacional de Seguridad Digital y del Centro Nacional de Datos.

²³ STC 00028-2010-PI/TC.

Situación incongruente con la exposición de motivos, respecto a la urgencia de la dación del decreto de urgencia en evaluación.

Por lo tanto, ante la incongruencia evidente, este **Grupo de Trabajo considera que el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, no cumple con los principios de razonabilidad y proporcionalidad para la emisión de este tipo de normas.**

4.3 Sobre materia incompatible de facultad legislativa extraordinaria del Poder Ejecutivo: Ley de Presupuesto y sobre modificaciones presupuestales

Es relevante mencionar que, según lo aprobado en el decreto de urgencia en evaluación, respecto a su financiamiento establece que: *"La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público"*²⁴, al respecto es pertinente señalar que la Constitución Política en sus artículos 78 (primer párrafo), establece que el Presidente de la República envía al Congreso de la República el proyecto de Ley de Presupuesto dentro de un plazo que vence el 30 de agosto de cada año; además, en sus artículos 80 (tercer párrafo) y 101 numeral 3, establece que los créditos suplementarios, habilitaciones y transferencias de partidas se tramitan ante el Congreso de la República tal como la "Ley de Presupuesto", y que le corresponde tal atribución a la Comisión Permanente durante el receso parlamentario. Sobre la materia, parte de la doctrina señala que lo anterior no puede tener excepción alguna²⁵.



Por otro lado, en la exposición de motivos, respecto del análisis costo – beneficio, del decreto de urgencia, se señala que: *"Las disposiciones referidas a la implementación del Centro Nacional de Seguridad Digital, Registro Nacional de Incidentes de Seguridad Digital, Centro Nacional de Datos y plataforma de aprendizaje en línea se encuentran contemplados como parte de los componentes del "Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional", que a la fecha viene ejecutando la Presidencia del Consejo de Ministros. El referido Proyecto tiene un monto de inversión de US \$ 60.9 millones, siendo el monto del préstamo de US \$ 50 millones y la contrapartida nacional de US \$ 10.9 millones, de este monto total el porcentaje destinado a dichas implementaciones es de 20% aproximadamente"*. Es decir, el costo de la implementación

²⁴ Artículo 14. Financiamiento. Decreto de Urgencia 007-2020.

²⁵ "Los créditos suplementarios, habilitaciones y transferencias de partidas son diversas modificaciones que se van haciendo al Presupuesto, conforme avanza su ejecución. Como se trata de aprobación de ingresos y egresos debe ser hecha también por el Congreso. Por eso dice la Constitución que se tramitan ante el Congreso como la Ley de Presupuesto y en el receso ante la Comisión Permanente, la que para aprobarlos requiere tres quintos del número legal de sus miembros". RUBIO CORREA, Marcial (1999). Estudio de la Constitución Política de 1993 (Vol. III) Lima: PUCP, p. 459:

"En síntesis, hemos podido apreciar que el requisito de legislar respecto a materias económicas o financieras no puede dejar de lado el contenido expreso de la Constitución. Así, es evidente que lo establecido en el párrafo tercero del artículo 80 de la Constitución es, asimismo, pauta de análisis para dilucidar qué materia económica o financiera puede ser regulada mediante un Decreto de Urgencia. Por ello, bien puede afirmarse que la materia presupuestaria, en general, no está vedada para la legislación de urgencia, pero sí, en específico, el otorgamiento de créditos suplementarios, transferencias de partidas y habilitaciones". BEDOYA DE VIVANCO, Javier. Op. Cit. P. 1340.

del Centro Nacional de Seguridad Digital, Registro Nacional de Incidentes de Seguridad Digital, Centro Nacional de Datos y plataforma de aprendizaje en línea demandará al Estado Peruano US \$ 12.18 millones, aproximadamente.

Al respecto se debe precisar²⁶ que, en setiembre de 2018, el Gobierno peruano, representado por el Ministerio de Economía y Finanzas (MEF), firmó con el Banco Interamericano de Desarrollo (BID) **tres contratos de operación de endeudamiento externo por un monto total de US\$ 225 millones**, que serían destinados al financiamiento parcial de proyectos de inversión en los sectores de Educación y Saneamiento, así como para mejorar la provisión de los servicios a los ciudadanos y las empresas.

La **primera operación** de endeudamiento externo, por US\$ 75,0 millones, estaría destinada a financiar el “Programa para la Mejora de la Calidad y Pertinencia de los Servicios de Educación Superior Universitaria y Tecnológica a Nivel Nacional”, a cargo del Ministerio de Educación (MINEDU) a través de la Unidad Ejecutora “Mejoramiento de la Calidad de la Educación Básica”. La amortización del préstamo se hará en 6 cuotas en los años 2024, 2025 y 2026, a una tasa de interés de Libor a 3 meses más un margen a ser determinado por el BID, siendo la comisión de crédito de hasta 0,75% de acuerdo a condiciones establecidas por el organismo. Cabe indicar que el costo total de Programa es de S/ 683,54 millones (equivalentes a US\$ 200,0 millones), financiado con la operación de endeudamiento externo (US\$ 75,00 millones) y contrapartida nacional (US\$ 125,00 millones).



De otro lado, la **segunda operación** de endeudamiento externo, por US\$ 100 millones, tiene como objetivo el financiamiento del “Programa Integral de Agua y Saneamiento Rural – PIASAR”, a cargo del Ministerio de Vivienda, Construcción y Saneamiento (MVCS), a través de su Programa Nacional de Saneamiento Rural. En este caso, la amortización del préstamo se hará en 3 cuotas en los años 2026 y 2027, a una tasa de interés de Libor a 3 meses más un margen a ser determinado por el BID, siendo la comisión de crédito de hasta 0,75% sobre el saldo no desembolsado. El costo total de Programa es de S/ 413,28 millones (equivalentes a US\$ 126,0 millones), financiado con la operación de endeudamiento externo (US\$ 100,00 millones) y contrapartida nacional (US\$ 26,00 millones).

Finalmente, la **tercera operación de endeudamiento externo**, materia de la evaluación, hasta por US\$ 50 millones, financiaría el “**Proyecto Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas a Nivel Nacional**”, a cargo de la Presidencia del Consejo de Ministros (PCM) y que tiene por objetivo mejorar y ampliar los servicios de soporte para la provisión de servicios a ciudadanos y empresas.

²⁶ <https://www.mef.gob.pe/es/noticias/notas-de-prensa-y-comunicados?id=5791>

La amortización del préstamo se hará en 2 cuotas en los años 2029 y 2030, a una tasa de interés de Libor a 3 meses más un margen a ser determinado por el BID, siendo la comisión de crédito de hasta 0,75% sobre el saldo no desembolsado. El costo total de Proyecto es de S/. 119,8 millones (equivalentes a US\$ 60,9 millones), financiado con la operación de endeudamiento externo (US\$ 50,00 millones) y contrapartida nacional (US\$ 10,90 millones).

Entonces, queda en evidencia que lo dispuesto en el Decreto de Urgencia 007-2020 sí demandará recursos adicionales al Tesoro Público, pues el costo de la implementación del Centro Nacional de Seguridad Digital, Registro Nacional de Incidentes de Seguridad Digital, Centro Nacional de Datos y plataforma de aprendizaje en línea demandará al Estado Peruano US \$ 12.18 millones, aproximadamente, monto superior a la contrapartida peruana. Peor aún, la amortización del préstamo se realizará en los años 2029 y 2030, fechas en las que el Poder Ejecutivo deberá tramitar la Ley de Presupuesto, según lo establecido Constitución Política en sus artículos 78 (primer párrafo), o en sus artículos 80 (tercer párrafo) y 101 numeral 3, establece que los créditos suplementarios, habilitaciones y transferencias de partidas se tramitan ante el Congreso de la República tal como la "Ley de Presupuesto", y que le corresponde tal atribución a la Comisión Permanente durante el receso parlamentario.

Entonces, si bien puede afirmarse que la materia presupuestaria, en general, no está vedada para la legislación mediante decretos de urgencia, este Grupo de Trabajo considera que sí, en específico, está vedada la aprobación de la Ley de Presupuesto mediante decretos de urgencia, cuando el Congreso de la República se encuentra vigente (2029 y 2030), y el otorgamiento de créditos suplementarios, transferencias de partidas y habilitaciones, la misma que deberían tramitarse ante el Congreso de la República, en todo caso, el otorgamiento de créditos suplementarios, transferencias de partidas y habilitaciones sólo a aplicarse durante el período del interregno parlamentario, no así a futuro, como es el caso del decreto de urgencia en evaluación.

En este mismo punto, cabe traer a colación lo señalado en la STC 0006-2018-PI/TC, mediante la que el Tribunal Constitucional analiza el principio de separación de poderes, como *"una exigencia ineludible en todo Estado Democrático y Social de Derecho, de manera que dicha separación de las funciones básicas del Estado constituye una garantía para los derechos constitucionalmente reconocidos y para limitar el poder frente al absolutismo y la dictadura"*, que *"no debe entenderse como una división tajante, sin puntos de contacto o interrelación entre ellos denominados poderes del Estado, sino que esta debe ser considerada en clave de equilibrio, de controles recíprocos, de pesos y contrapesos, e incluso debe ser entendida sobre la base de relaciones de coordinaciones y cooperación entre estos poderes"*²⁷.

²⁷ Fuente: <https://www.enfoquederecho.com/2019/10/31/limites-materiales-de-los-decretos-de-urgencia-en-materia-tributaria-durante-el-interregno-parlamentario/>

Debemos destacar que el Tribunal Constitucional considera que el “principio de separación de poderes» y lo concerniente al «régimen político» diseñado por la Constitución son parte de una especie de «núcleo duro», conformado por aquellos valores y principios básicos que dan identidad a nuestro texto constitucional y que, por tanto, constituyen un límite para la reforma constitucional²⁸.

Por las razones jurídica y constitucionalmente, el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, contendría materia incompatible con la facultad legislativa extraordinaria del Poder Ejecutivo, durante el periodo del interregno parlamentario, respecto a lo referido a la **Ley de Presupuesto y sobre modificaciones presupuestales**; siendo ello así, el Poder Ejecutivo, al extremo no podría legislar a través de un decreto de urgencia, sino a través de un Proyecto de Ley, que sigan los procedimientos y fases que exige la Constitución y el Reglamento del Congreso de la República, cuando corresponda, teniendo en cuenta que, es competencia exclusiva del Congreso de la República, de tal manera que, este Decreto de Urgencia 007-2020, transgrede los artículos 78, 80 y 101 de la Constitución Política del Perú.

5. CONCLUSIONES

1. Que, en concordancia con la **Constitución Política del Perú**, el **Decreto de Urgencia 007-2020**, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, **contendría materia incompatible con la facultad legislativa extraordinaria**, durante el periodo del interregno, toda vez que, la Ley de Presupuesto y las modificaciones presupuestales deben ser aprobado únicamente mediante una ley, es decir, estas materias cuya regulación solo se pueda realizar mediante actos legislativos propios al Congreso de la República, y no a través de un decreto de urgencia, conforme a lo dispuesto por el Artículo 78, 80 y 101 de la Constitución Política del Perú. En ese sentido el Decreto de Urgencia 007-2020, transgrede el ámbito Constitucional vigente en nuestro país.
2. Que, no se ha justificado el carácter de urgencia respecto a la dación del **Decreto de Urgencia 007-2020**, ni se ha demostrado que lo normado corresponde a una situación de carácter imprevisible. Más aún, si en la fecha de la publicación de la norma en evaluación no se conoce cuáles serán los principios, modelos, políticas, normas, procesos, roles y estándares mínimos, del Marco de Confianza Digital, del Registro Nacional de Incidentes de Seguridad Digital; ni los plazos de implementación del Centro Nacional de Seguridad Digital y del Centro Nacional de Datos, que permitan asegurar y mantener la confianza en el entorno digital, quebrándose el criterio de conexidad requerida para los decretos de urgencia.



²⁸ Fuente: <https://www.enfoquederecho.com/2019/10/31/limites-materiales-de-los-decretos-de-urgencia-en-materia-tributaria-durante-el-interregno-parlamentario/>

3. Corresponde elevar este informe a la Comisión Permanente para que continúe el procedimiento, de conformidad con lo previsto en el segundo párrafo del artículo 135 de la Constitución Política del Perú.

6. RECOMENDACIONES

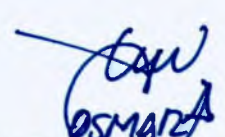
1. Dado que el presente Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, no regula materia excepcional, de suma necesidad, transitoriedad y generalidad, las que habilitan y legitiman los decretos de urgencia, resulta necesario declarar la inconstitucionalidad de dicho decreto.
2. Por la importancia de implementar el Marco de Confianza Digital en el Perú, se recomienda al Poder Ejecutivo, una vez instalado el nuevo Congreso de la República, Período 2020-2021, priorice la presentación, para su debate y aprobación de la iniciativa legislativa "Ley Marco de Confianza Digital".
3. Que, el nuevo Congreso de la República, Período 2020-2021, al margen de la primera recomendación, encargue a la Comisión de Fiscalización realizar el control parlamentario al Contrato de Préstamo N° 4399/OC-PE, especialmente a la tercera operación de endeudamiento externo, hasta por US\$ 60.9 millones (monto del préstamo de US\$ 50 millones y la contrapartida nacional de US\$ 10.9 millones), que financiaría el "Proyecto Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas a Nivel Nacional", a cargo de la Presidencia del Consejo de Ministros (PCM) y que tiene por objetivo mejorar y ampliar los servicios de soporte para la provisión de servicios a ciudadanos y empresas.

Lima, 10 de febrero de 2020.

Dese cuenta.



ANGEL NEYRA OLAYCHEA
Congresista de la República
Integrante de la Comisión Permanente
COORDINADOR
Grupo de Trabajo DU 006-2020

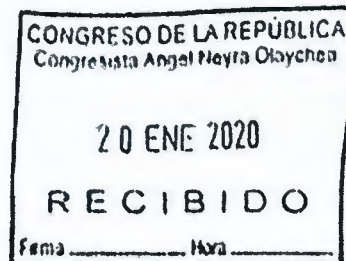


JOSÉ MARVIN PALMA MENDOZA
Congresista de la República
Integrante de la Comisión Permanente
Grupo de Trabajo DU 006-2020



ÁREA DE DESPACHO PARLAMENTARIO

Lima, 16 de enero de 2020



Oficio N° 198-2019-2020-ADP-CP/CB

Señor
ÁNGEL NEYRA OLAYCHEA
Congresista de la República



Tengo el agrado de dirigirme a usted para hacer de su conocimiento que la Comisión Permanente del Congreso de la República, en su sesión realizada el 15 de enero de 2020, de conformidad con la propuesta formulada por la presidencia y con la dispensa del trámite de sanción del acta, acordó designarlo como congresista coordinador para la elaboración del informe de los siguientes decretos de urgencia:

- ✓ Decreto de Urgencia N° 06-2020, que crea el Sistema Nacional de Transformación Digital.
- ✓ Decreto de Urgencia N° 07-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

De igual manera, le informo que el congresista Marvin Palma Mendoza participará en el estudio de los referidos decretos de urgencia y que el Departamento de Comisiones le brindará el apoyo técnico legal pertinente.

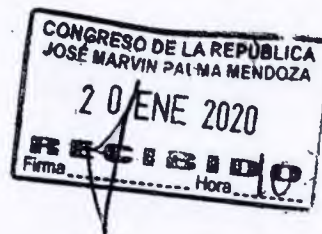
Con esta oportunidad reitero a usted, señor congresista, la expresión de mi especial consideración.

Atentamente,


GIOVANNI FORNO FLOREZ
Oficial Mayor del Congreso de la República

Lima, 16 de enero de 2020

Oficio N° 199-2019-2020-ADP-CP/CR



Señor

MARVIN PALMA MENDOZA

Congresista de la República

Tengo el agrado de dirigirme a usted para hacer de su conocimiento que la Comisión Permanente del Congreso de la República, en su sesión realizada el 15 de enero de 2020, de conformidad con la propuesta formulada por la presidencia y con la dispensa del trámite de sanción del acta, acordó designar al congresista Ángel Neyra Olaychea como congresista coordinador para la elaboración del informe de los siguientes decretos de urgencia:

- ✓ Decreto de Urgencia N° 06-2020, que crea el Sistema Nacional de Transformación Digital.
- ✓ Decreto de Urgencia N° 07-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.

De igual manera, le informo que usted participará en el estudio de los referidos decretos de urgencia.

Con esta oportunidad reitero a usted, señor congresista, la expresión de mi especial consideración.

Atentamente,

GIOVANNI FORNO FLOREZ
Oficial Mayor del Congreso de la República

JAP/JVCH/cel.

www.congreso.gob.pe

Plaza Bolívar, Av. Abancay s/n – Lima, Perú
Central Telefónica: 311-7777

RU 453505

22

95

GRUPO DE TRABAJO

ENCARGADO DE ELABORAR LOS INFORMES DEL

DECRETO DE URGENCIA 006-2020, DECRETO DE URGENCIA QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL

DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

ACTA DE LA PRIMERA SESIÓN

Lima, 10 de febrero de 2020

Acuerdos tomados por unanimidad:

- Aprobar el Informe Final del Grupo de Trabajo de la Comisión Permanente encargado del examen del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Aprobar el Informe Final del Grupo de Trabajo de la Comisión Permanente encargado del examen del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Aprobar el Acta de la Sesión de Instalación del Grupo de Trabajo, del 22 de enero de 2020.
- Dispensar el trámite de aprobación del Acta de la Primera Sesión de Instalación para la ejecución de los acuerdos.



Siendo las quince horas y catorce minutos del lunes 10 de febrero de 2020; en la Sala "María Elena Moyano", Palacio Legislativo, del Congreso de la República, el congresista **Angel Neyra Olaychea** (FP), en su condición de **Coordinador** del Grupo de Trabajo encargado de elaborar los informes sobre el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, dio inicio a la Primera Sesión, con el quórum correspondiente. Constando con la presencia del congresista **Marvin Palma Mendoza** (C21).

APROBACIÓN DE ACTAS

El señor **Coordinador** consultó la aprobación del Acta de la Sesión de Instalación, realizada el 22 de enero de 2020, siendo aprobado por UNANIMIDAD, sin observaciones.

INFORMES

- El señor **Coordinador** dejó constancia que en la sesión anterior¹, estuvieron presentes los funcionarios de la Presidencia del Consejo de Ministros, específicamente de la Secretaría de Gobierno Digital; del Ministerio de Justicia y Derechos Humanos y del INDECOPI, quienes informaron sobre las razones de necesidad, urgencia y justificación que motivaron la dación del Decreto de Urgencia

¹ Realizada de manera informativa el 30 de enero de 2020.

006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, lo cual han sido considerados en el Informe Final del Grupo de Trabajo.

- El señor **Coordinador** manifestó que había sido invitado, para la presente sesión, el experto en sistemas de digitalización, Sr. Enrique Mesones, quien por razones de su agenda no pudo estar presente.

ORDEN DEL DÍA

DEBATE DEL PRE INFORME DEL GRUPO DE TRABAJO ENCARGADO DEL DECRETO DE URGENCIA 006-2020, DECRETO DE URGENCIA QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL.

El señor **Coordinador** manifestó que, en atención al encargo de la Comisión Permanente, de realizar el examen del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, y que para el desarrollo del informe se ha seguido estrictamente las disposiciones que contempla la Constitución Política, norma máxima en la legislación peruana, procedió a detallar el informe correspondiente, manifestando lo siguiente:

- En esta sección se examinará el principio de razonabilidad y proporcionalidad del Decreto de Urgencia 006-2020.
- El Decreto de Urgencia 006-2020, señala de manera expresa que "la Política y Estrategia Nacional de Transformación Digital, serán los instrumentos estratégicos y orientadores para la transformación digital del país"; sin embargo, posterga la formalización de ambas herramientas a un plazo de 90 días hábiles, luego de publicado el Decreto de Urgencia. Al respecto, es menester referir, que el criterio de conexidad, dentro del principio de razonabilidad, estable que: "Las medidas extraordinarias y los beneficios que su aplicación produzcan deben pues surgir del contenido mismo del decreto de urgencia y no de acciones diferidas en el tiempo, pues ello sería incongruente con una supuesta situación excepcionalmente delicada". Del mismo modo, se debe señalar que, tratándose de contenidos propios de Política y Estrategia Nacional pudieron ser aprobadas en el marco de sus funciones mediante una ley ordinaria y no mediante un Decreto de Urgencia, conforme a lo dispuesto por el artículo 106 de la Constitución Política del Perú.
- Es decir, postergación de los 90 días, en el peor escenario, recién en mayo de 2020 sabremos en qué consiste, y cuáles son los objetivos, de la Política y Estrategia Nacional de Transformación Digital, para su respectiva implementación. Situación incongruente con la exposición de motivos, respecto a la urgencia de la dación del decreto de urgencia que es materia de examen de nuestro grupo de trabajo.
- Por otro lado, la exposición de motivos, también, trata de sustentar la necesidad de ampliar el plazo para que las entidades del Poder Ejecutivo puedan adecuar sus sistemas de trámite documentario, o equivalentes, para el envío automático de documentos electrónicos con otras entidades, así como dentro de sus áreas, órganos y unidades. El Decreto de Urgencia 006-2020, en su Primera Disposición Complementaria, amplía este plazo de adecuación hasta el 31 de diciembre de 2021, sustentándose en que aún existe una brecha tecnológica en algunas entidades del sector público, lo que habría impedido el cumplimiento de lo



establecido en el artículo 8 del Decreto Legislativo N° 1310. Esta situación lo califican como urgente, dado que el cumplimiento del Decreto Legislativo referido tenía como plazo máximo el 31 de diciembre de 2019.

- Entonces, si bien puede afirmarse que la materia de políticas públicas, en general, no está vedada para la legislación mediante decretos de urgencia, este Grupo de Trabajo considera que este tipo de normas deberían tramitarse ante el Congreso de la República, no cumpliendo los principios de razonabilidad para la emisión de este tipo de normas.
- Al respecto, el Tribunal Constitucional destaca que *"para la Constitución la fuente normativa denominada ley comprende a las leyes ordinarias, las leyes orgánicas, las leyes de desarrollo constitucional y las que tienen una denominación asignada directamente por la Constitución y cuyas diferencias no radican en su jerarquía ni en el órgano que las expide, sino en su procedimiento de aprobación y en las materias que regulan"*. En cuanto al tipo *"ley ordinaria"*, el mismo Tribunal señala que *"es la expedida por el Congreso de la República, inciso 1° del artículo 102° de la Constitución, y su modo de producción está regulado por los artículos 105°, 107°, 108° y 109° de la Constitución. En rigor puede normar cualquier materia, con excepción de las reservadas a la ley orgánica conforme al artículo 106° de la Constitución y las que sean materia exclusiva de los gobiernos regionales o locales"*.
- En ese contexto el artículo 106 del Texto Constitucional señala: *"Mediante leyes orgánicas se regulan la estructura y el funcionamiento de las entidades del Estado previstas en la Constitución, así como también las otras materias cuya regulación por ley orgánica está establecida en la Constitución. Los proyectos de ley orgánica se tramitan como cualquiera otra ley. Para su aprobación o modificación, se requiere el voto de más de la mitad del número legal de miembros del Congreso"*. En este mismo punto, cabe traer a colación lo señalado en la Sentencia del Tribunal Constitucional STC 0006-2018-PI/TC, mediante la que el Tribunal Constitucional analiza el principio de separación de poderes, como *"una exigencia ineludible en todo Estado Democrático y Social de Derecho, de manera que dicha separación de las funciones básicas del Estado constituye una garantía para los derechos constitucionalmente reconocidos y para limitar el poder frente al absolutismo y la dictadura"*.
- Por las razones jurídica y constitucionalmente expuestas, el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, forma parte de la estructura orgánica del Poder Ejecutivo; y, por lo tanto, contendría materia incompatible con la facultad legislativa extraordinaria, durante el período del interregno parlamentario; siendo ello así, el Poder Ejecutivo, al extremo no podría legislar a través de un decreto de urgencia, sino a través de un Proyecto de Ley, que sigan los procedimientos y fases que exige la Constitución y el Reglamento del Congreso de la República, una vez se instale el nuevo Congreso, teniendo en cuenta que, es competencia exclusiva del Congreso de la República, de tal manera que, este DU 006-2020, transgrede el artículo 106 de la Constitución Política del Perú; en ese sentido este grupo de Trabajo concluye con las siguientes conclusiones y recomendaciones.
- **Conclusión 1:** Que, en concordancia con la Ley 29158, Ley Orgánica del Poder Ejecutivo, el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, contendría materia incompatible con la facultad legislativa extraordinaria, durante el período del interregno, toda vez que, un sistema funcional debe ser creado únicamente mediante una ley, es decir, la creación de sistemas funcionales del Poder Ejecutivo están dentro de las materias cuya regulación solo



se pueda realizar mediante actos legislativos propios al Congreso de la República, y no a través de un decreto de urgencia, conforme a lo dispuesto por el Artículo 106 de la Constitución Política del Perú. En ese sentido el DU 006-2020, transgrede el ámbito Constitucional vigente de nuestro país.

- **Conclusión 2:** El Decreto de Urgencia 006-2020, no se ha justificado el carácter de urgencia respecto a la dación del mismo, ni se ha demostrado que lo normado corresponde a una situación de carácter imprevisible. Más aún, si en la fecha de la publicación de la norma en evaluación no se conoce cuál es la "Política y Estrategia Nacional de Transformación Digital", instrumento estratégico y orientador indispensable para lograr la transformación digital del país, quebrándose el criterio de conexidad requerida para los decretos de urgencia.
- **Conclusión 3:** Corresponde elevar este informe a la Comisión Permanente para que continúe el procedimiento, de conformidad con lo previsto en el segundo párrafo del artículo 135 de la Constitución Política del Perú.
- **Recomendación 1:** Dado que el presente Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, no regula materia excepcional, de suma necesidad, transitoriedad y generalidad, las que habilitan y legitiman los decretos de urgencia, resulta necesario declarar la inconstitucionalidad de dicho decreto. Más aún, si un sistema funcional del Poder Ejecutivo solo puede ser creado mediante una ley expresa, de acuerdo a lo dispuesto por el artículo 106 de la Constitución Política del Perú, y el estricto respeto al principio de separación de poderes, que la reafirma la Sentencia del Tribunal Constitucional, recaído en la STC 0006-2018-PI/TC, mediante lo cual el TC denomina a la separación de poderes, como "*una exigencia ineludible en todo Estado Democrático y Social de Derecho*".
- **Recomendación 2:** Por la importancia de la transformación digital en nuestro país, se recomienda al nuevo Congreso de la República, Periodo 2020-2021, priorice en la Agenda Legislativa la presentación, debate y aprobación de las iniciativas legislativas "Ley que crea el Sistema Nacional de Transformación Digital".
- **Recomendación 3:** Que, el nuevo Congreso de la República, Periodo 2020-2021, al margen de la primera recomendación, encargue a la Comisión de Ciencia, Innovación y Tecnología, el seguimiento de la formulación, aprobación e implementación de la "Política y Estrategia Nacional de Transformación Digital", a cargo de la Presidencia del Consejo de Ministros, política necesaria e indispensable para lograr la transformación digital en todas las instituciones de nuestro país.



Concluida la sustentación del Informe del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, el señor **Coordinador** puso a consideración el informe de los señores congresistas para sus aportes, observaciones o recomendaciones.

No habiendo intervenciones, el señor **Coordinador**, considerando que ya se contaba con el pre informe del Decreto de Urgencia 007-2020, puso a consideración la ampliación de la agenda para el debate correspondiente, siendo aprobado por **UNANIMIDAD** de los señores congresistas presentes.

AMPLIACIÓN DE AGENDA

DEBATE DEL PRE INFORME DEL GRUPO DE TRABAJO ENCARGADO DEL DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO.

El señor **Coordinador** manifestó que, en atención al encargo de la Comisión Permanente, de realizar el examen del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, y que para el desarrollo del informe se ha seguido estrictamente las disposiciones que contempla la Constitución Política, norma máxima en la legislación peruana, procedió a detallar las conclusiones y recomendaciones del informe, manifestando lo siguiente:

- **Primera conclusión:** En concordancia con la Constitución Política del Perú, el Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, contendría materia incompatible con la facultad legislativa extraordinaria, durante el periodo del interregno, toda vez que, la Ley de Presupuesto y las modificaciones presupuestales deben ser aprobado únicamente mediante una ley, es decir, estas materias cuya regulación solo se pueda realizar mediante actos legislativos propios al Congreso de la República, y no a través de un decreto de urgencia, conforme a lo dispuesto por el Artículo 78, 80 y 101 de la Constitución Política del Perú. En ese sentido el Decreto de Urgencia 007-2020, transgrede el ámbito Constitucional vigente en nuestro país.
- **Segunda conclusión:** No se ha justificado el carácter de urgencia respecto a la dación del Decreto de Urgencia 007-2020, ni se ha demostrado que lo normado corresponde a una situación de carácter imprevisible. Más aún, si en la fecha de la publicación de la norma en evaluación no se conoce cuáles serán los principios, modelos, políticas, normas, procesos, roles y estándares mínimos, del Marco de Confianza Digital, del Registro Nacional de Incidentes de Seguridad Digital; ni los plazos de implementación del Centro Nacional de Seguridad Digital y del Centro Nacional de Datos, que permitan asegurar y mantener la confianza en el entorno digital, quebrándose el criterio de conexidad requerida para los decretos de urgencia.

Tercera conclusión: Corresponde elevar este informe a la Comisión Permanente para que continúe el procedimiento, de conformidad con lo previsto en el segundo párrafo del artículo 135 de la Constitución Política del Perú.

- **Primera recomendación:** Dado que el presente Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, no regula materia excepcional, de suma necesidad, transitoriedad y generalidad, las que habilitan y legitiman los decretos de urgencia, resulta necesario declarar la inconstitucionalidad de dicho decreto.
- **Segunda recomendación:** Por la importancia de implementar el Marco de Confianza Digital en el Perú, se recomienda al Poder Ejecutivo, una vez instalado el nuevo Congreso de la República, Periodo 2020-2021, priorice la presentación, para su debate y aprobación de la iniciativa legislativa "Ley Marco de Confianza Digital".
- **Tercera recomendación:** Que, el nuevo Congreso de la República, al margen de la primera recomendación, encargue a la Comisión de Fiscalización y Contraloría realizar el control parlamentario al Contrato de Préstamo N° 4399/OC-PE, especialmente a la tercera operación de endeudamiento externo, hasta por US\$ 60.9 millones (monto del préstamo de US\$ 50 millones y la contrapartida nacional de US\$ 10.9 millones), que financiaría el "Proyecto Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas a Nivel Nacional", a cargo de la Presidencia del Consejo de Ministros (PCM) y que tiene por objetivo mejorar y ampliar los servicios de soporte para la provisión de servicios a ciudadanos y empresas.



Concluida la sustentación del Informe del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, el señor **Coordinador** puso a consideración el informe de los señores congresistas para sus aportes, observaciones o recomendaciones.

No habiendo intervenciones, el señor **Coordinador**, sometió al voto el Informe Final del Grupo de Trabajo de la Comisión Permanente encargado del examen del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, siendo aprobado por **UNANIMIDAD**, con los votos a favor de los señores congresistas **Marvin Palma Mendoza (C21)** y **Ángel Neyra Olaychea (FP)**.

Seguidamente, el señor **Coordinador**, sometió al voto el Informe Final del Grupo de Trabajo de la Comisión Permanente encargado del examen del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, siendo aprobado por **UNANIMIDAD**, con los votos a favor de los señores congresistas **Marvin Palma Mendoza (C21)** y **Ángel Neyra Olaychea (FP)**.

Finalmente, no habiendo otro tema a tratar, el congresista **Coordinador** agradeció la participación del congresista Marvin Palma Mendoza (C21) y consultó la dispensa del trámite de aprobación del Acta de la Primera Sesión, a fin de tramitar los acuerdos adoptados, siendo aprobado por **UNANIMIDAD**, dando por concluida la sesión a las quince horas con treinta y cinco minutos del lunes 10 de febrero de 2020.

Se deja constancia que la transcripción de la versión grabada de esta sesión, elaborada por el Área de Transcripciones y el audio registrado por el Área de Grabaciones en Audio y Video del Congreso de la República forman parte integrante de la presente acta, prevaleciendo lo expresado según el audio.



Ing. **ÁNGEL NEYRA OLAYCHEA**
Congresista de la República
COORDINADOR
Grupo de Trabajo que examina
Decretos de Urgencia 006-2020 y 007-2020

GRUPO DE TRABAJO DE EVALUACIÓN DEL DU 006-2020, QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL Y DEL DU 007-2020, QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO.

Día: Lunes 10 de febrero del 2020

Hora: 15:00 p. m.

Lugar: Sala María Elena Moyano - Palacio Legislativo

AGENDA

I. INTEGRANTES DEL GRUPO DE TRABAJO

- Ángel Neyra Olaychea - Coordinador
- José Marvin Palma Mendoza

II. ACTAS

- Aprobación del Acta de la Sesión de Instalación, realizada el 22 de enero de 2020.

III. INFORMES

IV. PEDIDOS

V. ORDEN DEL DÍA

- 5.1. Presentación del Experto en Sistemas de Digitalización Enrique Mesones quien brindará opinión técnica con respecto a los recientes D.U. 006 y 007-2020.
- 5.2. Debate del pre informe del Grupo de Trabajo encargado del Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

Lima, 7 de febrero de 2020.

GRUPO DE TRABAJO

DECRETO DE URGENCIA 006-2020, DECRETO DE URGENCIA QUE CREA
EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL

DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE
APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS
PARA SU FORTALECIMIENTO

Asistencia Segunda Sesión
Lima, 10 de febrero de 2020,
15:00 horas
Sala María Elena Moyano
Palacio Legislativo

INTEGRANTES	
	NEYRA OLAYCHEA ÁNGEL COORDINADOR Fuerza Popular
	PALMA MENDOZA JOSÉ MARVIN Cambio 21

CONGRESO DE LA REPÚBLICA
Es copia fiel del original

17 FEB 2020

HUGO CORTEZ TORRES
Fedatario

Área de Transcripciones

**CONGRESO DE LA REPÚBLICA
PERIODO LEGISLATIVO 2019-2020**

**COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA
GRUPO DE TRABAJO ENCARGADO DE ELABORAR EL INFORME SOBRE EL
DECRETO DE URGENCIA 006-2020, QUE CREA EL SISTEMA DE
TRANSFORMACIÓN DIGITAL Y GRUPO DE TRABAJO DEL DECRETO DE
URGENCIA 007-2020, QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y
DISPONE MEDIDAS PARA SU FORTALECIMIENTO**

**2.ª SESIÓN
(Vespertina)**

**LUNES, 10 DE FEBRERO DE 2020
COORDINACIÓN DEL SEÑOR ÁNGEL NEYRA OLAYCHEA**

—A las 15:14 h, se inicia la sesión.

El señor COORDINADOR.— Muy buenas tardes, señor congresista, miembros de asesores técnicos del Congreso.

Siendo las 3 y 14 minutos, del lunes 10 de febrero de 2020, en la Sala María Elena Moyano del Palacio Legislativo, con la presencia del congresista Marvin Palma Mendoza, contando con el *quorum* reglamentario se da inicio a la segunda sesión del Grupo de Trabajo encargado de elaborar los Informes del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital y del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

Aprobación del Acta.

Se consulta la aprobación del Acta de la primera sesión del presente grupo de trabajo realizado el 30 de enero de 2020.

Los que están a favor, sírvanse levantar la mano. Aprobado por unanimidad.

Informes

El señor COORDINADOR.— Se deja constancia que en la sesión anterior, es decir, en la primera sesión estuvieron presentes los funcionarios de la Presidencia del Consejo de Ministros, específicamente el Secretario del Gobierno Digital del Ministerio de Justicia y Derechos Humanos y de Indecopi, quienes informaron sobre las razones de necesidad, urgencia y justificación que motivaron la dación del Decreto de Urgencia 006-2020 que crea el Sistema Nacional de Transformación Digital y el Decreto de Urgencia 007-2020 que aprueba el Marco de Confianza Digital y dispone las medidas para su fortalecimiento, el cual han sido considerados en el Informe del grupo de trabajo.

¿Congresista Palma desea realizar algún informe?

No habiendo intervención, pasamos a la Orden del Día.

ORDEN DEL DÍA

El señor COORDINADOR.—

Primer punto.

Señor congresista, a la presente sesión fue invitado el experto en sistema de digitalización, el señor Enrique Mesones, habiéndose hecho las coordinaciones, pero por razones de su agenda no ha podido estar presente.

Segundo punto de la agenda. En este punto, señor congresista Marvin Palma, voy a presentar el Informe de nuestro grupo de trabajo sobre el examen del Decreto de Urgencia 006-2020 que crea el Sistema Nacional de Transformación Digital.

Reitero, en esta oportunidad nos corresponde presentar el Informe de examen del Decreto de Urgencia 006-2020 que crea el Sistema Nacional de Transformación Digital. Funciones que se nos ha encargado, la Comisión Permanente realizar, es por ello señor congresista Marvin Palma, que para el desarrollo del presente Informe se ha seguido estrictamente las disposiciones que contempla nuestra Constitución Política vigente, norma máxima en la legislación peruana.

En ese sentido, voy a explicar el alcance del Informe en materia de esta sesión, si es cierto que las exposiciones del Poder Ejecutivo han sido amplia, muy técnica, pero tiene dos componentes el Informe, la parte técnica y la parte legal constitucional.

A eso entramos, en ese sentido voy a explicar el alcance.

En esta sección se examinará el principio de razonabilidad y proporcionalidad del Decreto de Urgencia 006-2020. El Decreto de Urgencia 006-2020 señala de manera expresa que la política y estrategia nacional de transformación digital serán los instrumentos estratégicos y orientadores para la transformación digital del país; sin

embargo, posterga la formalización de ambas herramientas en un plazo de 90 días hábiles luego de publicado el decreto de urgencia.

Al respecto, es menester referir que el criterio de conexidad dentro del principio de razonabilidad establece que las medidas extraordinarias y los beneficios que su aplicación produzca deben pues surgir del contenido mismo del decreto de urgencia y no de acciones diferidas en el tiempo, pues ello sería incongruente con una supuesta situación excepcionalmente delicada.

Ese es una cita de la sentencia del Tribunal Constitucional 0028 de 2010.

Del mismo modo, se debe señalar que tratándose del contenido propio de la política y estrategia nacional pudieron ser aprobados en el marco de sus funciones mediante una ley ordinaria y no mediante un decreto de urgencia, conforme a lo dispuesto en el artículo 106.° de la Constitución Política del Perú.

Es decir, la postergación de los 90 días, en el peor escenario, recién en mayo de 2020, sabremos en qué consiste y cuáles son los objetivos de la política y estrategia nacional de transformación digital para su respectiva implementación, situación incongruente con la exposición de motivos respecto a la urgencia de la dación del decreto de urgencia que es materia de examen de nuestro grupo de trabajo.

Por otro lado, la exposición de motivos también trata de sustentar la necesidad de ampliar el plazo para que las entidades del Poder Ejecutivo puedan adecuar sus sistemas de trámite documentario o equivalentes para el envío automático de documentos electrónicos con otras entidades, así como dentro de sus áreas, órganos y unidades.

El Decreto de Urgencia 006-2020, en su primera disposición complementaria, amplía este plazo de adecuación hasta el 31 de diciembre de 2021, sustentándose en que aún existe una brecha tecnológica en algunas entidades del sector público, lo que habría impedido el cumplimiento de lo establecido en el artículo 8.° del Decreto Legislativo 1310, esta situación lo califican como urgente, dado que el cumplimiento del decreto legislativo referido tenía como plazo máximo el 31 de diciembre de 2019.

Entonces, si bien puede afirmarse que la materia de políticas públicas en general no está vedada para la legislación mediante el decreto de urgencia, este grupo de trabajo considera que este tipo de normas deberían tramitarse ante el Congreso de la República, no cumpliendo los principios de razonabilidad para la emisión de este tipo de normas. Al respecto el Tribunal Constitucional destaca que para la Constitución, las fuentes normativas denominada ley comprende a las leyes ordinarias, las leyes orgánicas, las leyes de desarrollo constitucional y las que tienen una denominación asignada directamente por la Constitución y cuyas diferencias no radican en su jerarquía, ni en el órgano que las expide, sino en su procedimiento de aprobación y en las materias que regulan.

En cuanto al tipo ley ordinaria el mismo Tribunal señala que es la expedida por el Congreso de la República, inciso primero del artículo 102.° de la Constitución y su modo de producción está regulada por los artículos 105.°, 107.°, 108.° y 109.° de la Constitución, en rigor puede normar cualquier materia con excepción de las reservas a la ley orgánica, conforme al artículo 106.° de la Constitución y a las que sean materia exclusiva de los gobiernos regionales o locales.

En este contexto, el artículo 106.° del texto constitucional señala: Mediante leyes orgánicas se regulan las estructuras y el funcionamiento de las entidades del Estado previstas en la Constitución, así como también a las otras materias cuya regulación por ley orgánica están establecidas en la Constitución.

Los proyectos de ley orgánica se tramitan como cualquier otra ley, para su aprobación y modificación se requiere el voto de más de la mitad del número legal de miembros del Congreso. En este punto, cabe traer a colación lo señalado en la sentencia del Tribunal Constitucional número 0006-2018, mediante la que el Tribunal Constitucional analiza el principio de separación de poderes como una exigencia ineludible en todo estado democrático y social de derecho, de manera que dicha separación de las funciones básicas del Estado constituye una garantía para los derechos constitucionalmente reconocidos y para limitar el poder frente al absolutismo y la dictadura.

Por las razones jurídicas, y constitucionalmente expuesta, el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, forma parte de la estructura orgánica del Poder Ejecutivo, y por lo tanto, contendría materia incompatible con la facultad legislativa extraordinaria durante el período de interregno parlamentario, siendo ello así, el Poder Ejecutivo al extremo no podría legislar a través de un decreto de urgencia, sino a través de un proyecto de ley que sigan los procedimientos y faces que exige la Constitución y Reglamento del Congreso de la República, una vez que se instale el nuevo Congreso, teniendo en cuenta que es competencia exclusiva del Congreso de la República, de tal manera que este Decreto de Urgencia 006-2020 transgrede el artículo 106.° de la Constitución Política del Perú.

En ese sentido, este grupo de trabajo concluye con las siguientes conclusiones y recomendaciones:

Primera conclusión.

Que en concordancia con la Ley 29158, Ley Orgánica del Poder Ejecutivo, el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital, tendría materia incompatible con la facultad legislativa extraordinaria durante el período de interregno, toda vez que un sistema funcional debe ser creado únicamente mediante una ley; es decir, la creación de un sistema funcional del Poder Ejecutivo están dentro de las materias cuya regulación solo se puede realizar mediante actos legislativos propios del Congreso de la República y no a través de

decretos de urgencia, conforme lo dispuesto en el artículo 106.º de la Constitución Política del Perú.

En ese sentido, el Decreto de Urgencia 006-2020 transgrede el ámbito constitucional vigente de nuestro país.

Dos.

El Decreto de Urgencia 006-2020 no se ha justificado el carácter de urgencia respecto a la dación del mismo, ni se ha demostrado que lo normado corresponde a una situación de carácter imprevisible, más aún si en la fecha de la publicación de la norma en evaluación no se conoce cuál es la política y estratégica nacional de transformación digital, instrumento estratégico y orientador indispensable para lograr la transformación digital del país, quebrándose el criterio de conexidad requerida para los decretos de urgencia.

Corresponde elevar este Informe a la Comisión Permanente para que continúe el procedimiento, de conformidad para lo previsto en el segundo párrafo del artículo 135.º de la Constitución Política del Perú.

Recomendaciones.

Dado que el presente Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital no regula materia excepcional de suma necesidad, transitoriedad y generalidad, las que habilitan y legitiman los decretos de urgencia.

Resulta necesario declarar la inconstitucionalidad de dicho decreto más aún si un sistema funcional del Poder Ejecutivo solo puede ser creado mediante una ley expresa, de acuerdo con lo dispuesto por el artículo 106 de la Constitución Política del Perú y el estricto respeto al principio de separación de poderes que lo reafirma la sentencia del Tribunal Constitucional recaído en su sentencia 0006-2018, mediante el cual el Tribunal Constitucional denomina la separación de poderes como una exigencia ineludible en todo estado democrático social de derecho. (2)

Dos. Sin embargo, por la importancia de la transformación digital en nuestro país se recomienda al nuevo Congreso de la República, periodo 2020-2021, priorice en la agenda legislativa la presentación, debate y aprobación de la iniciativa legislativa, ley que crea el Sistema Nacional de Transformación Digital.

Tres. Que el nuevo Congreso de la República periodo 2020-2021, al margen de la primera recomendación, encargue a la Comisión de Ciencia, Innovación y Tecnología el seguimiento de la formulación, aprobación, implementación de la política y estrategia nacional de transformación digital, a cargo de la Presidencia del Consejo de Ministros, política necesaria e indispensable para lograr la transformación digital de todas las instituciones de nuestro país.

Por tal razones, pongo en su consideración, señor congresista Marvin Palma y seguidamente para elevarlo a votación.

Quiero recalcar que nosotros no estamos aprobando ni rechazando el decreto de urgencia, simplemente estamos haciendo el análisis, el examen de esto y lo vamos a elevar a la Comisión Permanente, donde ahí será el debate y seguirá su siguiente paso de acuerdo a ley.

Entonces, pasamos. Casi el mismo sentido tiene el 007, voy a las conclusiones.

A este grupo se nos encargó el análisis del 006 y el 007, por eso lo estamos haciendo por separado cada análisis. Ahora voy a pasar al 007, ampliando la agenda de este grupo de trabajo.

¿Algunas observaciones?

Entonces, por esta ampliación de agenda para concluir y acelerar este análisis, pasamos a votación sobre la ampliación de agenda.

Los que estamos de acuerdo, por favor. A favor, por unanimidad.

Entonces, respecto al 007, las conclusiones.

Uno. Que en concordancia con la Constitución Política del Perú el Decreto de Urgencia 007-2020, decreto de urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento contendría materia incompatible con la facultad legislativa extraordinaria durante el período de interregno, toda vez que la Ley de Presupuesto y las modificaciones presupuestales deben ser aprobado únicamente mediante una ley; es decir, estas materias cuya regulación solo puede realizar mediante acto legislativo propio del Congreso de la República y no a través de un decreto de urgencia conforme lo dispuesto por el artículo 78.°, 80.° y 101.° de la Constitución Política del Perú.

En ese sentido, el Decreto de Urgencia 007-2020 transgrede el ámbito constitucional vigente de nuestro país.

Dos. No se ha justificado el carácter de urgencia respecto a la dación del Decreto de Urgencia 007-2020, ni se ha demostrado que la norma corresponde a una situación de carácter imprevisible, más aún si en la fecha de la publicación de la norma de evaluación no se conoce cuáles son los principios, modelos, políticas, normas, procesos, roles y estándares mínimos del marco de confianza digital del registro nacional de incidentes de seguridad digital, ni los plazos de implementación de los centros nacional de seguridad digital y del centro nacional de datos, que permitan asegurar y mantener la confianza en el entorno digital, quebrándose el criterio de conexidad requerido para los decretos de urgencia.

Tres. Corresponde elevar este Informe a la Comisión Permanente para que continúe el procedimiento de conformidad con lo previsto en el segundo párrafo del artículo 135.° de la Constitución Política del Perú.

Recomendaciones.

Dado que el presente Decreto de Urgencia 007-2020, decreto de urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, no regula materia excepcional de suma necesidad, transitoriedad y generalidad, tales que habilitan y legitiman los decretos de urgencia, resulta necesario declarar la inconstitucionalidad de dicho decreto.

Dos. Por la importancia de implementar el marco de confianza digital en el Perú se recomienda al Poder Ejecutivo, una vez instalado el nuevo Congreso de la República, período 2020-2021, priorice la presentación para su debate y aprobación de la iniciativa legislativa, ley marco de confianza digital.

Tres. Que el nuevo Congreso de la República, período 2020-2021, al margen de la primera recomendación, encargue a la Comisión de Fiscalización, realizar el control parlamentario al contrato de préstamo número 4399/OC-PE, especialmente en la tercera operación de endeudamiento externo, hasta por cincuenta millones de dólares, que financiaría el proyecto, mejoramiento y ampliación de los servicios soporte para la provisión de los servicios de ciudadanos y las empresas a nivel nacional, a cargo de la Presidencia del Consejo de Ministros, la PCM, que tiene por objetivo mejorar y ampliar los servicios de soporte para la provisión de los servicios ciudadanos y empresa.

Lima, 10 de febrero de 2020.

Dese cuenta.

Si hay alguna observación respecto a estos dos Informes, congresista Marvin Palma. Ninguna.

Entonces, pasamos a votación los dos Informes. Uno por uno mejor, lo más correcto.

Sobre el Decreto de Urgencia 006-2020, votar, por favor. Aprobado por unanimidad.

Sobre el Decreto de Urgencia 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. Los que están de acuerdo por su aprobación de este Informe. Aprobado por unanimidad.

Bueno, antes de cerrar el Acta quiero dejar constancia que la exposición técnica y del objetivo de los estos decretos son muy importantes para el país, pero viendo las inconvenientes legales constitucionales, en eso se basan nuestro Informe y yo creo que en el Pleno de la Comisión Permanente, quizá se podría dar más alcance y concluir con la aprobación de este Informe, conforme manda en esta etapa de interregno.

Bueno, señores, no habiendo más puntos que tratar en la agenda, hasta este momento, se consulta la dispensa del trámite de sanción del Acta de la presente sesión, a fin de ejecutar los acuerdos adoptados.

Quienes votan a favor. Ha sido aprobado por unanimidad.

Siendo las 3 con 35 minutos, del lunes 10 de febrero de 2020, se levanta la sesión.

Muchas gracias, señor congresista y a la comisión de apoyo.

—A las 15:35 h, se levanta la sesión.

GRUPO DE TRABAJO DE EVALUACIÓN DEL DU 006-2020, QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL Y DEL DU 007-2020, QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO.

Día: Jueves 30 de enero del 2020

Hora: 10:30 am

Lugar: Sala María Elena Moyano - Palacio Legislativo

AGENDA

I. INTEGRANTES DEL GRUPO DE TRABAJO

- Ángel Neyra Olaychea - Coordinador
- José Marvin Palma Mendoza

II. ACTAS

- Aprobación del Acta de la Sesión de Instalación, realizada el 22 de enero de 2020.

III. INFORMES

IV. PEDIDOS

V. ORDEN DEL DÍA

- Exposición de funcionarios de la **Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros**, para que informen sobre las razones que motivaron la dación del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.
- Exposición de funcionarios del **Ministerio de Justicia y Derechos Humanos**, para que informen sobre las razones de necesidad, urgencia y justificación que motivaron la dación del Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.
- Exposición de funcionarios del **Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual**, para que informen sobre las razones de necesidad, urgencia y justificación que motivaron la dación del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.
- Preguntas de los congresistas asistentes. Intercambio de ideas.

Lima, 28 de enero de 2020.

GRUPO DE TRABAJO

DECRETO DE URGENCIA 006-2020, DECRETO DE URGENCIA QUE CREA
EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL

DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE
APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS
PARA SU FORTALECIMIENTO

Asistencia Primera Sesión
Lima, jueves 30 de enero de 2020,
10:30 horas
Sala María Elena Moyano
Palacio Legislativo

INTEGRANTES	
	NEYRA OLAYCHEA ÁNGEL COORDINADOR Fuerza Popular
	PALMA MENDOZA JOSÉ MARVIN Cambio 21

CONGRESO DE LA REPÚBLICA
Es copia fiel del original
17 FEB 2020
HUGO CORTEZ TORRES
Fedatario

Área de Transcripciones

**CONGRESO DE LA REPÚBLICA
PERIODO LEGISLATIVO 2019-2020**

**COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA
GRUPO DE TRABAJO ENCARGADO DE ELABORAR EL INFORME DEL
DECRETO DE URGENCIA 006-2020, DECRETO QUE CREA EL SISTEMA
NACIONAL DE TRANSFORMACIÓN DIGITAL; Y EL DECRETO DE URGENCIA
007-2020, DECRETO QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y
DISPONE MEDIDAS PARA SU FORTALECIMIENTO**

**SESIÓN
(Matinal)**

**JUEVES, 30 DE ENERO DE 2020
COORDINACIÓN DEL SEÑOR ÁNGEL NEYRA OLAYCHEA**

—A las 10:43 h, se inicia la sesión.

El señor COORDINADOR.— Muy buenos días.

En la sala María Elena Moyano, hoy, jueves 30 de enero de 2020, se da inicio a la sesión del Grupo de Trabajo encargado de elaborar el informe del Decreto de Urgencia 006-2020, decreto que crea el Sistema Nacional de Transformación Digital, así como el Decreto de Urgencia 007-2020, decreto que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.

Para esta sesión vamos a recibir la información —a quienes saludo y agradezco su presencia— de nuestros invitados para que nos den alcances y algunos detalles con la finalidad de elaborar un informe. Como esta es materia muy técnica, nosotros también solicitamos que por escrito nos alcancen esa información, porque la próxima semana debemos cerrar el informe. Esa es la intención.

Reitero mi agradecimiento. Por favor, les invito a tomar asiento. Por favor, ayuden a ubicar a nuestros invitados.

Este grupo está constituido por el congresista Marvin Palma Mendoza, que está en camino, pero como es para recabar información, estamos dentro de lo correcto.

Iniciamos esta sesión informativa, dando la bienvenida a la señora Marushka Chocobar Reyes, directora de la Secretaría de Gobierno Digital; al señor Fernando Veliz Fazzio, —este pasa—; a los funcionarios del Ministerio de Justicia y Derechos Humanos, señor Eduardo Salcedo Guillén, del gabinete de asesores; señora Anaís Zavala Huaisara, de la Autoridad Nacional de Protección de Datos, y señor Eduardo Luna Cervantes, director de la Autoridad de Protección de Datos; a los funcionarios de Indecopi, señora Wendy Ledesma Orbegoza, directora de la Autoridad Nacional de Protección del Consumidor, y señor Josué Sandoval Zevallos, de la Autoridad Nacional de Protección del Consumidor.

Vamos a darle la palabra a la señora Marushka Chocobar Reyes. Tienen el tiempo que ustedes consideren necesario.

Créame que yo sí entiendo lo que van a hablar, es mi materia, no se preocupen. También estoy muy interesado por estos temas.

Tiene usted la palabra, señora Wendy.

La señora DIRECTORA DE LA SECRETARÍA DE GOBIERNO DIGITAL, Marushka Chocobar Reyes.— Muy buenos días, congresista Ángel Neyra. Muchas gracias por recibirnos esta mañana.

Venimos acompañados de la Autoridad Nacional de Protección de Datos del Ministerio de Justicia, del equipo de Indecopi y de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

Le agradecemos los minutos que nos va a conceder para poder sustentar estos decretos de urgencia que son importantes para nuestro país y que esperemos, de alguna manera, usted pueda despejar sus dudas o sus comentarios.

Vamos a comenzar con la sustentación del Decreto de Urgencia 006, que crea el Sistema Nacional de Transformación Digital.

En primer lugar, me gustaría comentar cuál es el contexto que hoy viene rodeando tanto al Perú como al mundo con respecto a la evolución digital y de manera más cercana cuáles son aquellos problemas de nuestra sociedad, en particular del Perú, que pudiéramos nosotros estar impactando positivamente con el despliegue de tecnologías digitales.

Tenemos un reciente informe sobre el dinero que pierde el Perú con respecto a los actos de corrupción. Y en los actos de corrupción es claro que esta situación afecta a los ciudadanos. Las tecnologías digitales pueden acelerar todo tipo de acciones para poder prevenir actos de corrupción y garantizar la transparencia en los actos públicos.

De la misma manera, no es una noticia nueva que tenemos también un serio problema con el avance de los feminicidios y estamos seguros que existe la urgencia por frenar esa situación. La tecnología puede permitir que exista

trazabilidad, que exista predictibilidad con respecto a estudio de patrones, usando inteligencia artificial, y que de alguna manera se puedan prevenir ciertas situaciones tomando decisiones sobre la base de datos, decisiones basadas en datos.

Tenemos también una situación digital en el sector Educación. Más del 69% de los colegios hoy no tiene conectividad, hay un esfuerzo importante del Estado para poder llevar conectividad a todas las regiones, pero todavía la brecha es importante. De la misma manera, hay más de dos millones de niños que están expuestos a riesgos digitales.

Se viene avanzando también en la capacitación de docentes, pero tenemos un 81% de docentes en el Perú que todavía no han sido incorporados a las tecnologías digitales.

Y lo más interesante e importante de mirar de cara a cómo viene la evolución digital en el mundo, es que el 65% de los niños hoy están estudiando carreras, probablemente, o están siendo preparados para un futuro del trabajo, que es totalmente diferente. El futuro del trabajo es algo que viene analizando el Foro Económico Mundial y sobre lo cual existe una gran preocupación.

Si miramos, esta es la situación a nivel del sector Educación, pero también nos preocupan las pequeñas y medianas empresas. En el Perú solamente el 12% de las pequeñas y medianas empresas compran por Internet, y solo el siete vende.

Sin embargo, si hacemos un análisis más profundo del millón setecientas empresas que hoy son formales, aquellas que se acercan a lo digital facturan el doble. Significa que hay una gran oportunidad en la promoción de la economía digital para poder promover, efectivamente, los espacios productivos para las pequeñas y medianas empresas.

En el mundo también, congresista, no se está evaluando ya solamente la brecha digital, se está evaluando no solo el acceso, sino cómo la población puede utilizar las tecnologías en favor de su propio bienestar y del desarrollo económico y social.

Y hay un estudio español que dice que también estamos evaluando el aprovechamiento de la tecnología para el ejercicio de deberes y derechos en el mundo digital.

Por esa razón es que el avance y el cierre de brechas que tiene que ejercer el Perú son inminentes y los números de alguna manera están puestos en cada noticia que aparece día a día.

Tenemos también una noticia que salió el año pasado con respecto al entorno para hacer negocios en el Perú, el *ranking* del *Doing Business*. La noticia no fue buena, el Perú pasa por su peor momento en los últimos 15 años para hacer negocios y hay un informe del Foro Económico Mundial que relaciona directamente la digitalización de un país con la competitividad, por lo tanto, la forma en que un emprendedor puede hacer negocios.

La digitalización pone al ciudadano, a las empresas y al gobierno en general en una nueva manera de toma de decisiones. Hay nuevas herramientas y también se promueve la transparencia en la provisión de los servicios públicos.

También tenemos el informe del IDH, del Índice de Desarrollo Humano, que si bien refleja que el Perú va subiendo en los últimos años hasta el 60% en la mejora del IDH, también se generan nuevas desigualdades. Eso lo menciona el informe. El Perú ha crecido 60% en los últimos 16 años, subsisten brechas, pero hoy se abren nuevas desigualdades con dos fenómenos que están ocurriendo en el mundo: el cambio climático y la revolución digital.

Por lo tanto, concluyen que aquel país que no aproveche el uso de la tecnología en favor de la población, está generando desigualdades, pero que ya no van a crecer de manera... que van a crecer de manera exponencial, porque, efectivamente, no solo se trata de acceso, sino también se trata del uso y el aprovechamiento de la tecnología en favor de las personas, de la gente.

Una mirada internacional nos ubica en uno de los países donde desarrollar un trámite es mucho más largo en cuestión de tiempo que con nuestros compañeros, por ejemplo, de la Alianza del Pacífico. En el Perú solamente el 30% de los trámites, de acuerdo a un informe del Banco Interamericano de Desarrollo, se resuelve la primera vez. O sea, el ciudadano va una vez al Estado y lo resuelve sin necesidad de regresar. Sin embargo, el 70% de los trámites no.

El mismo informe indica que un trámite en el Perú demora 8.6 horas. Hay sin duda una necesidad inminente de que al interior del Estado también aceleremos en procesos de digitalización.

A nivel de la ONU nosotros nos encontramos en el puesto 77 de 139 economías. Esto en evolución de digitalización al interior del sector público en combinación con el sector privado.

Pero cuando ya vamos al aprovechamiento de tecnología, que esto es un informe del Foro Económico Mundial, nos encontramos en el puesto 90, también de 139 economías.

El Perú acaba de lanzar dos grandes políticas fundamentales para el avance del país y con ello el avance de la población:

Primero. La política nacional de inclusión financiera. Hoy vemos que cada vez más pequeñas y medianas empresas utilizan tecnología con pagos digitales, y eso también involucra que, efectivamente, la tecnología se pueda poner al servicio de la población. Existe ya la política nacional de inclusión financiera sobre la cual se prioriza el despliegue de plataformas digitales para colaborar con los objetivos de la política.

El 46% de las medidas del plan de competitividad y de productividad hacia el 2030 tienen un componente de transformación digital y de alguna manera se ha

transversalizado en este plan el uso de tecnología para poder acelerar el logro de los objetivos.

En este contexto, señor congresista, esta no es una responsabilidad solamente del Estado, es una responsabilidad que tenemos que compartir con el sector privado, con la academia, con la sociedad civil, y por eso es que los hemos incluido en un Sistema Nacional de Transformación Digital que evoluciona solamente el ámbito público a comprometer al sector privado en esta tarea.

Es fundamental la integración del sector privado por el aporte que pueden tener en cuanto al conocimiento de tecnología, pero también con compartir una única visión y una única agenda.

¿En qué consiste la norma?

La norma tiene como finalidad fortalecer la institucionalidad digital en el Perú. Si nosotros miramos países cercanos, tenemos una Colombia que tiene un Ministerio de Tecnología de la Información y Comunicaciones, pero al mismo tiempo tiene una asesoría directa al presidente, que es una alta consejería en temas de transformación digital, ubicado a nivel de la presidencia.

Si miramos, por ejemplo, Uruguay, existe una Agencia Nacional de la Sociedad de la Información y el Conocimiento. Igual en México existe una Coordinadora Nacional de Transformación Digital.

Ninguno de estos tres países tiene el arreglo institucional, que puede tener la Presidencia del Consejo de Ministros, y hemos considerado que es importante respetar la recomendación de la OCDE de colocar los temas digitales en el centro de gobierno.

Entonces, finalidad es fortalecer la institucionalidad con un ente rector para dirigir la agenda digital del país, no solamente la agenda digital del sector público.

Segundo. Con esto definimos una ruta articulada público-privada para un proceso de transformación digital donde se promueva la economía digital, la educación digital, la conectividad y también el gobierno digital.

Impulsar la innovación digital y el fortalecimiento de una sociedad que sea más inclusiva no solamente con el acceso a la tecnología, sino también con el ejercicio de deberes y derechos de los ciudadanos.

Fortalecer el ejercicio de una ciudadanía digital. Y aquí es muy importante porque hemos involucrado a los mismos ciudadanos dentro del sistema, lo que involucra que existan responsabilidades, no solamente derechos, de los ciudadanos para comportarse en el mundo digital.

Promover la economía digital, la competitividad, la productividad y la inclusión financiera también es importante dentro de este decreto de urgencia.

45

Finalmente, fortalecer el acceso y la inclusión a las tecnologías digitales en el país, dependiendo de aquello que realmente cubre las necesidades de los ciudadanos. Sabemos que la tecnología puede involucrarse en cualquier sector productivo y también para resolver cualquier problema de la población, de alguna manera acelera la resolución de este tipo de problemas.

La norma crea el Sistema Nacional de Transformación Digital, que en términos generales es un ecosistema que evoluciona lo que existía como Sistema Nacional de Informática. Involucra al sector privado, a la academia, a la sociedad civil y a los ciudadanos.

Establece principios en torno a la transformación digital. De hecho define la transformación digital como un proceso continuo, disruptivo, estratégico y de cambio cultural que genera valor finalmente para las personas. Usa tecnología, usa datos, pero genera finalmente valor para las personas.

Define la materia de transformación digital incorporando también la innovación digital, sin afectar las autonomías dentro del Estado, sin afectar las economías del sector privado. Se trata de construir una agenda común.

Establece también las funciones de un ente rector, fortaleciendo la institucionalidad.

Finalmente, da cumplimiento a las recomendaciones de la OCDE con respecto a gobernanza digital.

Con respecto al Sistema Nacional de Transformación Digital y a este Decreto de Urgencia 006, consideramos que lo contenido en la norma favorece fuertemente al avance de la digitalización en el país y ordena las rutas separadas que veníamos siguiendo el sector público y el sector privado hacia una agenda compartida, pero que (2) finalmente tenga un único objetivo, que es mejorar la competitividad y fomentar la economía digital en el país. Este es el primer decreto de urgencia.

El señor COORDINADOR.— Okay.

Agradecemos.

Bueno, tenemos un comentario. En primer lugar, por el punto, perdón. Estamos de acuerdo sobre la motivación y la visión que se quiere con el avance tecnológico y lo atrasado que estamos en esa materia. En eso no hay discusión.

Lo que sí motivado a ese objetivo, a esa visión, la pregunta sería de mucho, ¿cuál es la proyección? O sea, ¿qué indicadores tenemos para medir? ¿De acá a cinco años, qué cosa vamos a avanzar? ¿Y de acá a 20 años, qué vamos a tener?

Acá no estamos diciendo que esto va a tener éxito en año y medio, pero lo importante es, como todo planificado, en política pública es a largo plazo, el objetivo de acá a 20 años, nuestra productividad en esta materia o en estos sectores gracias

4p

a la tecnología digital o al propósito de esto, vamos a lograr este grado de competitividad, de productividad.

Pero cuando se habla de productividad hay que hablar de muchos sectores también, porque productividad es muy... Yo puedo decir productividad es directamente proporcional a la producción, inversamente proporcional a los costos de implica de los factores. Pero eso es la fórmula, sino la conclusión, los resultados.

No importa que demore 20 años lograr una meta de lo que ustedes fijen, pero podemos decir en 10 años "¡oiga!, nos faltan 10 años", porque esto lo venimos viendo en muchas materias como la productividad, por ejemplo, no, la competitividad, el Plan Nacional de Competitividad. Te conozco de memoria el primer plan, conozco lo que es el Consejo Nacional, y ahora estamos entrando nuevamente al Plan Nacional de Productividad y Competitividad; hemos aumentado la palabra productividad.

Y como Michael Porter dijo, la mejor forma de alcanzar la competitividad es lograr primero las metas de productividad de un país, nacional. O sea, ¿me entiendes? La visión, el deseo está perfecto, y de hecho que el informe es positivo, pero vamos a pedir recomendaciones y a precisar en dónde es el sector. Y le voy a explicar por qué, en el sector que yo conozco bastante, el sector industrial, la manufactura.

Antes era el 15% del PBI, ahora creo está en caída. Y ese análisis lo ha hecho con la información que me dado la Sunat, le he pedido la información de todos los empresarios, de todos los empresarios, desde el año 2011 al 2017.

Hay sectores como cuero y calzado que están en caída. La pregunta es: ¿en qué momento, en qué siglo o en qué década vamos a tratar ese sector que es importante, un sector importante que está cayendo? Estamos hablando de la productividad, estamos hablando de muchos factores: el ordenamiento territorial, no tienen territorio; los insumos son caros, ¿no es cierto?; tienen denuncias por el tema ambiental, o sea, están en exterminio.

Entonces, la pregunta: ¿no tiene que ver nada con esto? Perfecto.

Miren, yo estoy mirando la productividad regional, no tenía información, tenía información desde la Sunat.

Entonces, medimos 700 empresas en Tacna, de las cuales solo dos decían que tenían de productividad cuatro, imagínese, cuatro, o sea, altamente rentable, porque si tú divides la producción, ventas versus los factores, pero si lo restas esa es la utilidad bruta.

Si decimos que tiene productividad, una es que compra pan para vender pan. Es economía de supervivencia. Pero si tiene cuatro, ¡caramba!, es de acumulación.

Pero el 99% tenía productividad negativa, ¿sabe lo que pasa? Que son formales. Lo que pasa es que declaran. Estos que tienen alta productividad declaran sus

42

ventas mas no sus compras, no su planilla. O sea, hay un grado de informalidad dentro de la formalización, y eso no lo han visto. A cuántos ministros les he contado eso.

¿Y los otros qué es lo que pasa? Declaran sus compras, mas no sus ventas. Lo que llaman "San Francisco".

Entonces, tienen una productividad negativa. Obvio. Tienen más costos que venta. Eso es con la información de la Sunat oficial.

Entonces, ¿cómo vamos a ayudar a la productividad de estos sectores?

Solamente a los de arriba, a los grandes, a leche Gloria, a Saga Falabella, a las mineras, las carreteras y los puentes solamente van a ser. ¿Y los indicadores de ellos, los de arriba, es lo que vamos a responderle a la OCDE?

Entonces, yo les digo, de abajo, de abajo cómo se ven las cosas.

Entonces, cuando yo profundizo, y que el concepto de competitividad también, está bien, la competitividad estamos creando infraestructura, puentes para... Oye, ¿pero qué producto es lo que vamos a trasladar?

Cuando hablamos de productividad estamos hablando de producción y servicios que van a competir. La competitividad.

¿Cuál es el mercado? ¿Cuál es esta fuerza de los proveedores que influyen a mi competitividad negativa? La competencia. Eso cuando hablamos de competitividad, porque ustedes me están hablando de la micro y pequeña empresa; entonces, yo me bajo a la microeconomía.

Ahora, si ustedes me dicen, "no, los indicadores macroeconómicos, que ya tenemos más carreteras, tenemos la red, todo, y eso no da un indicador", no, no, el indicador es qué producto coloco yo al mercado, esa es la economía.

El costo de producción de esto es diez dólares, el costo de materiales —son los factores de producción— tres dólares, pero se vende a mil dólares. ¿Me entiende? Entonces, a eso vamos.

Yo veo, por ejemplo, la ministra de la Producción dice, "vamos a hacer parques industriales", sí, pero lo que está promoviendo son lotizaciones en vez de ayudar a la zona productiva. No, eso va a ayudar, quizás, a una constructora que el Estado va a pagar seis millones y le va a mejorar la plusvalía y para que pueda vender bien los lotes, no está ayudando a la productividad ni a la competitividad, porque el 99% de nuestro universo industrial en el Perú es micro y pequeña empresa y solo el 1% es gran y mediana empresa.

UB

Entonces, ¿cuál es la política que estamos haciendo, para los de arriba o para los de abajo? Eso es el malestar. Esto no tiene que ver nada con el Congreso, nada, sino la gente del día a día, él que vive su día a día.

Otro de la productividad, Mesa Redonda. Mesa Redonda en cualquier momento se va a incendiar, va a haber una tragedia, eso es sin lugar a duda.

Le hemos dado espacio, le hemos cobrado impuestos, le hemos autorizado que comercialice, la importación, todo. Ahora no, ahora quiero que se vaya. Ves, ahora quiero que se vaya. ¿Y a dónde me voy? Eso es lo que no se está viendo.

Por eso, digo, esto está muy bien, pero a nosotros lo que nos gustaría saber para nuestra recomendación, para ponerlo para ver la visión, ¿no es cierto?, qué indicadores dicen. Está bien, que estamos mal, que vamos a instalar la red dorsal, ya lo tenemos, todo eso está bien, sino cómo va a influenciar esto en el PBI o en la productividad de Tacna o de Ayacucho. Esa es la motivación, que nos diga, "¡caramba!, de acá a diez años nosotros vamos a tener este acceso".

Porque yo ahorita veo si mi mascota se ha subido al mueble, yo lo tengo, yo lo puedo ver, y lo voy a llamar. O sea, estamos utilizando.

Pero el otro punto es qué valor va a generar esto en esos campos de la economía y especificarlo en Lima. Lima es un desorden territorial terrible, el caos del tráfico es terrible porque toda la industria, el 60% de la industria está en Lima y está en el casco urbano. O sea, que no van a resolver nunca jamás el tema del ordenamiento del tráfico, todo está congestionado, va a haber más ambulantes, obviamente, donde hay movimiento ahí están. Así como los puertos antiguos, donde hay puerto ahí está todo el movimiento, así como Gamarra.

Entonces, lo digo esto, en buena leche, como se dice, porque conocemos el tema.

Yo les invito también, ya que están todos, yo viajé últimamente a Corea, a un foro el 13, donde justamente hablan de hospitales digitales, conoce la seguridad digital, que me dicen que las elecciones dentro de poco van a ser solamente por celular. Punto, más barato, listo, la gente no se mueve.

Por celular yo pongo un aplicativo, yo elijo el sistema, "papá, eso es fácil", pero el... No, es mucho mejor en el momento en que tú haces tu voto, pasas uno a los partidos, pasas otro, no sé, a la ONPE y pasas otro al Ejército y listo. Y todo el mundo, y creo que todo el mundo sabe la información como se mueve... los pico. Entonces, eso lo vi allá.

Le cuento otra investigación digital. Yo estaba sentado acá, yo nomás escuchaba la música y ustedes no escuchaban la música. Fui a una universidad de investigación científica, me sacaron esto así, lo último fue por Purdue, acá en Indiana, increíble en agricultura como aplican los drones, la investigación, todo lejos, y podemos ver cómo en Estados Unidos en 200 años de la PEA, que era agricultura el 87%, en 200 años, esa es información de la OCDE, 2% de la PEA en agricultura.

ya

¿Que no ha desarrollado? Es una potencia. ¿Pero dónde se ha desplazado esa PEA que ya no está en agricultura? En los TIC, tecnología investigadora, el 67% de la gente ahí quedó. Ese es el impacto de lo que estamos conversando acá, ellos en 200 años.

Por eso, decía, si ustedes dicen que en 20 años vamos a lograr este grado de productividad en este, este..., como lo están diciendo, competitividad, la productividad, ese tema. Eso es lo que hay que trabajar, decirlo para qué. Para que los alcaldes, porque pasan los alcaldes y se olvidaron; viene otro gobierno y se olvidaron. Así como el ministro de la Producción, cada ministro de la Producción tiene su propia agenda personal y sectorial, no hay política ahí. ¿Por qué? Porque tenemos la Ley General de Industrias del año 1982.

Yo he sacado la Ley de los Parques Industriales que es mejor, 100 veces mejor que la ley, que tiene los objetivos, el desarrollo sostenible, la OCDE, todo, pero a la ministra de la Producción no le interesa. Ella está pensando cómo desarrollar el parque industrial de Ancón para beneficiar a algunas constructoras, pero no a la productividad y a la competitividad. Ese es el tema. O sea, en el sector de Producción cómo va a ayudar esto.

Ahora, yo los invito al gremio al que yo pertenezco, estamos mucho más adelantados en América Latina, en la tecnología, desarrollo del litio, baterías. Pero la ministra no quiere ir, los ministros, porque quedan mal, pues. Ellos están avanzando solos, y nosotros que somos el ente rector no hemos puesto nuestra cuota para la pollada. Esa es la preocupación. Y créanme, lo que usted ha resumido, todo, todo, está muy bien la visión, estamos atrasados y es una necesidad de ponernos al día. Y con esto término.

Va a haber un momento en que se va a inventar un casco, me lo voy a poner en la cabeza, voy a pensar y al lado una impresora y va a salir mi pensamiento, el escrito o el plano que he pensado. Eso es posible. La pregunta es: ¿Cuál es más importante, la tecnología que me he puesto o el pensamiento? El conocimiento. Eso nos falta.

¿Qué cosa va a fluir por la red digital? Conocimiento, va a generar valor a la sociedad. Entonces, paralelamente eso tenemos que medir.

De qué vale llenar de computadoras, red a todas las universidades, cuando no lo pueden aplicar.

Corea invirtió en un pequeño satélite en la UNI, ¿y qué pasó? Se tiraron los fondos. ¿Y qué tenemos? Me dejó entender.

También Corea regaló en el Callao también unos sistemas y nada. A la UNI le dio un sistema, nada.

Nosotros tenemos un sitio de energía que es el mejor de América Latina, con acreditaciones que podemos que exportar cualquier cosa. Mientras en otro país

5

cobran sesenta mil dólares la prueba, ahí se cobra mil ochocientos. ¿Se dan cuenta?

Nanotecnología. Pero no lo quieren visitar los ministros pues. Yo los invito para que lo visiten, porque ellos sí lo están aplicando y lo entienden y van a apoyar este tema. Yo también lo voy a apoyar obviamente. Pero hay que decir cuál es la meta de acá a tres años, qué es lo que vamos a ver en tres años, qué es lo que vamos a ver en cinco años.

Si esto va a demorar 50 años, demorará 50 años porque estamos en el Perú, pero que sea política que trascienda los gobiernos. Esa sería nuestra recomendación en simple, que trascienda y que se vea, para que el que venga lo siga, porque si no...

Yo voy a salir del Congreso y necesito esto también para poder trabajar. Gracias.

No sé si tienen más información.

La señora DIRECTORA DE LA SECRETARÍA DE GOBIERNO DIGITAL, Marushka Chocobar Reyes.— Le agradezco los comentarios, hemos tomado nota para poder dar...

Y tiene toda la razón con respecto a que tenemos que precisar más estas metas, porque efectivamente hay metas trazadas de aquí a los próximos años. Correcto.

Procedo, entonces, a sustentarle el Decreto de Urgencia 007. Si bien el Decreto de Urgencia 006 crea el ecosistema alrededor del avance en la transformación digital del país, también tenemos (3) que ser conscientes de los riesgos digitales.

Entonces, este decreto de urgencia aprueba un marco de confianza digital y dispone medidas para fortalecer este marco. El contexto es el siguiente.

El 2018 tuvimos un ataque informático importante en la banca, y recientemente, bueno, después de varios meses, fue el BCP el que dijo, efectivamente, fuimos hackeados y hubo fuga de datos personales. Hay un informe sobre todas las ciberamenazas que enfrentará el sector financiero al 2020.

De la misma manera, a inicios de enero hubo una inminente Tercera Guerra Mundial, Irán contra Estados Unidos, bueno, todo lo que conocemos, sin embargo enfocándonos en aquello que Irán pueda hacer o cualquier país que esté avanzado en temas de tecnología, se puede desplegar un ejército de *hackers* y ya no se necesita una bomba nuclear para afectar a la gente; basta con, por ejemplo, ingresar en las unidades de cuidados intensivos de un hospital y se hackean los sistemas y puede morir gente. O sea, se puede, en realidad, afectar a la población.

De la misma manera, existe ya hace tres días una exposición de datos personales importantes en una cadena de cines en el Perú. Entonces, nos damos cuenta que esto no solamente ocurre en el sector público, sino también en el sector privado, y no existía hasta antes de este decreto una obligación del sector privado de poder

51

reportar estos incidentes en un único gran repositorio de incidentes digitales que permitan que como país nos preparemos ante estos riesgos, no solamente de la seguridad digital propiamente dicha de los sistemas informáticos sino también de la protección de datos, y de la protección del consumidor cuando hace uso de servicios en el mundo digital.

De esta misma manera, por ejemplo, nos encontramos como país rezagados en materia de ciberseguridad o de seguridad digital frente a países de la región.

Otro tema que impacta directamente ya a las familias como tal es el avance del *grooming* en el Perú, y esto es un informe de la Divindat. El *grooming* es el acoso sexual a menores de edad a través de las redes sociales. Y eso ya tiene un avance en el país que no nos vamos dando cuenta. Entonces, necesitamos fortalecer la relación público-privada con respecto a estos riesgos digitales.

¿Cómo se ha definido la confianza digital? Y esto también está alineado a lo que vienen haciendo otros países. Estos dos decretos de urgencia van colocando al Perú poco a poco en una situación ya de liderazgo con respecto a temas digitales que tenemos que ir implementando de manera rápida, como bien usted lo ha comentado.

Es el Estado que emerge como resultado de cuán veraces, predecibles, éticas, que esa es una palabra central en el uso de tecnologías proactivas, transparentes, seguras y confiables, son las interacciones digitales que tienen las personas, las empresas, las entidades públicas, pero también las cosas. No existe el internet de las cosas; entonces hay que también pensar que esto ya no solamente es de celular y de laptop, no existe el internet de las cosas, con el propósito de impulsar el desarrollo de la economía y la transformación digital.

Esto, entonces, no es solamente una responsabilidad del Sector Público, tenemos que comprometer al sector privado de una manera mucho más eficiente.

Entonces, ¿cómo se define la confianza digital?

Existen tres grandes aspectos y uno transversal.

Primero. La seguridad digital que pasa por la disponibilidad tecnológica para poder hacer frente a los ciberataques, que tiene diferentes ambientes o ámbitos en la ciberinteligencia, la ciberdefensa, la ciberseguridad, y los ciberdelitos.

El segundo gran aspecto es la protección de los datos personales en el entorno digital y la protección del consumidor. Estos tres ámbitos tienen una fase transversal importantísima que es la transparencia y la ética en la gestión de los datos.

Los datos que tienen el sector público y sector privado tienen que ser usados de manera ética, para que los ciudadanos finalmente vean respetados sus derechos.

¿Cuál es la finalidad?



Definir una ruta del país en el marco de confianza digital.

Establecer principios, modelos, normas, procesos.

Impulsar la innovación digital, pero respetando la privacidad de los datos de los ciudadanos.

Y ejercer una ciudadanía digital con deberes y derechos. Y deberes también porque los ciudadanos también son dueños de sus propios datos y tienen que ser responsables, todos tenemos que ser responsables de lo que subimos a las redes sociales con respecto a nuestros datos.

¿Cuáles son los puntos centrales de la norma?

Establece medidas para garantizar la confianza de las personas en su interacción en el mundo digital, compromete al sector privado en este reto.

Define la confianza digital, la economía, el entorno de los riesgos digitales.

Define el marco de confianza digital, como lo acabo de presentar.

Establece un ente rector que guía la ruta hacia la confianza digital.

Crea tres componentes importantísimos en este tema:

Primero. El Registro Nacional de Incidentes Digitales, donde tendrán que reportar sector público y privado los incidentes, y que no nos tengamos que enterar de lo que pasa en el sector privado por un tuit o por una noticia después de varios meses sin poder haber hecho nada para proteger los datos de los ciudadanos. Siempre se resguardarán la reputación y lo que tenga que haber, pero es importante que exista este Registro Nacional.

Se crea el Centro Nacional de Seguridad Digital y el Centro Nacional de Datos. Señor congresista, nosotros tenemos, y qué bueno que usted haya podido visitar Corea, dos años de apoyo de la cooperación coreana. Ellos nos han hecho toda una asesoría en el diagnóstico tanto para el Centro Nacional de Seguridad Digital como para el Centro Nacional de Datos. De hecho nos llevan muchos años de avance en este tema.

Se establecen los datos como objetivo y como activo estratégico de las entidades públicas y privadas.

Establece la obligación de las empresas privadas de reportar estos incidentes digitales, y fortalece la gobernanza en materia digital en el país.

¿Cuáles son los puntos que recomienda la OCDE?

De manera general, es desarrollar un marco regulatorio adaptado digitalmente. Las normas tienen que nacer digitales, porque eso de alguna manera favorece el avance

para no estar encontrando normas que atentan contra el avance de la economía digital, y que más bien favorecen de alguna forma también al avance del desarrollo de las personas a nivel nacional.

Tenemos un avance importante a nivel de las regiones y el compromiso de los gobernadores y de los alcaldes, y estamos avanzando poco a poco, pero estamos avanzando en las regiones también.

Recientemente el Foro Económico Mundial, esta es una noticia de hace algunos días, ha creado su Centro Global de Ciberseguridad al que se conectará el Centro Nacional de Seguridad Digital del Perú. Y mire lo interesante, porque lo que hace es, crea, dice, "el Centro fomentará la colaboración público-privada contra las amenazas cibernéticas". Nos encontramos en esa misma línea para poder seguir avanzando en esta materia.

Finalmente, la política general de gobierno establece de alguna forma la guía para lograr estas metas hacia el 2020-2021. Creemos que la tecnología es un habilitador importante para dar cumplimiento a esta política, y pretendemos de manera central que esto tenga continuidad en los próximos años independientemente del gobierno, independientemente de quien está a cargo de la materia digital, estamos creando esta ruta, y creo que de alguna manera estamos dando pasos importantes para el país.

El señor COORDINADOR.— Gracias.

Ya que mencionó Corea, yo visité el Centro de Ciberseguridad de ellos, y era increíble, le voy a explicar qué problemas tenían ellos.

Ellos veían los bombardeos, un mapa mundi tenían, identificaban de qué país venía. Pero tenían un problema. Que no tenían convenio con esa empresa en la parte legal. Eso tienen que prever.

Ahora lo que me dice que el Banco Mundial está haciendo un sistema, ese es el tema, porque yo puedo identificar donde viene internamente, bueno, internamente puede decir.

En Rusia, también lo que yo vi, ellos identificaban con satélites, increíble. Ellos no persiguen al delincuente, al que asalta un banco, ellos lo siguen por satélite, y cuando el otro ya se cansó de corretear y esconderse, ahí recién interviene. O sea, el tema es de la seguridad.

El otro es también, últimamente cuando viajé los periódicos dicen, "congresistas viajan". Pero yo le voy a decir que cada vez que viajo transfiero la información; por eso estoy haciendo un foro el 13. Entonces, cuando yo les dije a los periodistas, ya me pararon, tranquilo. Yo fui ocho días y los ocho días tuve una intensa actividad con todos. Más bien el consejero comercial en esos eventos no apareció, el embajador no apareció, eso para que vean. Y si van, escuchan, pero no transfieren la información. Queda un informe en el gabinete pero no queda información.

54

Yo he viajado junto con una congresista. Ahora están viniendo como ocho de centros de cooperación a dar información de lo que hemos visto. Están dando información sobre los hospitales digitales, me enteré de esa intención que hubo, porque no cuajó en el gobierno anterior, hay mucho, como que hay 22 proyectos de Dohwa que están haciendo ingeniería, que la población no lo sabe, cree que solamente está haciendo Chinchero o el Metro 2, no, hay más proyectos importantes. Eso es lo que está faltando. Se debería informar a la gente de esta tecnología, de lo que ellos están haciendo. Hay mucha confusión de la intervención de otros países.

Eso es lo que se llama darle valor agregado a través de la tecnología. O sea, tenemos tecnología, pero nadie se entera de lo que sucede, de las buenas cosas que suceden. Lamentablemente los que tenemos es tecnología para las malas cosas que suceden; o sea, no genera valor en la ética y todo.

Entonces, eso es importante.

El 13 los invito, porque ellos están viniendo, hemos invitado a los ministerios, también a la PCM. Si, hoy día estamos corriendo las invitaciones para que ustedes opinen, es un foro, y de eso queda un informe. Cada vez que he viajado siempre hemos logrado eso. La vez pasada trajimos robótica, mandamos unos chicos de robótica, se han capacitado; los emolienteros también fueron, ahora tienen sus carritos con panel solar y hacen cargadores. Es cómo generamos valor a la tecnología. Ese es uno.

Y el otro es sobre la seguridad, la confiabilidad de este sistema, no solamente la información de los datos o de los ataques, también hay que dar la seguridad a los *hardwares*, o sea, de los instrumentos. Eso, ¿quién va a garantizar?, ¿quién acredita y quién certifica? El Sistema Nacional de la Calidad tendrá su parte acá en esta coordinación gobernanza, Indecopi. O sea, ¿quién acredita?

Por eso, yo les invito también al CITE Energía, ellos tienen un aparato que ellos pueden ver el grado de confiabilidad de este aparatito, lo ponen ahí en su cabinita y al instante sale como un fax el Certificado de Laboratorio KEMA, de Holanda, automático, está acreditado. Entonces, con eso ya puede recibir certificación, que no lo tiene ninguna universidad, nadie lo tiene.

Eso sería bueno para que vean como se vincula para dar garantía, y me gustaría que Indecopi vaya y haga un convenio, porque el CITE es parte de la ley, es parte del Estado, Ministerio de la Producción le da un fondo para que las Pyme hagan sus certificaciones, tienen tres, Convenio con Suiza, Convenio con Estados Unidos, tienen todo.

Entonces, ellos pueden demostrar que este aparato tiene confiabilidad, porque estos aparatos si tienen un problema de tierra, tienen un problema de carga, van a fallar los datos, puede distorsionar los datos, y eso lo sabemos. Ese es el único de última generación de tecnología, que no lo tiene ni Chile, no lo tiene México. Ellos están en el tema del sistema de electrificación, por eso es que están desarrollando

SS

el tema del litio. Saben que la batería, el litio, sí podemos exportar baterías. Es interesante ese tema, pero están solos.

Ya que está la PCM, le pido, vaya y visítelo, para que les jale la oreja a los demás ministros, porque esas cosas son muy importantes.

Yo les invito para que podamos... Y me comprometo que esto va a pasar, esto pasa.

El señor Salcedo, ¿está invitado? que tome asiento, ya estoy terminando.

Quería hacer esos comentarios ya que está acá Indecopi. ¿Quién garantiza que este aparato tenga?, ¿quién garantiza que este aparato no me va a explotar? Ese CITE lo hace, que comercialmente, claro, paga impuesto de su arancel y punto. Ellos pueden prever que esto va a calentar en 300 horas y el peligro que puede reventar la pila, ese aparato tienen todos ellos; pueden simular un radio, tienen todo para dar seguridad al sistema, no al *software*, sino al *hardware* también, al cuerpo y alma.

Gracias.

No sé quién va a continuar.

La señora DIRECTORA DE LA SECRETARÍA DE GOBIERNO DIGITAL, Marushka Chocobar Reyes.— Muchas gracias, congresista. Está bien.

El señor COORDINADOR.— ¿Alguna intervención más, por favor?

Ministerio de Justicia. Sí, por favor, empiece. Ustedes se toman el orden.

El señor REPRESENTANTE DE LA AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS DEL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, don Eduardo Luna.— Buenas tardes, señor congresista.

Eduardo Luna, de la Autoridad Nacional de Protección de Datos.

Solo agregar a lo que ya comentó Marushka, que este es un trabajo que es conjunto, que tiene los enfoques, por supuesto, desde el lado del consumidor, de Indecopi, desde el lado de la protección de datos, que es el que nos corresponde, y, por supuesto, como ente rector gobierno digital.

Solo agregar que desde el lado nuestro (4), por supuesto, vemos con satisfacción que se han insertado la lógica de protección de datos desde el lado de los principios.

El DU dedicado a la confianza digital, efectivamente, instituye una vía, hace visible una vía que antes se entendía como una buena práctica empresarial. Nosotros hemos recibido reportes de entidades del sistema financiero, dando cuenta de estas brechas de seguridad. No se han hecho público hasta que las propias entidades lo han hecho público, pero lo han hecho sobre la base de interpretar estas buenas

66

prácticas que ya son comunes en Europa, desde la vigencia del Reglamento Europeo, y que este decreto intenta plasmar, que lo plasma eficientemente.

Entonces, a través, por ejemplo, de este Registro Nacional de Incidentes de Seguridad, la Autoridad Nacional de Protección de Datos directamente podrá, como tiene acceso al mismo, iniciar las fiscalizaciones que correspondan para salvaguardar los datos personales de los ciudadanos que se vean eventualmente afectados por los eventos de ciberseguridad.

Por el lado nuestro, eso es lo que quería agregar.

Muchas gracias.

El señor COORDINADOR.— Por favor, señorita Wendy Ledesma.

La señora DIRECTORA DE LA AUTORIDAD NACIONAL DE PROTECCIÓN DEL CONSUMIDOR, doña Wendy Rocío Ledesma Orbegoza.— Muchas gracias, congresista Neyra, por darnos la oportunidad de poder exponer estas iniciativas.

Desde el lado de Indecopi, garantizarle que su preocupación en realidad es nuestra, venimos trabajando desde la aprobación de la política y el Plan Nacional de Protección de los consumidores, en todo lo referente a seguridad de productos.

Como usted bien ha señalado, ahora, por el internet de las cosas, pues se podrían dar afectaciones a los consumidores; por ejemplo, algunas alteraciones en los equipos, no solo a través de redes sociales, ahora estamos hablando hasta de refrigeradoras que se conectan en línea y con algunas direcciones de voz, pues uno puede dar las determinadas instrucciones, pero que también capta alguna información que se puede revelar allí.

Así que en eso estamos con entidades internacionales, como la OCDE, Naciones Unidas, incluyendo dentro de nuestras acciones nuestras directrices, o a las directrices que ha dado Naciones Unidas o las recomendaciones de la OCDE.

Asimismo, el Indecopi es presidente del Comité de Políticas del Consumidor del INACAL. Y allí este comité, es un comité espejo de ISO, y nosotros lo que hacemos es trabajar para que se puedan incorporar dentro de la normativa nacional normas técnicas en materia de protección al consumidor, que evidentemente están aprobadas con estándares internacionales y estamos trabajando en temas de autorregulación y también de ciberseguridad.

Así que cuente con nuestro apoyo también. Esperamos prontamente la invitación para participar de este evento, en el cual vamos a conocer otras tecnologías de otros países.

Gracias.

El señor COORDINADOR.— Hoy día mismo hacemos las invitaciones.

57 ✓

También si quieren conocer el tema del CITE Energía, pueden pedirle al INACAL, porque está vinculado con INACAL. El que desea oficiar, con ellos mismos, no vayan a pensar que tengo un conflicto de intereses, porque no tengo nada que ver.

Yo organicé ese sistema cuando vino Michael Porter, en el CADE 10. Nosotros hicimos un clúster, lo hemos formado.

Y no es público y no necesitamos hacer publicidad, porque no necesitamos competencia, eso es privado. Pero la ley, el Estado está invirtiendo en aparatos ahí, porque si no tendrían que irse a México, a Brasil, y les cobran quince mil dólares, sesenta mil dólares, lo que cobran treinta y cuatro mil dólares, treinta y ocho dólares, acá están cobrando mil ochocientos, solamente en viaje ya se ahorra.

Y si protocolo dice que la prueba debe ser dos pruebas, y si te falla la primera prueba, ya tiene que gastar más, otro viaje.

Eso sí ayuda a la competitividad, a la productividad, porque reduce los costos.

Entonces, eso es lo que espera el común y silvestre ciudadano que cuando escucha productividad y competitividad, ¿no es cierto?

Yo puedo tener una carretera, un tren bonito, pero no hay productos pues. Puede haber locomotora, pero no hay vagones que traigan productos. Entonces, no me ayuda en la competitividad en nada.

Señor Eduardo Salcedo, tiene usted la palabra.

El señor ASESOR DEL GABINETE DE ASESORES DEL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, Eduardo Salcedo Guillén.— Muy agradecido, señor congresista.

Acaso para concluir, porque en realidad me parece que ha sido muy amplio, al mismo tiempo muy enriquecedor en este grupo de trabajo.

Simplemente señalar que el sector competencia, el sector proponente y los organismos competentes en la materia que nos convoca han sido amplios y correctos y concretos en una situación que nos parece, efectivamente, crítica, es una situación álgida, y en la que lamentablemente el Perú está bastante atrasado, como usted muy bien ha podido identificar.

Esto implica de parte del Estado acciones concretas, que felizmente el gobierno ha podido dar en esta coyuntura actual; acciones concretas con las cuales nosotros estamos perfectamente de acuerdo, precisamente por ello estamos acá sentados con usted. Y por ello mismo, saludamos no solamente el conocimiento de usted y del grupo de trabajo respecto al tema, sino que lo aplaudimos y confiamos en que efectivamente todo lo que se vaya a hacer a raíz de esto, como Estado, como República del Perú, porque finalmente somos todos unos solo, va a repercutir sí y solo sí para el beneficio de la población.

SA

Dicho ello, no me queda más que tomarle respetuosamente la palabra y confiar que efectivamente los informes que se obtengan de este grupo de trabajo sean de aquiescencia y positivos, porque lo que queremos es trabajar a un solo norte. Es todo.

Muy agradecido.

El señor COORDINADOR.— Gracias.

Bueno, nosotros, como has dicho, este dialogo, esta reunión resalta los beneficios a futuro que esperamos. De eso no hay duda. Más bien yo puedo decir la pelota está ahora en la cancha de ustedes.

Pero a la población también incentívela diciéndole dentro de 10 años ya vamos a... no sé, algunas cosas que pueden ustedes identificar. Pero lo importante, como usted dice, han puesto hasta el 21, deberían proyectarlo mucho más, como es proyección, pero al menos poner la meta para que el que venga y la misma población presione al que venga, presione. "Ustedes me dijeron esto".

No vaya a pasar como ese camión que voló en Villa El Salvador. Revisión técnica, ¿quién se hace responsable?

Y yo estuve en esa comisión. Se quejaban. A la revisión técnica van carros... Cómo pasan la revisión técnica, quién controla, quién acredita esos aparatos. Y también tiene responsabilidad el Instituto Nacional de la Calidad, obvio.

Ese es mi tema, conozco yo esos temas, y responsabilidad, porque yo aprobé el proyecto de ley, la ley para crear el Instituto Nacional de Calidad. No había ningún congresista que quería sustentarlo. A pesar que yo era oposición, vinieron del ministerio a decir que yo lo sustente. Y le faltaba una cosa: "oye, pero se han olvidado de la competencia laboral también, la calidad laboral". Incluimos ese tema. Le puse esa condición, incluye eso para futuro, porque si yo me acredito acá como un buen soldador, cuando voy a Chile no me reconocen pues, cuando voy a Estados Unidos no me reconocen, voy a Colombia no me reconocen, en Ecuador no reconocen mi profesión, porque no tenemos convenios, no estamos homologados

Yo llevé esa maestría en Europa y cuando vine acá, fui a Indecopi, no había el convenio con Indecopi como para homologar ese tema. ¿Me dejo entender? O sea, eso contribuye a la productividad, a la competitividad, a las relaciones.

Hay mucho por hacer. Por eso digo, está bien, esto es importantísimo, pero la pelota está en su cancha pues.

Bueno, gracias. Creo que no hay más.

Para cerrar esto, agradecemos la participación de los funcionarios de la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros, del Ministerio de Justicia y Derechos humanos, y del Indecopi.

59

Se les invita a retirarse en el momento que lo crean conveniente.

Reitero mi agradecimiento porque esto ha quedado registrado, vamos a difundirlo, nosotros lo difundimos a los gremios, pasamos este dialogo.

No habiendo más puntos a tratar de la agenda, se consulta la dispensa... Bueno, en este caso como es informativa.

Siendo las once con treinta y siete minutos, se levanta la sesión.

Muchas gracias, señores.

-A las 11:37 h, se levanta la sesión.



GRUPO DE TRABAJO

ENCARGADO DE ELABORAR LOS INFORMES DEL

DECRETO DE URGENCIA 006-2020, DECRETO DE URGENCIA QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL

DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

ACTA DE LA SESIÓN DE INSTALACIÓN

Lima, 22 de enero de 2020

Acuerdos tomados por unanimidad:

- Invitar a los funcionarios de la Presidencia del Consejo de Ministros (Secretaría de Gobierno Digital), del Ministerio de Justicia y Derechos Humanos; e, INDECOPI, para que informen respecto a los Decretos de Urgencia 006-2020 y 007-2020.
- Dispensar el trámite de aprobación del Acta de la Sesión de Instalación para la ejecución de los acuerdos.

Siendo las once horas y cincuenta y ocho minutos del miércoles 22 de enero de 2020; en la Sala "María Elena Moyano", Palacio Legislativo, del Congreso de la República, el congresista **Ángel Neyra Olaychea** (FP), en su condición de **Coordinador** del Grupo de Trabajo encargado de elaborar los informes sobre el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, dio inicio a la Sesión de Instalación, con el quórum correspondiente. Constando con la presencia del congresista **Marvin Palma Mendoza** (C21).

El congresista **Ángel Neyra Olaychea** (FP) manifestó que, en la sesión de la Comisión Permanente, de fecha 16 de enero de 2020, se le designó como **Coordinador** del Grupo de Trabajo encargado de elaborar los informes sobre los Decreto de Urgencia 006-2020 y 007-2020; y, como único integrante al señor congresista **Marvin Palma Mendoza** (C21), decisión que se le había comunicado con el Oficio N° 198-2019-2020-ADP-CP/CR. Seguidamente, el **Coordinador** declaró instalada el presente Grupo de Trabajo de la Comisión Permanente.

En esta estación en congresista **Coordinador** planteó que, para el Decreto de Urgencia 006-2020, se convoque a la siguiente sesión a los funcionarios que designe la Presidencia del Consejo de Ministros, especialmente a los funcionarios de la Secretaría de Gobierno Digital, y a quien designe la ministra de Justicia y Derechos Humanos; a efectos de que informen respecto al Decreto de Urgencia 006-2020.

Por otro lado, planteó, para el Decreto de Urgencia 007-2020, se convoque a los funcionarios que designe la Presidencia del Consejo de Ministros, de la Secretaría de Gobierno Digital; a quien designe la ministra de Justicia y Derechos Humanos; y, a quien designe la presidencia del Consejo Directivo de INDECOPI, para que informen respecto al Decreto de Urgencia 007-2020.

No habiendo intervenciones, el congresista **Coordinador** sometió al voto la propuesta planteada, siendo aprobado por **UNANIMIDAD**.

Finalmente, no habiendo otro tema a tratar, el congresista **Coordinador** consultó la dispensa del trámite de aprobación del Acta de la Sesión de Instalación, a fin de tramitar los acuerdos adoptados, siendo aprobado por **UNANIMIDAD**, dando por concluida la sesión a las doce horas con un minuto del miércoles 22 de enero de 2020.

Se deja constancia que la transcripción de la versión grabada de esta sesión, elaborada por el Área de Transcripciones y el audio registrado por el Área de Grabaciones en Audio y Video del Congreso de la República forman parte integrante de la presente acta, prevaleciendo lo expresado según el audio.



Ing. **ÁNGEL NEYRA OLAYCHEA**
Congresista de la República
COORDINADOR
Grupo de Trabajo que examina
Decretos de Urgencia 006-2020 y 007-2020

GRUPO DE TRABAJO

DECRETO DE URGENCIA 006-2020, DECRETO DE URGENCIA QUE CREA
EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL

DECRETO DE URGENCIA 007-2020, DECRETO DE URGENCIA QUE
APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS
PARA SU FORTALECIMIENTO

Asistencia de la Sesión de Instalación

Lima, miércoles 22 de enero de 2020,
Sala María Elena Moyano
Palacio Legislativo

INTEGRANTES	
	NEYRA OLAYCHEA ÁNGEL COORDINADOR Fuerza Popular
	PALMA MENDOZA JOSÉ MARVIN Cambio 21

CONGRESO DE LA REPÚBLICA
Es copia fiel del original

7 FEB 2020

HUGO CORTEZ TORRES
Fedatario

63

**CONGRESO DE LA REPÚBLICA
PERÍODO LEGISLATIVO 2019-2020**

**COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA
GRUPO DE TRABAJO ENCARGADO DE ELABORAR EL INFORME SOBRE EL
DECRETO DE URGENCIA 006-2020, QUE CREA EL SISTEMA DE
TRANSFORMACIÓN DIGITAL Y GRUPO DE TRABAJO DEL DECRETO DE
URGENCIA 007-2020, QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y
DISPONE MEDIDAS PARA SU FORTALECIMIENTO**

Instalación

**MIÉRCOLES, 22 DE ENERO DE 2020
COORDINADOR EL SEÑOR ÁNGEL NEYRA OLAYCHEA**

—A las 11:58 h, se inicia la sesión.

El señor COORDINADOR.— Muy buenas tardes, congresista José Marvin Palma y el equipo de asesores, perdón, muy buenos días, siendo las 11 y 58 minutos del miércoles 22 de enero de 2020, en la Sala María Elena Moyano, del Palacio Legislativo del Congreso de la República, con la presencia del congresista Marvin Palma Mendoza.

Contando con el *quorum* reglamentario, ya que este grupo está constituido por ambos congresistas, y el que habla, se da inicio a la sesión de Instalación del Grupo de Trabajo encargado de elaborar los informes de Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital y del Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital, dispone medidas para su fortalecimiento.

Como es de conocimiento en la sesión de la Comisión Permanente, con fecha 16 de enero de 2020, se me designó como congresista Coordinador para la elaboración del informe correspondiente de los decretos de urgencia 006-2020 y 007-2020, decisión que se me comunica con el Oficio 198-2019-2020-ADPCP/CR.

Asimismo, se designó como único integrante del grupo de trabajo al congresista Marvin Palma Mendoza.

Por lo tanto, con el *quorum* correspondiente doy por instalado el presente Grupo de Trabajo de la Comisión Permanente.

¿Congresista Palma, desea hacer alguna intervención?, no.

No habiendo intervención en esta instalación, por otro lado, en el decreto de urgencia se sugiere invitar también para el Decreto de Urgencia 007 a los funcionarios que designe el Presidente del Consejo de Ministros, y también para el Decreto de Urgencia

64

006, a quien designe la ministra de Justicia y de Derechos Humanos, y a quien designe Indecopi en informe respecto al Decreto de Urgencia 007. Es decir, que con la presencia de altos funcionarios técnicos para poder recabar los insumos que se requiere para concluir con un informe que será elevado a la Comisión Permanente.

Se sugiere alguna intervención o sometemos la votación respecto de los invitados que vamos a realizar, ¿estamos de acuerdo? Por unanimidad se aprueba.

Entonces, se sugiere convocar la próxima sesión, informaremos al congresista las coordinaciones que tengamos con los coordinadores de las respectivas instituciones invitadas.

No habiendo otro tema a tratar, consulto la dispensa del trámite del acto de instalación, a fin de ejecutar los acuerdos adoptados.

Sometemos a votación. Los que estemos de acuerdo. Aprobado por unanimidad.

Agradeciendo la participación del congresista Marvin Palma, se da por concluido la sesión, siendo las 11 con 01 minuto.

Muchas gracias.

—A las 11:01 h, se levanta la sesión.

GRUPO DE TRABAJO DE EVALUACIÓN DEL DU 006-2020, QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL Y DEL DU 007-2020, QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO.

OFICIO N° 006-2020-GT.DU.006-2020:007-2020/CR

Lima, 7 de febrero de 2020

Señor Congresista

JOSÉ MARVIN PALMA MENDOZA

Miembro del Grupo de Trabajo que examina el DU-006-2020 / DU-007-2020

Presente.-



Es grato dirigirme a usted para saludarlo cordialmente y al mismo tiempo por especial encargo del **Congresista Ing. Ángel Neyra Olaychea**, invitarlo a la Primera Sesión del Grupo de Trabajo encargado de examinar el *Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital*; y, el *Decreto de Urgencia 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento*.

La sesión se realizará el lunes 10 de febrero del año en curso a las 15:00 horas en la Sala María Elena Moyano, ubicada en el sótano del Palacio Legislativo, Congreso de la República. Se adjunta la agenda respectiva.

Hago propicia la oportunidad para renovarle las expresiones de mi consideración.

Atentamente,



EDWIN RUÍZ MONDRAGON
ASESOR

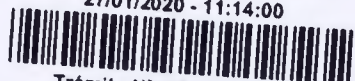
Despacho Congresista de la República y
COORDINADOR
Grupo de Trabajo DU 006-2020 y DU 007-2020

68



INDECOPI - MESA DE PARTES

27/01/2020 - 11:14:00



Trámite N°: 0018897-2020

Nota: La recepción no da conformidad al contenido.

ORDENADO DE EXAMINAR EL DECRETO DE URGENCIA 006-2020, QUE CREA TRANSFORMACIÓN DIGITAL; Y, EL DECRETO DE URGENCIA 007-2020, QUE DISPONE DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU

Lima, 23 de enero de 2020

OFICIO N° 004-2020-GT.DU.006-2020:007-2020/CR

Señor:

IVO SERGIO GAGLIUFFI PIERCECHI

Presidente del Consejo Directivo del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

Calle de la Prosa 104

San Borja.-

Asunto: Invitación a sesión del Grupo de Trabajo encargado de elaborar el informe de los Decreto de Urgencia 007-2020.

Referencia: Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.

Es grato dirigirme a usted a fin saludarle cordialmente y, a la vez, invitar a través suyo a la **Alta Dirección de Indecopi** a participar de la sesión del Grupo de Trabajo encargado de examinar el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, para que sustente las razones que motivaron la dación de los decretos de urgencia bajo análisis en el interregno parlamentario, detallando su necesidad, urgencia y justificación, que hacen referencia en la exposición de motivos del **Oficio N° 007-2020-PR**, de la Presidencia de la República, de fecha 9 de enero de 2020.

La presente se realiza en virtud del Acuerdo aprobado por unanimidad de los congresistas integrantes del Grupo de Trabajo en la sesión celebrada con fecha 22 de enero de 2020. En ese sentido, comunico a usted que dicha sustentación se realizará el **jueves 30 de enero de 2020 a las 10:30 horas**, en la Sala María Elena Moyano, del Palacio Legislativo, Congreso de la República.

Agradeciendo la atención que brinde a la presente, me despido.

Atentamente,



Ing. ANGEL NEYRA OLAYCHEA

Congresista de la República

Coordinador

Grupo de Trabajo que examina

Decreto de Urgencia N°006 y 007-2020

A V/phc

CONGRESO DE LA REPÚBLICA
Es copia fiel del original

17 FEB 2020

HUGO CORTEZ TORRES
Fedatario

2020 ENE 24 P 1:01

CONGRESO DE LA REPÚBLICA
MESA DE PARTES
RECIBIDO

Lima, 23 de enero de 2020

OFICIO N° 003-2020-GT.DU.006-2020:007-2020/CR

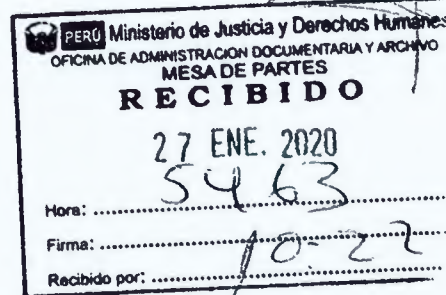
Señora:

ANA TERESA REVILLA VERGARA

Ministra de Justicia y Derechos Humanos

Jr. Scipión Llona 350, Miraflores

Presente.-



Asunto: Invitación a sesión del Grupo de Trabajo encargado de elaborar el informe de los Decretos de Urgencia 006-2020 y 007-2020.

Referencia: Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.

Es grato dirigirme a usted a fin saludarle cordialmente y, a la vez, invitar a través suyo a la **Alta Dirección de su sector** a participar de la sesión del Grupo de Trabajo encargado de examinar el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, para que sustente las razones que motivaron la dación de los decretos de urgencia bajo análisis en el interregno parlamentario, detallando su necesidad, urgencia y justificación, que hacen referencia en la exposición de motivos del **Oficio N° 006-2020-PR** y **Oficio N° 007-2020-PR**, de la Presidencia de la República, ambos de fechas 9 de enero de 2020.

La presente se realiza en virtud del Acuerdo aprobado por unanimidad de los congresistas integrantes del Grupo de Trabajo en la sesión celebrada con fecha 22 de enero de 2020. En ese sentido, comunico a usted que dicha sustentación se realizará el **jueves 30 de enero de 2020 a las 10:30 horas**, en la Sala María Elena Moyano, del Palacio Legislativo, Congreso de la República.

Agradeciendo la atención que brinde a la presente, me despido.

Atentamente,



Ing. ANGEL NEYRA OLAYCHEA
Congresista de la República
Coordinador
Grupo de Trabajo que examina
Decreto de Urgencia N°006 y 007-2020

2020 ENE 24 P 1:01

CONGRESO DE LA REPÚBLICA
MESA DE PARTES
RECIBIDO

CONGRESO DE LA REPÚBLICA
Es copia fiel del original

17 FEB 2020

HUGO CORTEZ TORRES
Fedatario

Lima, 23 de enero de 2020

OFICIO N° 002-2020-GT.DU.006-2020:007-2020/CR

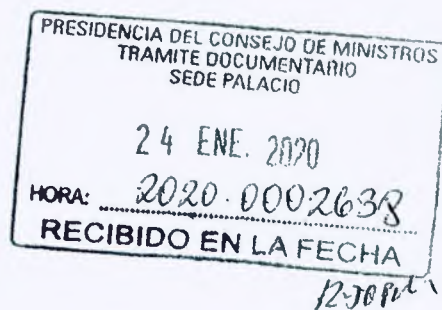
Señor:

VICENTE ANTONIO ZEBALLOS SALINAS

Presidente del Consejo de Ministros

Jr. Carabaya S/N Cuadra 1

Cercado de Lima.-



Asunto: Invitación a sesión del Grupo de Trabajo encargado de examinar el informe de los Decretos de Urgencia 006-2020 y 007-2020.

Referencia: Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento.

Es grato dirigirme a usted a fin saludarle cordialmente y, a la vez, invitar a través suyo a la **Secretaría de Gobierno Digital** a participar de la sesión del Grupo de Trabajo encargado de examinar el Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital; y, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone de medidas para su fortalecimiento, para que sustente las razones que motivaron la dación de los decretos de urgencia bajo análisis en el interregno parlamentario, detallando su necesidad, urgencia y justificación, que hacen referencia en la exposición de motivos del **Oficio N° 006-2020-PR** y **Oficio N° 007-2020-PR**, de la Presidencia de la República, ambos de fechas 9 de enero de 2020.

La presente se realiza en virtud del Acuerdo aprobado por unanimidad de los congresistas integrantes del Grupo de Trabajo en la sesión celebrada con fecha 22 de enero de 2020. En ese sentido, comunico a usted que dicha sustentación se realizará el **jueves 30 de enero de 2020 a las 10:30 horas**, en la Sala María Elena Moyano, del Palacio Legislativo, Congreso de la República.

Agradeciendo la atención que brinde a la presente, me despido.

Atentamente,



Ing. ANGEL NEYRA OLAYCHEA

Congresista de la República

Coordinador

Grupo de Trabajo que examina

Decreto de Urgencia N°006 y 007-2020

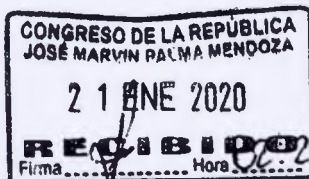
69

AN/phc

CONGRESO DE LA REPÚBLICA
Es copia fiel del original

17 FEB 2020

HUGO CORTEZ TORRES
Fedatario



GRUPO DE TRABAJO DE EVALUACIÓN DEL DU 006-2020, QUE CREA EL SISTEMA NACIONAL DE TRANSFORMACIÓN DIGITAL Y DEL DU 007-2020, QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO.

CARGO

OFICIO N° 001-2020-GT.DU.006-2020:007-2020/CR

Lima, 20 de enero de 2020

Señor Congresista:

JOSÉ MARVIN PALMA MENDOZA

Miembro del Grupo de Trabajo que examina el DU-006-2020 / DU-007-2020

Presente.-

REFERENCIA: Oficio N° 198-2019-2020-ADP-CP/CR.

Es grato dirigirme a usted para saludarlo cordialmente y citarlo a la Sesión de Instalación del Grupo de Trabajo encargado de examinar el *Decreto de Urgencia 006-2020, que crea el Sistema Nacional de Transformación Digital*; y, el *Decreto de Urgencia 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento*.

La sesión se realizará el día miércoles 22 de enero del año en curso a las 10:30 horas en la Sala Mará Elena Moyano, ubicada en el sótano del Palacio Legislativo, Congreso de la República.

Hago propicia la oportunidad para renovarle las expresiones de mi consideración.

Atentamente,



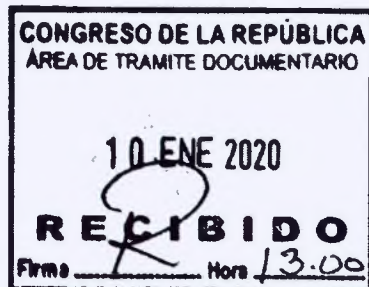
Ing. ANGEL NEYRA OLAYCHEA
Congresista de la República
COORDINADOR

Grupo de Trabajo DU 006-2020 y DU 007-2020

CONGRESO DE LA REPÚBLICA
Es copia fiel del original

17 FEB 2020

HUGO CORTEZ TORRES
Fedatario



"Decenio de la Igualdad de oportunidades para mujeres y hombres"

Lima, 9 de enero de 2020

OFICIO N° 007 -2020 -PR

Señor

PEDRO CARLOS OLAECHEA ÁLVAREZ-CALDERÓN

Presidente de la Comisión Permanente

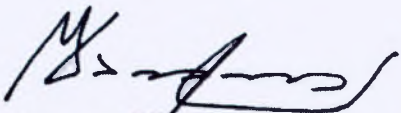
Congreso de la República

Presente. -

De acuerdo con lo dispuesto por el artículo 135° de la Constitución Política del Perú, nos dirigimos a usted señor Presidente de la Comisión Permanente, con el objeto de dar cuenta de la promulgación del Decreto de Urgencia N° 007 -2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, para que lo examine y lo eleve al Congreso, una vez que éste se instale.

Sin otro particular, hacemos propicia la oportunidad para renovarle los sentimientos de nuestra consideración.

Atentamente,

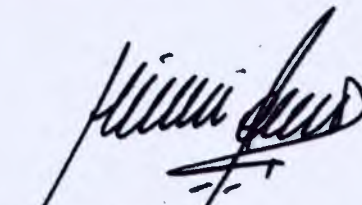

MARTIN ALBERTO VIZCARRA CORNEJO
Presidente de la República


VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

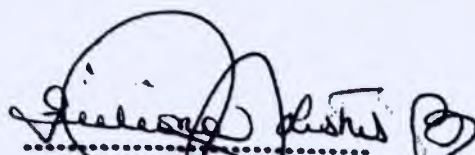
COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA

Lima, 13 de ENERO de 2020

De conformidad con el segundo párrafo del artículo 136° de la Constitución Política del Perú, pase el Decreto de Urgencia N° 007 a la Comisión Permanente.


GIOVANNI FORNO FLÓREZ
 Oficial Mayor
 CONGRESO DE LA REPÚBLICA

DEPARTAMENTO DE RELATORÍA, ASSESORÍA Y ACTAS	URGENTE ☐	IMPORTANTE ☐
Área de Despacho Parlamentario ☐	Atender ☐	Agregar a sus Antecedentes ☐
Área de Redacción de Actas ☐	Tramitar ☐	Junta de Portavoces ☐
Área de Relatoría y Agenda ☒	Conocimiento y Fines ☐	Consejo Directivo ☐
Área de Trámite Documentario ☐	Elaborar Informe ☐	Comisión Permanente ☒
	Conformidad VU* ☐	Licencia ☐
	Otros:	


GIULIANA LASTRES BLANCO
 Jefe del Departamento de Relatoría, Agenda y Actas
 CONGRESO DE LA REPÚBLICA

COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA

Lima, 15 de enero de 2020

En sesión de la fecha, la Presidencia dio cuenta de los siguientes decretos de urgencia remitidos por el Poder Ejecutivo.-----

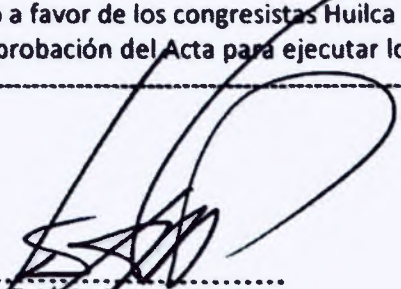
Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, presentado mediante el Oficio 006-2020-PR, recibido el 10 de enero de 2020.-----

Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, presentado mediante el Oficio 007-2020-PR, recibido el 10 de enero de 2020.-----

Seguidamente, la Presidencia propuso como coordinador al congresista Neyra Olaychea para la elaboración del informe sobre los **Decretos de Urgencia 006 y 007-2020** con el congresista Palma Mendoza.-----

Efectuada la votación nominal, se aprobó por 14 votos a favor, ningún voto en contra y ninguna abstención la designación del congresista Neyra Olaychea como coordinador para la elaboración del informe de los **Decretos de Urgencia 006 y 007-2020**, con el congresista Palma Mendoza quienes recibirán la asesoría técnica legal del Departamento de Comisiones.-----

La Presidencia dejó constancia del voto a favor de los congresistas Huilca Flores y Arana Zegarra.---
Se acordó la dispensa del trámite de aprobación del Acta para ejecutar lo acordado en la presente sesión.-----



JAIME ABENSUR PINASCO
Director General Parlamentario
CONGRESO DE LA REPÚBLICA

27

3



COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

Decreto de Urgencia

N° 007 -2020

DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia de los que da cuenta a la Comisión Permanente para que los examine y los eleve al Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo N° 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, mediante Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece 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;

Que, 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 afectan la seguridad de las personas y la prosperidad económica y social en dicho entorno;

Que, mediante Decreto Supremo N° 237-2019-EF, se aprueba el Plan Nacional de Competitividad y Productividad, el cual presenta un conjunto de medidas consensuadas entre el sector público y privado con miras a establecer un entorno



74

favorable y competitivo que permita generar bienestar para todos los peruanos sobre la base de un crecimiento económico sostenible con enfoque territorial;

Que, del precitado Plan Nacional se entiende que las tecnologías digitales tienen un valor estratégico para reducir brechas, impulsar la innovación y apoyar en el crecimiento del país; más aún, señala que los cambios tecnológicos por los cuales atraviesa el mundo actual serían mucho más fáciles de adoptar si es que realizamos una transformación digital a lo largo del país;

Que, mediante Decreto Supremo N° 086-2015-PCM se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) e implementación del Programa País, en esa línea, cobra relevancia las Recomendaciones para la Gestión de Riesgos de Seguridad Digital realizadas por la OCDE, entre las cuales se señala la importancia del establecimiento de Equipos de Respuestas a Incidentes de Seguridad Digital a nivel de los Estados;

Que, en el documento Gobierno Digital en el Perú "Trabajando con los ciudadanos" la OCDE señala como recomendación que el Estado Peruano debe "considerar establecer un Centro Nacional de Seguridad Digital" que busque articular acciones con los actores relevantes para gestionar incidentes de seguridad digital y fortalecer la confianza;

Que, la confianza digital es un estado que emerge como resultado de cuan veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital. La confianza digital es un componente de la Transformación Digital y tiene como ámbitos la protección de datos, transparencia, seguridad digital y protección del consumidor en el entorno digital;

Que, ante ello como parte de nuestro proceso de vinculación, resulta necesario dictar medidas en materia de confianza y seguridad digital, estableciendo los mecanismos de colaboración y articulación con actores públicos, privados y sociedad civil en el entorno digital, a través de un enfoque sistémico e integral que asegure el fortalecimiento de la confianza en los servicios digitales por las personas, entidades y sociedad en general;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta a la Comisión Permanente para que lo examine y lo eleve al Congreso, una vez que éste se instale:

DECRETA:

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Decreto de Urgencia tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.



75



COPIA DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE VISTOS

Decreto de Urgencia

Artículo 2. Alcance

Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia.

Artículo 3. Definiciones

Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:

- a) **Confianza Digital.**- Es 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.
- b) **Economía digital.**- Es la innovación y la transformación de la economía basada en el uso estratégico y disruptivo de las tecnologías digitales. Desarrolla la capacidad de incrementar la eficiencia, productividad, transparencia, seguridad y eficacia de los procesos y actividades económicas y sociales, sustentada en el uso intensivo de tecnologías digitales, redes de datos o comunicación y plataformas digitales. Conlleva a la generación de beneficios económicos y sociales, prosperidad y bienestar para la sociedad.
- c) **Entorno Digital.**- Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes e infraestructuras de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, plataformas que sirven como base para la interacción entre personas, empresas, entidades públicas o dispositivos.
- d) **Actividad crítica.**- Es la actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, en el funcionamiento efectivo de los servicios esenciales que mantienen la economía, sociedad y el gobierno, o afectan la prosperidad económica y social en general.
- e) **Incidente de seguridad digital.**- Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.
- f) **Gestión de incidentes de seguridad digital.**- Proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.



74

- g) **Riesgo de seguridad digital.**- Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.
- h) **Ciberseguridad.**- Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.
- i) **Servicio digital.**- Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo, al menos una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.
- j) **Proveedor de servicios digitales.**- Comprende a cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional.

CAPÍTULO II MARCO DE CONFIANZA DIGITAL

Artículo 4. Marco de Confianza Digital

4.1 El Marco de Confianza Digital se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital.

4.2 El Marco de Confianza Digital tiene los siguientes ámbitos:

- a) **Protección de datos personales y transparencia.**- El Ministerio de Justicia y Derechos Humanos (MINJUSDH), quien ejerce las autoridades nacionales de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.
- b) **Protección del consumidor.**- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.
- c) **Seguridad Digital.**- La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de seguridad digital en el país, norma, dirige, supervisa y evalúa la materia de seguridad digital.



72



Decreto de Urgencia

Artículo 5. Ente rector del Marco de Confianza Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos.

Artículo 6. Atribuciones del Ente rector

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la Confianza Digital, tiene las siguientes funciones:

- Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.
- Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.
- Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.
- Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.
- Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.



Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias.

Artículo 7. Centro Nacional de Seguridad Digital

7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

7.2 El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.



24

7.3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional responsable de: i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y, ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital

7.5 La Secretaría de Gobierno Digital establece los protocolos de escalamiento, coordinación, intercambio y activación ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes.

CAPÍTULO III MEDIDAS PARA FORTALECER LA CONFIANZA DIGITAL

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

8.1 Créase el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

8.2 El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad.

8.3 El Centro Nacional de Seguridad Digital brinda información sobre los registros de incidentes de seguridad digital, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, y del Marco de Confianza Digital debiendo observar para tal efecto la normatividad vigente en materia de protección de datos personales.

Artículo 9. Obligaciones del Proveedor de servicios digitales

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

- Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
- Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.
- Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.



9



Decreto de Urgencia

- d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.
- e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.
- f) Mantener una infraestructura segura, escalable e interoperable.

9.2 Las organizaciones privadas toman como referencia las normas emitidas por la Secretaría de Gobierno Digital en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

9.3 Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

9.4 Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Artículo 10. Articulación internacional

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias.

Artículo 11. Articulación en Materia de Comunicaciones

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Transportes y Comunicaciones las acciones vinculadas a la materia de comunicaciones en el marco de sus competencias.

CAPÍTULO IV

USO ÉTICO DE LAS TECNOLOGIAS DIGITALES Y DE LOS DATOS

Artículo 12. Datos como activos estratégicos

12.1 Las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accesen, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad en materia de protección de datos personales, gobierno digital y seguridad digital.



22

12.2 Las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

12.3 El tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

Artículo 13. Centro Nacional de Datos

13.1 Créase el Centro Nacional de Datos como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de datos a nivel nacional, a fin de fortalecer la confianza y bienestar de las personas en el entorno digital en el marco de la presente norma.

13.2 El Centro Nacional de Datos se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

13.3 El Centro Nacional de Datos intercambia información y articula acciones con las entidades públicas, academia, sociedad civil y sector privado y con las entidades responsables de los ámbitos del Marco de Confianza Digital para la gobernanza de datos.

13.4 La Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos, establece los protocolos y mecanismos en materia de gobierno de datos y emite los lineamientos y las directivas correspondientes.

Artículo 14. Financiamiento

La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 15. Refrendo

El presente Decreto de Urgencia es refrendado por el Presidente del Consejo de Ministros y la Ministra de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación

El Poder Ejecutivo, dentro de los noventa (90) días hábiles siguientes a la entrada en vigencia de la presente norma, aprueba su reglamento mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

SEGUNDA. Registro Nacional de Incidentes de Seguridad Digital

En un plazo no mayor a noventa (90) días hábiles, posterior a la publicación del presente Decreto de Urgencia, la Presidencia del Consejo de Ministros implementa el Registro Nacional de Incidentes de Seguridad Digital y dicta normas, lineamientos y directivas para su correcto funcionamiento.





ES COPIA FIEL DEL ORIGINAL
FÉLIX PINO FIGUEROA
SECRETARIO DEL CONSEJO DE MINISTROS

Decreto de Urgencia

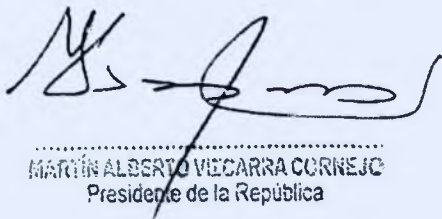
TERCERA. Gestión e Impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE)

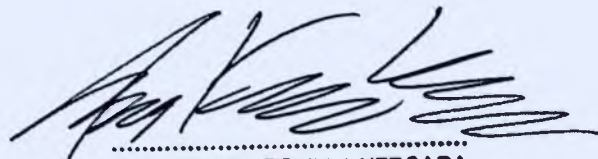
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, se encarga de la gestión e impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE) a las que se refiere la Ley N° 29904 a fin de coadyuvar al logro de las políticas nacionales, el fortalecimiento de una sociedad digital y la transformación digital del Estado. La contratación de los servicios para la conectividad de la REDNACE es realizada por cada entidad de la Administración Pública, de conformidad con lo dispuesto en el artículo 19 de dicha Ley.

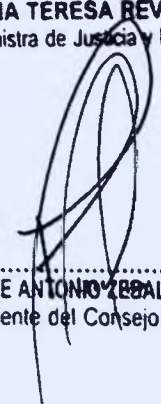
CUARTA. Aplicación de la Norma

La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.


MARTÍN ALBERTO VECARRA CORNEJO
Presidente de la República


ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos


VICENTE ANTONIO ZABALLOS SALINAS
Presidente del Consejo de Ministros

EXPOSICIÓN DE MOTIVOS

DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE LA CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

I. FUNDAMENTO

A. Necesidad y Urgencia

- 1.1 En el Perú se ha tomado la decisión de garantizar la transformación digital del Estado para el logro de los objetivos del país¹ en el marco de la Política General de Gobierno cuyos pilares se centran en integridad y lucha contra la corrupción; fortalecimiento institucional para la gobernabilidad; crecimiento económico equitativo, competitivo y sostenible; desarrollo social y bienestar para la población y descentralización efectiva para el desarrollo. La transformación digital del país es fundamental para el logro de estos objetivos.
- 1.2 De igual manera, el Perú tomó la decisión de adherirse al Convenio de Budapest o Convenio contra la Ciberdelincuencia reconociendo la necesidad de fortalecer la regulación en materia de seguridad digital dado el avance de la digitalización y el crecimiento de los delitos cometidos en Internet. El Convenio de Budapest 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 firmantes². Dicha adhesión establece plazos perentorios para adecuar la regulación digital en torno a los riesgos digitales y fortalecer la confianza digital de los ciudadanos.
- 1.3 Bajo ese objetivo, la necesidad de emitir el presente Decreto de Urgencia durante el interregno se fundamenta en las siguientes razones:
 - a. Durante el 2018 y 2019 el avance de las tecnologías digitales ha sido exponencial. En medio de este avance, se ha verificado el crecimiento de los ciberataques, el robo de datos, los delitos contra niños y adolescentes, suplantación, ingeniería social, entre otros delitos en Internet. Ello ha ocasionado pérdidas económicas tanto en el sector público como en el sector privado y, sobre todo, ha afectado a millones de ciudadanos. Esta situación, que va en franco incremento, nos brinda un pronóstico bastante negativo respecto al cual la normativa resulta insuficiente y revela la necesidad de emitir una norma de rango legal para su resolución.
 - b. El impacto de los ciberataques afecta la credibilidad y confianza en el país, impacta la competitividad, la productividad, las condiciones para hacer negocios en el país, la productividad en las regiones y la seguridad de las personas. De igual manera, los delincuentes comunes utilizan las redes y el Internet para facilitar sus delitos: acosan a sus víctimas por redes sociales, ingresan a cámaras de vigilancia y a cualquier dispositivo de los hogares, hacen seguimiento a las víctimas rastreando maliciosamente. Por ello, existe la urgencia de establecer un marco regulatorio con el fin primario de salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital³, especialmente en materia de intimidad personal, familiar y seguridad, así como también atender el deber constitucional del Estado peruano de proteger a la población de las amenazas contra su seguridad⁴, incluyendo aquellas que provienen por agentes perjudiciales en el referido entorno digital. Si bien, la aprobación de la Ley de Gobierno



¹ Discurso Presidencial del 28 de Julio de 2019: <https://www.gob.pe/institucion/presidencia/mensajes-a-la-nacion>

² https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

³ Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas. Fuente: Decreto Legislativo N° 1412

⁴ Artículo 44 de la Constitución Política del Perú de 1993.

83

Digital constituye un gran paso para este objetivo, el gobierno digital solo implica acciones al interior del Estado, lo cual resulta insuficiente. Revertir esta situación es urgente. Para ello debe garantizarse la articulación público privada y que el Estado emita lineamientos para los servicios y plataformas digitales públicas y privadas que se implementen para lograr estos objetivos.

- c. La Política General de Gobierno tiene metas definidas que deben ser cumplidos antes del 28 de julio de 2021. Es así que la lucha contra la corrupción y la generación de bienestar social; así como la competitividad y productividad tienen un componente La transformación digital es un proceso fundamental para el logro de los objetivos de dicha Política en beneficio de los ciudadanos y empresas. Por ello, la Política General de Gobierno y la adhesión del Perú al Convenio de Budapest se constituyen en un componente normativo que establece metas sobre la materia a ser cumplidas a corto plazo.

Ahora, la confianza digital NO solo tiene como pilar la seguridad digital, sino también la protección de los datos personales y la protección del consumidor en el entorno digital, por ello, considerando que el plazo para el cumplimiento de **la Política General de Gobierno vence el 2021**, se hace urgente establecer mecanismos y normas que permitan luchar contra la corrupción en el entorno digital, robo y venta de datos personales, clonación de tarjetas de identidad, robo por internet, estafa por internet, etc. En esa línea, Perú no dispone de una norma legal de alto nivel (Norma con rango de Ley) que establece un marco de articulación acorde con las necesidades y demandas de la transformación digital y uso de tecnologías digitales, tal cual se viene dando en países desarrollados, Reino Unido, Estados Unidos, Dinamarca, Estonia, así como nuestros vecinos en América Latina (Colombia, Brasil, Uruguay y Chile).

En ese sentido, para revertir el estado de cosas hasta la fecha de vencimiento de la Política de General de Gobierno al 2021, es necesario que a la brevedad se incorporen nuevos estándares a nivel legal. Como puede apreciarse, este escenario debe ser revertido antes del referido plazo, por lo cual es imperioso que se incorporen nuevos estándares a nivel legal que coadyuven en dicha tarea.

Por tal motivo, aguardar hasta la instalación del nuevo Congreso implicaría dejar de contar con tiempo valioso para la aprobación de la ley correspondiente, la realización de las acciones operativas a nivel de las instituciones involucradas en la medida (como emisión de directivas, actos de difusión y capacitación, entre otros), lo cual impediría la aplicación de la norma a la brevedad, manteniendo un estado de cosas que repercuten negativamente sobre un sector de la población en situación de vulnerabilidad. Por el contrario, la aprobación del presente decreto de urgencia permitirá revertir esta situación de manera progresiva, de tal manera que a la fecha de vencimiento de la Política General de Gobierno al 2021 se podrá contar con un marco normativo idóneo para la resolución progresiva del problema y generar un mejor escenario que garantice el fortalecimiento de la confianza digital.

Al respecto, y si bien a través del Decreto Legislativo N° 1412, se aprobó la Ley de Gobierno Digital, que configura un Marco de Seguridad Digital para el Estado Peruano, la estadística que veremos a continuación nos permite apreciar que esta norma no resulta aún del todo eficaz en la prevención y solución de la problemática en esta materia particular, máxime cuando su alcance solo comprende al sector público, lo cual hace necesaria la emisión de una norma que permita un despliegue más efectivo y enfocado en dicho aspecto, en particular para articular no sólo con las entidades públicas sino también con actores privados, academia y sociedad civil, esto es, como país frente a las amenazas que como veremos se ciernen sobre el proceso de transformación digital que nuestro país ha decidido adoptar.



En dicho sentido, se aprecia que la prestación de servicios digitales por parte de entidades públicas y organizaciones privadas en el país ha crecido de manera exponencial en los últimos años, siendo utilizados por miles de personas en sus actividades económicas, sociales, educativas, entre otros; no obstante, con ello también se ha incrementado de manera alarmante los ataques y riesgos digitales que afectan la seguridad, tranquilidad y privacidad de las personas, sin que hasta la fecha se establezcan medidas efectivas para su prevención o atención.

Empero, y a la par de lo antes indicado, durante 2018 y 2019 se verifica el alto nivel de crecimiento de los ciberataques en el país, como también las pérdidas económicas resultado de ciberataques, problemática que se encuentra en escalada.

- **Somos el segundo país con mayor cantidad de variantes de RANSOMWARE, software malicioso que captura el sistema para chantajear.**

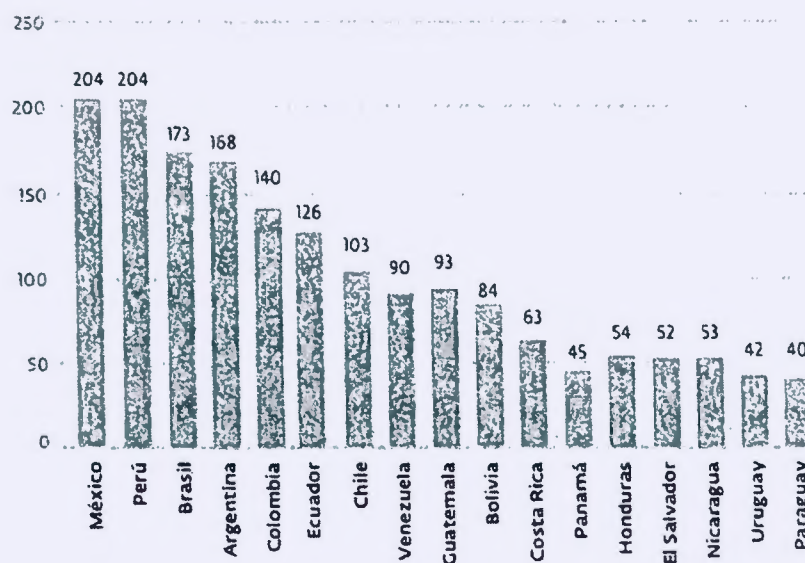


Tabla 1. Cantidad de variantes de Ransomware por país
Fuente: ESET Security Report Latinoamérica 2019

- **Alto nivel de crecimiento de los ciberataques en el país en los últimos 02 años**

ESET Security Report - Latinoamérica 2019

- Según el reporte de ESET Security Report - Latinoamérica 2019⁵ el Perú es el **segundo país de América Latina más afectado por incidentes de seguridad**, 71% de los incidentes en América Latina se concentraron en nuestro país, solo nos supera México con un 72%. Asimismo, es el **segundo país** con mayor presencia de variantes de Ransomware (204).
- Ahora bien, entre los **principales incidentes** reportados por las empresas en América Latina tenemos: El acceso indebido (61%), el robo de información (58%) y la privacidad de la información (48%).

Kaspersky

- De acuerdo con reportes de Kaspersky, los ataques en Perú se han incrementado hasta en un 39%, y las ciber amenazas llegan a 3,7 millones por día solo en Latinoamérica, teniendo como objetivo datos sensibles y dinero. En el caso de nuestro país, la modalidad



⁵ Ver: <https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf>

85

más forzada desde la delincuencia digital es el secuestro de información o ransomware, una modalidad que exige un pago de dinero para liberar los datos o los equipos secuestrados, a cambio de no borrar la información dentro de la PC infectada.

Casos Perú

- Ataque cibernético al sector financiero de alcance mundial que afectó la banca peruana en agosto de 2018, debiendo suspender o limitar algunos servicios financieros como parte de los procedimientos de respuesta a incidentes de seguridad, según lo informado por la Superintendencia de Banca, Seguros y AFP (SBS).
- Incremento en un 600% de los ciberataques según la Asociación de Bancos del Perú (ASBANC)⁶.
- Ataque cibernético al Banco de Crédito del Perú (BCP) en el año 2018, en el cual accedieron a datos de identificación personal de clientes de dicho banco (números de L.
- La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) conforme los casos atendidos viene **evidenciando el incremento de delitos en el entorno digital**, de entre los cuales ha identificado como los más frecuentes: clonación de tarjetas, acoso, espionaje, robo de información a través de páginas falsa, chantaje, extorsión, difamación y estafa a organizaciones del sector público y privado través de internet.

● Bajo nivel de gestión de la seguridad digital

Ahora bien, con respecto a la gestión de la seguridad digital el Perú ocupa el último lugar de los países de América Latina en implementar prácticas de gestión de para la seguridad del país. Solo un 42% de las organizaciones encuestadas afirma disponer de una Política de Seguridad de la Información y, peor aún, solo un 8% de las entidades clasifica la información.

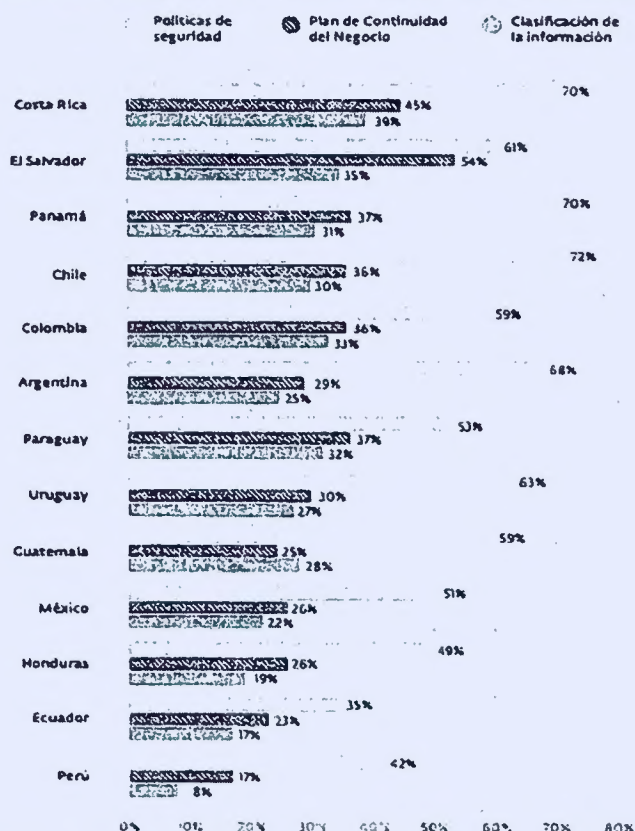


Tabla 1. Perú no implementa prácticas de gestión - Fuente: ESET Security Report Latinoamérica 2019

⁶ Ver: <https://gestion.pe/economia/empresas/ciberataques-empresas-peruanas-aumentaron-600-ultimos-12-meses-242114-noticia/>

Falta de articulación entre actores públicos y privados

De otro lado, una problemática adicional en esta materia es que nuestro país **NO cuenta** con una entidad y marco articulador en materia de confianza digital que permitan coordinar y articular acciones entre entidades públicas y privadas con el fin de gestionar los riesgos e incidentes en el entorno digital que afecte los objetivos, procesos y servicios de dichas organizaciones, tal como se señaló precedentemente el Decreto Legislativo N° 1412 tiene como alcance sólo al sector público, y sus disposiciones sólo alcanzan a las entidades públicas. Cabe señalar que pese a los esfuerzos desplegados por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, aún las acciones para atender los riesgos en el entorno digital son desarticulados, no existe una entidad o mecanismo que centralice los reportes de incidentes de seguridad digital a nivel nacional que permita desarrollar soluciones para su atención.

Actualmente, las organizaciones privadas gestionan sus riesgos e incidentes de manera independiente, de manera desarticulada con el sector público, lo anterior evidencia la falta de articulación para atender este tema complejo (distintos actores con diversas necesidades), puesto que un mismo incidente de seguridad digital puede afectar los activos digitales tanto a entidades públicas y organizaciones privadas, sin distinción.

Ahora, los países más desarrollados a nivel mundial han abordado esta problemática institucionalizando un ente articulador, implementando un centro nacional de seguridad digital, definiendo obligaciones para las entidades públicas y privadas; y, sobre todo, estableciendo un marco de confianza en el que se establezca los responsables en el entorno digital y obligaciones para aquellos que prestan servicios digitales. Dichos países tienen determinado:

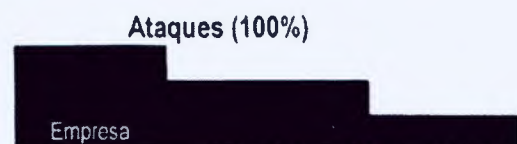
- ¿Quién protege al ciudadano "consumidor" en el entorno digital?
- ¿Quién protege los datos personales de los ciudadanos?
- ¿Quién articula la gestión de un incidente en el entorno digital?
- ¿Cómo se articula acciones con los operadores de justicia?
- ¿Cómo se recopila evidencia digital (correo, mensaje, dato, etc.) que sirva para atender un caso de ciberestafa, ciberespionaje, ciberacoso, etc.?

Lo anterior, exige un abordamiento integral e inmediato, no solo basta con castigar el delito o el mal comportamiento en internet o el mal uso de tecnologías digitales (**Ley de Delitos Informáticos**); sino se debe prevenir y atender articuladamente -empresa y entidad pública-, un incidente a la seguridad digital, ello con miras a evitar pérdidas humanas, financieras y reputacionales. Por lo tanto, resulta urgente establecer un marco de articulación entre entidades públicas y privados, que permita un intercambio de información rápido para desarrollar soluciones integrales que ayuden a todos los actores del ecosistema digital, asimismo, se hace necesario establecer obligaciones mínimas a los proveedores de servicios digitales conforme las buenas prácticas y experiencia internacional.

Pérdidas económicas resultado de ciberataques

La Organización de los Estados Americanos (OEA) ha indicado en el "Estudio de Ciberseguridad en América Latina y el Caribe" alrededor del 37% de los ciberataques que se concretan están dirigidos a bancos y entidades financieras, mientras que el resto va dirigido a personas, proveedores o clientes.

Ataques a entidades financieras (37%)
Ataques a personas o clientes (63%)
Total de ataques (100%)



Ataques ⁷ - Fuente: OEA



⁷ <https://www.asbank.com.pe/Paginas/Noticias/DetalleNoticia.aspx?ItemID=828&lang=es>

Asimismo, en el caso del sector financiero se han identificado alrededor de 18 millones de dólares en pérdidas económicas y aproximadamente 17 millones de dólares de pérdidas económicas en servicios públicos y energía.



Lo anterior, impacta directamente a la competitividad y productividad de nuestras empresas y entidades, **resultando urgente** el establecimiento de un marco de articulación público y privado para hacer frente a esta problemática, países como Colombia, Estonia, Uruguay, Reino Unido y Estados Unidos, han establecido normas con rango de Ley para promover la colaboración entre entidades públicas y privadas, implementar centros de seguridad digital y, sobre todo, mejorar la relación e intercambio de información con las autoridades responsables de proteger los datos personales (privacidad), protección del consumidor en el entorno digital y la seguridad digital en el país.

Deficiencias de la actual regulación

En el caso peruano no disponemos de una norma con rango de ley en materia de confianza digital que establezca disposiciones obligatorias para públicos y privados en dicho ámbito, así como mecanismos de articulación para una gestión preventiva y atención de incidentes digitales; como se ha mencionado el Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital establece un Marco de Seguridad Digital solo alcanza a entidades del sector público, por lo que no resulta del todo eficaz en la prevención y solución de la problemática en esta materia particular, faltando el componente de articulación con el sector privado, sociedad civil y academia para una gestión oportuna de los riesgos e incidentes de seguridad digital, desarrollo de capacidades, entre otros, así como la definición de obligaciones para todos los actores que presten servicios digitales.

Más aún, con la emisión del Decreto de Urgencia se estaría fortaleciendo el accionar de las entidades responsables en materia de protección de datos personales, seguridad digital y protección al consumidor en el entorno digital, a fin de asegurar la confianza del ciudadano en los servicios digitales.

Diferente, es el caso Europeo donde existe un consenso sobre la materia de confianza digital, contando con normas con rango de ley que permiten la adecuada articulación y enfoque integral y sistémico del problema de la desconfianza en el entorno digital. Los países más desarrollados en materia de confianza y seguridad digital han aprobado normas con rango de Ley para atender la compleja problemática sobre los riesgos y confianza en el entorno digital.

1. **Estonia**, tiene Ley de Ciberseguridad⁹
2. **Dinamarca**, tiene un Centro Nacional de Ciberseguridad y una Estrategia¹⁰ para la seguridad de la información y ciberseguridad danesa.

⁸ <https://www.asbanc.com.pe/Paginas/Noticias/DetalleNoticia.aspx?ItemID=828&lang=es>

⁹ Ver: <https://www.rigiteataja.ee/en/eli/523052018003/consolide>

¹⁰ Ver: <https://diqst.dk/media/16943/danish-cyber-and-information-security-strategy-pdfa.pdf>



AB

3. Australia, tiene un Centro Nacional de Ciberseguridad¹¹, una Estrategia Nacional de Ciberseguridad y ha establecido una red de intercambio de información de confianza¹² para atender los incidentes de seguridad digital a actividades e infraestructuras relevantes para las operaciones del país.
4. Chile, Política Nacional de Ciberseguridad¹³.
5. Colombia, Política de Confianza y Seguridad digital¹⁴.

De otro lado, el Estado Peruano mediante el **Decreto Supremo N° 086-2015-PCM**, declaró de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la OCDE e implementación del Programa País y crea la Comisión Multisectorial de naturaleza permanente para promover las acciones de seguimiento del referido proceso. En línea con ello, mediante el **Decreto Supremo N° 118-2018-PCM**, se declaró de interés nacional el desarrollo del **Gobierno Digital, la innovación y la economía digital** con enfoque territorial, lo cual se sustenta en las recomendaciones de la OCDE en materia de Gobierno Digital contenidas en el Estudio de Gobernanza Perú (OCDE, 2016)¹⁵.

El año 2015, la OCDE emite el documento "Recomendaciones sobre **gestión de riesgos de seguridad digital** para la prosperidad económica y social", en el cual busca ser una guía en la **formulación de estrategias integrales y sistémicas para abordar los riesgos en el entorno digital desde un alto nivel**. Conforme lo anterior, el Estado Peruano ha optado por abordar los riesgos, delitos, actos ilícitos, operaciones militares en el entorno digital mediante un marco integral, holístico y sistémico, definido en la Ley de Gobierno Digital como Marco de Seguridad Digital del Estado, dentro del cual ya comprende a la **ciberseguridad** como una capacidad que refleja la **perspectiva técnica de la Seguridad Digital**. Así, en la propuesta de DU se establece una definición de ciberseguridad y su articulación con el Marco de Seguridad Digital del Estado peruano. Sobre el Consejo de Seguridad y Defensa Nacional, señalar que el **artículo 13 de la Ley N° 30999, Ley de Ciberdefensa**, señala que la PCM, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, a través de la **Secretaría de Gobierno Digital**, establece los **protocolos de escalamiento** para atender los incidentes de seguridad digital.

No obstante, a lo indicado precedentemente, se tiene la necesidad de fortalecer y asegurar mecanismos de articulación en materia de política exterior que contribuyan en la confianza en el entorno digital, para lo cual se debe prever articular acciones con el Ministerio de Relaciones Exteriores a fin de atender dicha necesidad.

Asimismo, en el caso del Perú, la norma propuesta incorpora como factor clave, el uso ético de las tecnologías digitales como la inteligencia artificial, bigdata entre otros, a fin de proteger al ciudadano en todas las perspectivas. Cabe indicar que el uso ético de datos y tecnologías digitales se introduce con miras a generar un marco tal como lo tiene Reino Unido¹⁶ y Australia, países desarrollados en materia de servicios digitales, así como también siguiendo las recomendaciones de la OCDE para un uso ético de los mismos, puesto que se debe fortalecer que la ética debe estar presente en todo el ciclo de vida del dato: captación, gestión, privacidad y uso, así como en el uso de la tecnología para el bienestar de la población. Este esfuerzo debe ser articulado con la Autoridad Nacional de Protección de Datos Personales.



¹¹ Ver: <https://www.cyber.gov.au/>

¹² Ver: <https://www.jisn.gov.au/Pages/default.aspx>

¹³ Ver: <https://www.ciberseguridad.gob.cl/media/2017/05/PNGS-CHILE-FEA.pdf>

¹⁴ Ver: <https://estrategia.gobiernonlinea.gov.co/623w3-articulo-106311.html>

¹⁵ Ver: <http://bit.ly/2SCyK7c>

¹⁶ Por ejemplo el Data Ethics Framework del Reino Unido se crea dentro de la unidad de servicios digitales - <http://bit.ly/364YGmv>.

89

Como parte de los Principios recomendados por la OCDE en materia de adopción de Inteligencia Artificial en sus economías miembro, se ha identificado que existe una preocupación por el uso ético de tecnologías digitales y datos al momento de diseñar servicios y políticas. En esa línea, se ha indicado que le compete, a cada país miembro, asegurarse de que el diseño de los sistemas de Inteligencia Artificial respete nuestros valores y leyes, de forma que las personas puedan confiar en que su seguridad y privacidad serán objeto de una consideración prioritaria. Estos principios, se constituyen en un referente global para una IA confiable, de modo que las oportunidades que brinda redunden en los mejores resultados para todos. <http://bit.ly/2MDFZhL>

Adicionalmente a lo anterior, el presente decreto de urgencia debe de cumplir con requisitos formales, tanto previos como posteriores a su promulgación. Así, el requisito ex ante está constituido por el refrendo del Presidente del Consejo de Ministros (inciso 3 del artículo 123 de la Constitución Política del Perú), mientras que el requisito ex post lo constituye la obligación del Ejecutivo de dar cuenta a la Comisión Permanente par que lo examine y lo eleve al Congreso una vez que este se instale, de acuerdo a lo señalado en el artículo 135 de la Constitución. En ese sentido, la presente norma cuenta con la rúbrica del Presidente de la República y el refrendo del Presidente del Consejo de Ministros, la Ministra de Justicia y Derechos Humanos y la Ministra de Economía y Finanzas, de acuerdo a lo señalado en el Decreto de Urgencia.

De otro lado, debe tenerse presente que la norma constituye un decreto de urgencia, cuyo origen se encuentra en la aplicación de los artículos 134 y 135 de la Constitución Política del Perú, encontrándose habilitado el Poder Ejecutivo para legislar mediante decretos de urgencia durante el interregno. Así, durante este periodo del interregno el Poder Ejecutivo se encuentra habilitado para emitir decretos de urgencia que no se encuentren limitados únicamente sobre temas económicos y financieros, lo contrario llevaría a sostener que durante el interregno y ante la inexistencia de un órgano legislativo, el Poder Ejecutivo se encuentra impedido de regular situaciones de atención urgente que no correspondan únicamente a estas materias. Como resulta claro, esto último no puede resultar amparable en un Estado de Derecho ya que pondría en grave riesgo el goce de derechos fundamentales y objetivos y deberes constitucionales, como lo que se buscan a través de la presente norma.

Así las cosas, la propuesta de Decreto de Urgencia también responde al cumplimiento de políticas y planes de cara al 2021:

- **Política de General de Gobierno 2021**

Mediante Decreto Supremo N° 056-2018-PCM, se aprueba la **Política General de Gobierno al 2021**, la cual establece en como uno de sus lineamientos la "Lucha contra la corrupción", en esa línea, disponer de un marco de confianza digital que articule el actuar de las entidades públicas y empresa, aboga a que los ciudadanos identifiquen una respuesta integral frente a este problema toda vez que serán estos actores que intercambiarán información digital de manera inmediata para atender un incidente que impacte la seguridad de las personas y empresas.

Ahora, la confianza digital **NO solo tiene como pilar la seguridad digital**, sino también la protección de los datos personales y la protección del consumidor en el entorno digital, por ello, considerando que el plazo para el cumplimiento de la Política General de Gobierno vence el 2021, se hace urgente establecer mecanismos y normas que permitan luchar contra la corrupción en el entorno digital, robo y venta de datos personales, clonación de tarjetas de identidad, robo por internet, estafa por internet, etc. En esa línea, Perú no dispone de una norma legal de alto nivel (Norma con rango de Ley) que establece un marco de articulación



ap

acorde con las necesidades y demandas de la transformación digital y uso de tecnologías digitales, tal cual se viene dando en países desarrollados, Reino Unido, Estados Unidos, Dinamarca, Estonia, así como nuestros vecinos en América Latina (Colombia, Brasil, Uruguay y Chile).

El Decreto de Urgencia cuenta con un plazo de reglamentación de noventa (90) días hábiles, asimismo, se han considerado las siguientes actividades a realizar con anterioridad a la instalación del nuevo congreso:

ID	ACCIÓN URGENTE	2020					
		ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
1	Formular el Reglamento del DU de Confianza Digital						
2	Implementar el Registro Nacional de Incidentes de Seguridad Digital						
3	Implementar el Centro Nacional de Seguridad Digital						
4	Implementar el Centro Nacional de Datos						
5	Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital						
6	Adecuación de normas para implementación Convenio de Budapest						
7	Articular estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento						
8	Plan de difusión en materia de Confianza Digital						

● **Convenio de Ciberdelincuencia**

El Perú ratificó, mediante Decreto Supremo N° 010-2019-RE, su adhesión al "Convenio de Ciberdelincuencia", también conocido como Convenio de Budapest; suscrito el 23 de noviembre de 2001, por el Consejo de Ministros de Europa, compuesto por Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con Estados Unidos de Norteamérica, Sudáfrica, Canadá y Japón, al cual se han adherido diversos países a la fecha. Entre los objetivos de este Convenio se encuentran:

- Armonizar leyes penales sustantivas aplicables a las conductas delictivas con entorno informático.
- Proveer reglas de procedimiento, normas procesales, persecución del delito y rastreo
- Establecer un régimen de cooperación internacional, esto es, la colaboración entre Estados para perseguir los delitos informáticos.

Se observa que, entre las consideraciones más relevantes del Convenio de Ciberdelincuencia, se establece como cuestión prioritaria la política penal común respecto de la protección de la sociedad contra los delitos informáticos, aprobando legislación apropiada y fomento de la cooperación internacional. El Convenio no sólo establece lineamientos en cuestión de un país en particular, sino en función de una normativa con miras a establecer el carácter globalizado para combatir el ciberdelito. Entre otros, establece la preocupación de los Estados suscriptores



ante el riesgo que las redes informáticas y la información electrónica puedan también, ser utilizadas para cometer delitos y que las pruebas relacionadas con dichos delitos puedan ser almacenadas y transferidas por estas redes.

En esa línea, el Perú requiere fortalecer su legislación para atender lo establecido en el referido Convenio, definir un mecanismo de cooperación con los Estados y el sector privado para reducir los riesgos de seguridad digital e intercambio de información de incidentes de seguridad digital.

Cabe indicar que el referido Convenio de Budapest entró en entró en vigor en nuestro país el 01 de diciembre del año 2019, en consecuencia, se precisa realizar la adecuación de las normas que resulten necesarias para la implementación efectiva del referido convenio ello en la medida que de sufrir ataques que afecten la seguridad digital, en particular en lo referido a ciberdelincuencia, ello podría en devenir en daños irreparables en aquellos que se vean afectados así como en la confianza en la gestión que realice nuestro país en dicha materia.

- **Política Nacional de Inclusión Financiera**

Mediante Decreto Supremo N° 255-2019-EF, se aprueba la Política Nacional de Inclusión Financiera, la cual establece en como uno de sus objetivos prioritarios 4 "Desarrollar infraestructura de telecomunicaciones y plataformas digitales para incrementar la cobertura de servicios financieros. Lo cual se sustenta en desarrollar infraestructura de telecomunicaciones para facilitar que los servicios financieros se encuentren al alcance de todos los segmentos de la población, así como en desarrollar plataformas digitales a fin de favorecer la colaboración, interoperabilidad, autenticación, **seguridad digital** y el uso optimizado de las tecnologías digitales".

Consistente con ello, se estableció como uno de sus lineamientos "Desarrollar plataformas digitales a fin de favorecer la colaboración, interoperabilidad, autenticación, **seguridad digital** y el uso optimizado de las tecnologías digitales."

En esa línea, resulta urgente fortalecer la **regulación y plataformas** que permitan desplegar servicios digitales para promover la inclusión financiera, en un marco de confianza digital. En esa línea, **resulta urgente** establecer una norma que permita articular acciones en materia de seguridad digital como parte del marco de seguridad digital, las acciones se coordinarán con actores públicos y privados. Adicionalmente, es importante que asegurar que las plataformas digitales recojan las disposiciones emitidas por la Autoridad Nacional de Protección de Datos Personales y el INDECOPI en su calidad de protector del consumidor. Ahora bien, para preservar la seguridad digital se hace necesario que se establezcan obligaciones mínimas a los proveedores de servicios digitales, tal cual lo desarrolla Estonia, Colombia, Reino Unido, Dinamarca, etc.

Cabe señalar que la OCDE, en el año 2019, publicó el estudio "**Digital Government in Perú: Working Closely with Citizens**"¹⁷ recomienda:

- a. Considere establecer un Centro Nacional para gestionar los riesgos e incidentes de seguridad digital, conforme las mejores prácticas y las Recomendación de la OCDE sobre Gestión de riesgos de seguridad digital para la prosperidad económica y social (OCDE, 2015).

¹⁷ Obterido de OECD (2019), Digital Government in Peru: Working Closely with Citizens, OECD Digital Government Studies, OECD Publishing, Paris, <https://doi.org/10.1787/0c1eb85b-en>



- b. Buscar la cooperación con el sector privado y otros actores relevantes en este entorno.

B. Estado del Arte

Según estadísticas de la Cámara Peruana de Comercio Electrónico (CAPECE) se sabe que el comercio electrónico en el Perú creció un 30% en el año 2018 y ascendiendo a un monto de \$3,100 millones, estimando para el 2019 un crecimiento entre el 40% y 45% y un monto aproximado de \$4,000 millones¹⁸.

Adicionalmente, según datos del Instituto Nacional de Estadística e Informática (INEI) a setiembre 2019¹⁹ en el Perú la población de 06 años a más de edad que hace uso de internet es de 59.8%, con respecto al grupo etario se sabe que el 76.8% corresponde a adolescentes de 12 a 18 años de edad, el 88.5% a jóvenes de 19 a 24 años, y el 72.5% a adultos entre los 25 y 40 años, siendo estos grupos la población que más accede a este Internet. Un aspecto importante a considerar es el porcentaje de población que hace uso de Internet a través del teléfono celular es el 82.6%.

Con respecto a las actividades que realiza la población en Internet es mayormente para comunicarse (90.2%), obtener información (89.3%) y en actividades de entretenimiento (85.5%), operaciones en banca electrónica (14.5%), transacciones con entidades públicas (12%), comprar productos y/o servicios (13.4%), y vender productos y/o servicios (4.1%), descargar antivirus y aplicativos o software (23.3%).

Lo anterior, evidencia que para el caso peruano, la población viene incrementado su presencia e interacción en el entorno digital, se incrementan las transacciones, las ventas y compras, lo cual es producto de una mayor conectividad y que tanto entidades públicas como empresas han abierto canales digitales para ello. No obstante, se requiere dictar medidas que aseguren la confianza digital en la interacción de las personas con dichos servicios, más aun considerando que a la fecha nuestro país ha evidenciado la voluntad política y social por acoger la denominada transformación digital.

Indicador	Resultado
Confianza en el Estado Peruano	El 40% de los encuestados desconfía del Estado Peruano
Manera preferida para realizar gestiones	El 67 % de encuestados lo realiza de manera presencial El 24 % de encuestados lo realiza a través de internet El 9 % de encuestados lo realiza por teléfono
Trámites con alguna entidad por internet	9 de cada 10 encuestados no ha realizado ningún trámite a través de la página web de la entidad

Tabla 1.- Algunos Indicadores sobre satisfacción ciudadana | Fuente: Encuesta Nacional de Satisfacción Ciudadana 2017

Más aún, el Foro Económico Mundial (FEM) señala en su "Informe Global sobre Riesgos 2018"²⁰ (Global Risk Report, su denominación en inglés) que uno de los cinco (05) riesgos con mayor probabilidad es la ocurrencia de un "ciberataque a gran escala o malware", que causaría grandes daños económicos, tensiones geopolíticas o pérdida generalizada de la confianza en Internet.

En esa línea, se ha urgente emitir disposiciones específicas para establecer una norma que genera el Marco de Confianza digital, así como crear un Centro Nacional de Seguridad Digital, un Registro



¹⁸ Ver: <https://www.ecommerce-news.pe/ecommerce-insights/2019/crecimiento-del-comercio-electronico-en-peru.html>

¹⁹ Ver: <https://www.inei.gob.pe/media/MenuRecursivo/boletines/tidiciembre.pdf>

²⁰ El documento puede ser consultado en: <https://www.weforum.org/reports/the-global-risks-report-2018>

Nacional de Incidentes de Seguridad Digital y la constitución del dato como un activo estratégico refleja la voluntad del Estado por atender las preocupaciones y riesgos de las personas en el entorno digital, velar por su tranquilidad y asegurar confianza en los servicios digitales, aspecto que no puede esperar.

Estudios internacionales

Al respecto, en el 2018 Microsoft publicó el documento denominado "Global Cyber Risk Perception Survey"²¹, un estudio que proporciona una perspectiva sobre el estado de la gestión del riesgo cibemético en organizaciones a nivel mundial, concluyendo que estas últimas cada vez más son parte de una cadena de valor digital y por ende la gestión de riesgos de seguridad digital se constituye entre sus más altas prioridades en la gestión de riesgos.

La Unión Internacional de Telecomunicaciones (UIT) elabora anualmente una evaluación del Estado de la **ciberseguridad** en las economías miembros en base a cinco pilares: (i) Medidas legales, (ii) Medidas técnicas, (iii) Medidas organizativas, (iv) Desarrollo de capacidades, y (v) Cooperación. En el estudio 2018 nuestro país está ubicado en el puesto 95 de 193 economías evaluadas.

Confianza Digital

En esa línea, la **adecuada satisfacción** de las expectativas y la atención de las demandas y necesidades de los ciudadanos cuando realizan transacciones, consultas compras, descarga de información, etc., configura lo que denominados **confianza digital**, la cual tiene una serie de variables que necesitan ser entendidas, valoradas y tratadas con miras a favorecer que las personas, organizaciones y entidades usen y aprovechen las tecnologías digitales de manera sencilla, segura y confiable, atendiendo sus expectativas y necesidades.

Ahora bien, sobre la materia de confianza y sus componentes, se han realizado estudios para conocer el Estado del Arte, entre los cuales resaltan:

MasterCard presentó el Índice de Evolución Digital 2017²² (de sus siglas en inglés DEI 17), donde se propone un **Marco de la confianza digital** compuesto por cuatro habilitadores que ayudan a esbozar sobre la confianza digital y su importancia, siendo los siguientes:

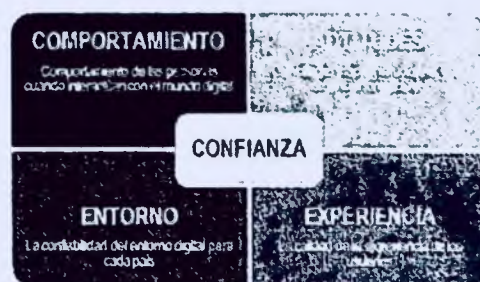


Figura 4.- Habilitadores de la Confianza Digital – Fuente: DEI 17

- Donde el **entorno y experiencia** es responsabilidad de las empresas, instituciones y gobierno. Ahora bien, el entorno se relaciona con la **seguridad**, los sistemas de responsabilidad y la **privacidad**. La **experiencia** se caracteriza por **cuan sencillo y predecible es para los usuarios interactuar con el entorno digital**.

²¹ El documento puede ser consultado en <https://bit.ly/2EFzKUX>

²² Digital Evolution Index 2017, MasterCard and The Fletcher School, https://globalrisk.mastercard.com/wp-content/uploads/2017/07/Mastercard_DigitalTrustL_PDFPrintL_FINAL_AG.pdf

- Las actitudes y el comportamiento son dimensiones relacionadas con los consumidores. La actitud corresponde a usuarios con niveles de auto-informados sobre tecnología, las transacciones en línea y la capacidad del gobierno para mantener sus datos seguros. El comportamiento es una medida de cómo los usuarios interactúan con el mundo digital.

Consistente con lo anterior, podemos referir que cuando **MasterCard** aborda el ámbito de confianza entiende aspectos vinculados a privacidad (**protección de datos personales, seguridad digital y protección de las personas en el entorno digital**)

Ahora bien, según el informe, el **Perú** se encuentra en el puesto **49 de 60 países** en la calificación de su evolución digital (estado de digitalización), por lo que se tiene mucho trabajo por hacer, en términos de desarrollo de infraestructura como de innovación.

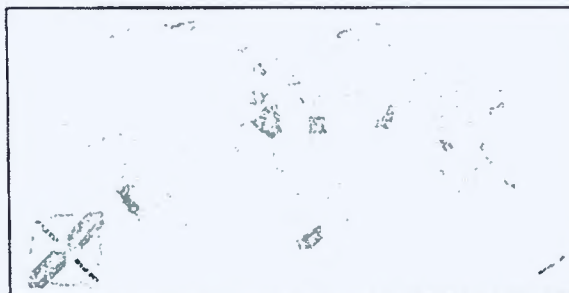


Figura 5.- Mapa de calor del Índice de Evolución Digital 2017 – Fuente: DEI 17

DELOITTE Insights, en su informe del Desarrollo de la Confianza Digital: La Tecnología puede liderar el camino²³, propone cuatro (04) pilares de la confianza, las cuales se describen a continuación:

1. **Ética y Responsabilidad:** A medida que las innovaciones tecnológicas plantean cuestiones éticas al dar a las organizaciones más poder, su disposición a trabajar por el bienestar de su cliente, puede generar mayores niveles de credibilidad y confianza.
2. **Privacidad y Control:** Las organizaciones que respetan las preferencias de los clientes sobre qué datos recopilar y cómo se manejan esos datos, pueden recibir mayores permisos para manejar la información de su cliente y proporcionar servicios personalizados.
3. **Transparencia y Accesibilidad:** La transparencia en torno a las prácticas comerciales digitales junto con divulgaciones fáciles de entender pueden ayudar a generar confianza en las intenciones de una organización y su promesa de ofrecer productos y servicios digitales de calidad.
4. **Seguridad y Confiabilidad:** Con una mayor conciencia sobre los riesgos cibernéticos y una mayor dependencia de los dispositivos inteligentes, los clientes cada vez más eligen organizaciones que utilizan la última tecnología para mantener los productos y servicios seguros y confiables.

De lo anterior, se deduce que la tecnología, por sí sola, no puede construir confianza, la confianza se soporta en **cuatro (04) pilares integrados**, los cuales abordan aspectos de **protección de datos personales, transparencia, seguridad digital y protección de las personas en el entorno digital**.



²³ Mayor información en "Building digital trust: Technology can lead the way", Deloitte 2019, https://www2.deloitte.com/content/dam/insights/us/articles/6320_Building-digital-trust/DI_Building-digital-trust.pdf

C. Problema

La confianza digital es un problema complejo que comprende diversos actores (público, privado, academia y sociedad civil) con diferentes intereses, pero un solo afectado que son las personas. En esa línea, la urgencia de establecer un Marco de confianza responde a:

- Vulneración de los derechos fundamentales del ciudadano en el entorno digital.
- Falta de una norma con rango de ley que establezca un marco de articulación entre actores públicos y privados para atender incidentes de seguridad digital a nivel nacional.
- No existe un registro unificado de los incidentes de seguridad digital en el Estado
- Pérdidas económicas como resultado de los ciberataques
- No se tiene un Centro Nacional de Seguridad Digital que gestione la respuesta en el ámbito nacional, interactuando con actores públicos y privados.

II. PROPUESTA O ALTERNATIVA DE SOLUCIÓN

Consistente con lo analizado, la propuesta de Decreto de Urgencia responde a motivaciones de naturaleza estratégica, económica, social, política y técnica, con miras a promover la confianza de los ciudadanos en el entorno digital, asegurando su desenvolvimiento con las mismas garantías que en el entorno digital.

La propuesta normativa tiene como primer aspecto a relevar aquel referido a Disposiciones Generales, las cuales establecen disposiciones sobre el "Objeto", "Alcance" y "Definiciones" que allana la comprensión e interpretación de las disposiciones sustantivas de la norma.

3.1 Objeto de la norma

El Decreto de Urgencia tiene por objeto establecer las medidas que resulten necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

3.2 Alcance de la propuesta

El Decreto de Urgencia comprende como alcance: "Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia", esto en conformidad de las recomendaciones establecidas por la OCDE, buenas prácticas internacionales y contexto internacional²⁴.

3.3 Definiciones

Conforme estándares y buenas prácticas internacionales se establecen un conjunto de definiciones con miras a entender de manera integral la propuesta normativa, los términos definidos son: Confianza Digital, Economía digital, Entorno Digital²⁵, Actividad crítica, Incidente de seguridad digital, Gestión de incidentes de seguridad digital, Riesgo de seguridad digital, Ciberseguridad, Servicio digital y Proveedor de servicios digitales.



²⁴ Conforme se recomienda en el libro "Best Practices for Establishing a National CSIRT", 2016, OEA

²⁵ La definición de "entorno digital" toma como base lo establecido en el numeral 2 del artículo 3 del Decreto Legislativo N° 1412.

3.4 Marco de Confianza Digital

Conforme el análisis del contexto normativo, tendencias y el impacto que la confianza en el entorno digital tiene en la confianza en el gobierno, emprendimiento, uso de servicios digitales, se establecen disposiciones en materia de confianza digital, las cuales se integran en tres ámbitos 1. Marco de Confianza Digital y 2. Medidas para fortalecer la confianza digital y 3. Uso ético de las tecnologías digitales y de los datos.

Así, considerando las investigaciones y estudios revisados (**Mastercard, Deloitte, ISG y la OCDE**) sobre la **confianza digital**, se constituye el Marco de Confianza Digital indicando que es el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital.

Asimismo, se establece que el **Marco de Confianza Digital** tiene los siguientes ámbitos:

- Protección de datos personales y transparencia.**- El Ministerio de Justicia y Derechos Humanos (MINJUSDH), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.
- Protección del consumidor.**- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.
- Seguridad Digital.**- La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de seguridad digital en el país, norma, dirige, supervisa y evalúa la materia de seguridad digital.

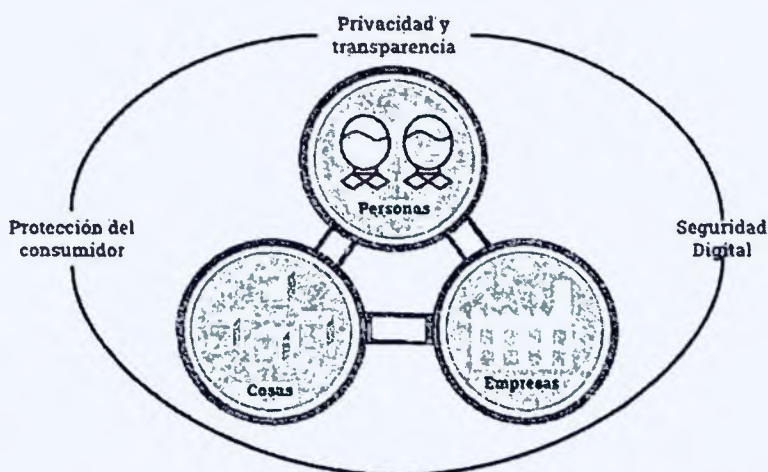


Figura 7.- Confianza digital – Fuente: Secretaría de Gobierno Digital

Consistente con lo anterior, y entendiendo que este ámbito requiere un actor articulador se establece que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital en el país y responsable de la articulación de cada uno de sus ámbitos. Cabe resaltar que la PCM es responsable de la coordinación de las políticas nacionales de carácter sectorial y multisectorial del Poder Ejecutivo y de la coordinación con los demás Poderes del Estado, organismos constitucionales autónomos, gobiernos regionales, gobiernos locales, y sociedad civil, conforme lo establece el artículo 2 de su Reglamento de Organización y Funciones y la Ley Orgánica del Poder Ejecutivo, artículos 17 y 18. En ese sentido, el posicionamiento y la autoridad de la Presidencia del Consejo de Ministros, resulta un factor determinante en el cumplimiento de las mismas.



En esa línea, se le confiere una serie de atribuciones en su calidad de ente rector, las cuales son tomadas de las recomendaciones y estándares internacionales, las cuales son las siguientes:

- a. Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.
- b. Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.
- c. Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.
- d. Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.
- e. Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.

Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias

Adicionalmente, conforme las recomendaciones de la OCDE señaladas en el documento "Gobierno Digital en el Perú – Trabajando de cerca con los ciudadanos", y de conformidad con el Marco de Seguridad Digital creado en el Decreto Legislativo N° 1412, Ley de Gobierno Digital, se dispone la creación del Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza y bienestar de las personas en el entorno digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

En esa línea, se establece que el Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

Asimismo, se establece que el referido Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional como responsable de i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital.

Otro aspecto a relevar es su capacidad de articular e intercambiar información con los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.



98

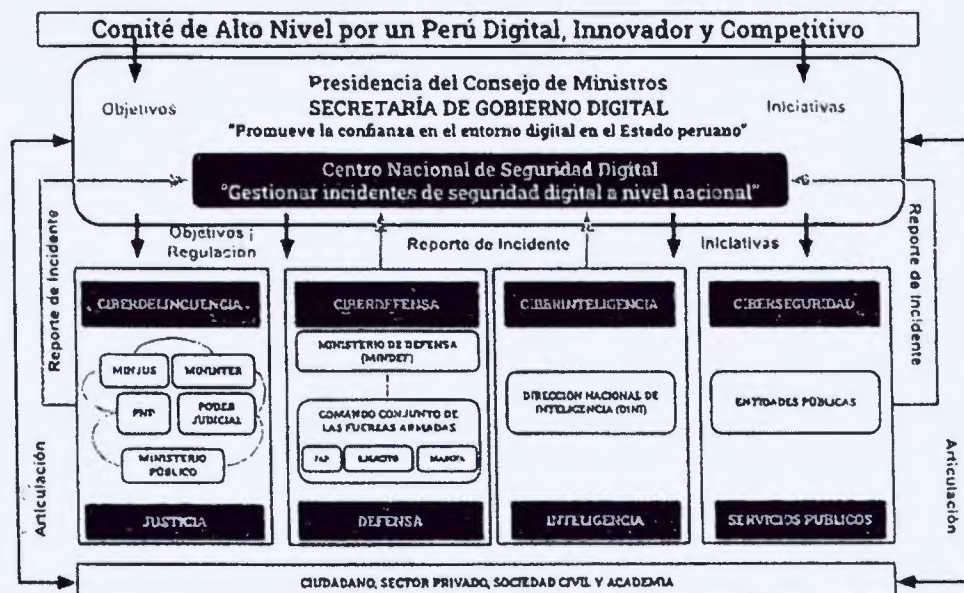


Figura 8. - Marco de Gobernanza de Seguridad Digital – Fuente: Secretaría de Gobierno Digital

3.5 Medidas para fortalecer la confianza digital

Entendiendo que la seguridad digital es un ámbito de la confianza digital y que siendo consistente con su definición es una tarea de intensa cooperación, colaboración y articulación con actores públicos, privados y sociedad civil, se plantea la creación de un Registro Nacional de incidentes de seguridad digital, que tiene por finalidad recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

El **Registro Nacional de Incidentes de Seguridad Digital** y la información contenida en el mismo tiene carácter confidencial y se soporta en una plataforma digital, el cual es administrado por la Secretaría de Gobierno Digital, quien mantiene su disponibilidad, confidencialidad e integridad.

Cabe señalar que atendiendo la diversidad de actores que pueden aprovechar la información del registro de incidentes, es el Centro Nacional de Seguridad Digital, en su calidad de administrador quien brinda información sobre los registros de incidentes de seguridad digital, por mandato judicial o cuando corresponda, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412 y del Marco de Confianza Digital conforme a la presente norma.

En línea con lo anterior, también es necesario establecer obligaciones para los proveedores de servicios digitales. En esa línea, las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y proveedores de servicios educativos deben:

- Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
- Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.
- Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.



- d. *Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.*
- e. *Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad que involucre datos personales.*
- f. *Mantener una infraestructura segura, escalable e interoperable.*

No obstante, dichas obligaciones no comprenden a la infraestructura de telecomunicaciones a cargo de los concesionarios de servicios de internet, quienes se rigen por sus contratos de concesión vigentes.

Ahora bien, en el caso de entidades de la administración pública, en materia de seguridad digital deben cumplir con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y toda regulación emitida por la Secretaría de Gobierno Digital en su calidad de ente rector de la seguridad digital en el país.

Las organizaciones privadas toman como referencia las normas emitidas por la Presidencia del Consejo de Ministros en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

Asimismo, se refiere que toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Adicionalmente, se requieren mecanismos de articulación concordantes con la política exterior y que contribuyan a la confianza en el entorno digital. En esa línea, se ha previsto que la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordine con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias

Consistente con lo anterior, la propuesta hace una mención especial a los datos, considerando que estos son activos estratégicos. En esa línea, se establece que las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, los biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accedan, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad vigente.

Así, las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

Es preciso indicar que la propuesta normativa no pretende emitir regulaciones sobre contenidos en Internet, siendo esto facultad del sector privado salvo aquellos contenidos que se tipifiquen como delitos o violación de los derechos de las personas, para lo cual la autoridad competente establecerá las sanciones correspondientes en el marco de confianza digital.

Cabe señalar que en el marco de la Ley N° 29733, el tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales ejercida, a través del Ministerio de Justicia y Derechos Humanos.



100

Por otro lado, el artículo 17 de la Ley N° 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica (en adelante, Ley de Banda Ancha), establece que el Estado cuenta con una Red Nacional del Estado Peruano (REDNACE) definida como una red de acceso que se utiliza para la conectividad a nivel nacional aspecto base para el desarrollo de una Sociedad Digital, cabe señalar que se ha establecido que se priorizara ámbitos relacionados con la educación, salud, defensa nacional, seguridad, cultura, investigación y desarrollo e innovación para cumplir con las políticas y lograr los objetivos nacionales, quedando prohibido su uso comercial.

Asimismo, el artículo 25 de la Ley de Banda Ancha establece la incorporación de todas las universidades públicas e institutos de investigación a la REDNACE, formando la Red Nacional de Investigación y Educación (RNIE), a efectos de su integración a las redes regionales de investigación y educación del mundo, con la finalidad de mejorar los procesos de investigación, desarrollo tecnológico e innovación.

Cabe señalar que la OCDE²⁶, ONU y el BID ²⁷en sus distintos informes reconocen lo importante de contar con redes de acceso y alta velocidad para promover la digitalización de la economía y sociedad.

Conforme lo anterior se puede advertir que la REDNACE y la RNIE constituyen redes estratégicas para el Estado, más aun, debido a que:

- Son un activo clave para el proceso de digitalización del Estado, de los cuales se deben gestionar sus riesgos.
- Involucra a todas las entidades de la administración pública para asegurar la conectividad de dichas entidades en la prestación de servicios en favor de la población.
- Involucra a universidades públicas e institutos de investigación los que, a través de procesos de investigación, desarrollo tecnológico e innovación, generan valor en la población.
- Sobre la REDNACE es posible configurar otras subredes por software, en base a las facilidades del IP MPLS, como son las redes de teleservicios (telesalud, teleducación, televigilancia, entre otros) con prestaciones y prioridades configurables y que permitirían proveer servicios en la nube o el uso de plataformas y aplicativos compartidos o virtualizados para una mejor gestión de los recursos del Estado.



Dada la relevancia de ambas redes, resulta preponderante que su uso y despliegue sean promovidos por un órgano que permita la adecuada articulación con las distintas entidades e instituciones involucradas, supervise su adecuado funcionamiento, así como su utilización en la implementación de servicios básicos habilitados por las tecnologías digitales en favor de la población, lo que implica una constante coordinación con los sectores involucrados en cada caso.

Siendo ello así, y en atención a las funciones que viene desempeñando la Secretaría de Gobierno Digital, respecto a la coordinación de la seguridad digital, interoperabilidad de los sistemas informáticos del Estado, la asistencia técnica para la implementación de proyectos de tecnologías de la información, así como el impulso en el proceso de desarrollo e innovación tecnológica para la mejora de la gestión pública y digitalización del Estado promoviendo la integración tecnológica,

²⁶ Toma como fuente el documento "Perfilando la transformación digital en América Latina". https://www.oecd-ilibrary.org/science-and-technology/perfilando-la-transformacion-digital-en-america-latina_4817d61b-es

²⁷ Toma como fuente el "Informe anual del Índice de Desarrollo de la Banda Ancha en América Latina y el Caribe: IDBA 2018" <https://publications.iadb.org/es/informe-anual-del-indice-de-desarrollo-de-la-banda-ancha-en-america-latina-y-el-caribe-idba-2018>

101

esta Secretaría sería el ente idóneo para asumir la gestión y administración de la REDNACE y la RNIE.

Centro Nacional de Datos

La seguridad es un componente esencial para generar "confianza" y el mismo requiere contar con espacios que permitan técnicamente custodiar la información bajo un modelo efectivo de gobernanza. Es por ello, que el crear un Centro Nacional de Datos, como una plataforma digital, permitirá disponer de espacios de uso exclusivo donde las entidades públicas y privadas, mantienen y operan sus infraestructuras tecnológicas. Es ese espacio donde se pueden alojar los servidores y sistemas de almacenamiento para ejecutar las aplicaciones que procesan y almacenan datos.

El Centro Nacional de Datos intercambia información y articula acciones con las entidades públicas, academia, sociedad civil y sector privado y con las entidades responsables de los ámbitos del Marco de Confianza Digital para la gobernanza de datos.

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en su calidad de ente rector en gobernanza de datos, establece los protocolos y mecanismos en materia de gobierno de datos y emite los lineamientos y las directivas correspondientes.

Adicionalmente, en materia de gestión de proyectos de inversión privada o en relación a contratos suscritos para dicho fin, se establece que no serán afectados o comprendidos en el alcance de la presente norma. En esa línea, se ha establecido una disposición complementaria final que indica lo siguiente:

CUARTA.- Aplicación de la Norma

La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

III. ANÁLISIS COSTO – BENEFICIO

La presente sección identifica los costos y beneficios de la propuesta. Al respecto, entre los beneficios advertidos se encuentran los siguientes:

- Mayor confianza en el uso de canales digitales por parte de la ciudadanía, al establecer obligaciones a los proveedores de servicios digitales con respecto a la implementación de medidas de seguridad físicas, técnicas, organizativas y legales, la correcta gestión de sus riesgos de seguridad digital, entre otros, que permita acceder a las personas a servicios digitales seguros, escalables y confiables.
- Fortalecer el despliegue del proceso de transformación digital de manera sostenible, al ser la confianza digital un aspecto clave para dicho proceso. La transformación digital conlleva a una serie de desafíos, algunos de los cuales pueden representar una ventaja, no obstante, otros pueden representar riesgos para la seguridad. En esa línea, contar con un Marco de Confianza Digital que comprende a actores del sector público, privado, academia y sociedad civil permitirá fortalecer las medidas que aseguren la seguridad digital, la protección de datos personales y la protección al consumidor en el entorno digital, tanto las personas, como empresas y entidades públicas deben compartir la responsabilidad de la seguridad digital.
- Garantizar la seguridad con respecto al resguardo y acceso a los datos e información que gestiona el sector público, al tener un mayor nivel de comprensión por parte de los funcionarios con respecto



102

a los datos como activo estratégico, así como al contar con un centro nacional de datos para su gobernanza. Lo anterior implica ahorros por la ocurrencia de posibles incidentes relacionados al robo de información o acceso indebido a la misma.

- Mejora en los indicadores de satisfacción ciudadana asociados al uso de los servicios digitales.
- Contar con funcionarios y servidores públicos capacitados en materia de seguridad digital, ya que la implementación del Centro Nacional de Seguridad Digital comprende acciones para el fortalecimiento de capacidades en los aspectos técnicos, legales, organizacionales de la seguridad digital.
- Contribuir al crecimiento del comercio electrónico y gobierno digital en el país al fortalecer el ecosistema digital que requiere un mayor nivel de articulación entre actores públicos y privados para asegurar la adecuada protección de las personas, en sus diferentes roles (administrado, consumidor, usuario, etc.) en el entorno digital, al favorecer el intercambio de información sobre amenazas, vulnerabilidades e incidentes.

De otro lado, con respecto a los costos que implicaría el establecimiento de un marco de confianza digital y medidas para su fortalecimiento, señalar lo siguiente:

En el año 2016, **Kaspersky Lab**²⁸, en conjunto con B2B International, realizó un estudio global en más de 4,000 empresas representativos de 25 países, observando sus presupuestos de seguridad informática, la complejidad de su infraestructura, la actitud que toman ante las amenazas de seguridad y soluciones, el costo real de las filtraciones de información, y los incidentes de seguridad que han sufrido. La **inversión anual promedio** por parte de las empresas varía entre **\$1,000 USD** para las empresas más pequeñas y **\$1,000,000 USD** en el caso de las más grandes, donde el **costo promedio de la recuperación** de un solo incidente de seguridad está estimado en **\$86.5 mil USD** para las pequeñas y medianas empresas y **\$861 mil USD** para las grandes.

	Empresas pequeñas	Empresas grandes
Inversión anual	\$1,000 USD	\$1,000,000 USD
Costo promedio de la recuperación	\$86.5 mil	\$861 mil USD

Tabla 3.- Costo e inversión – Fuente: Kaspersky Lab

Los ciberataques le han costado a las pequeñas y microempresas un estimado de \$149,000 y a las empresas \$2 millones de dólares, y los ataques dirigidos resultan en un impacto financiero de \$134,000 y \$1.7 millones de dólares respectivamente.



Conviene indicar, que según estudios realizados por ESET SECURITY REPORT Latinoamérica 2019, en la cual participan entidades públicas, banca y finanzas, educación, entre otros, las organizaciones afrontan los retos de seguridad digital llevando acciones relacionadas a la implementación de proyectos de seguridad y actividades de educación, resaltando que el porcentaje de organizaciones que lleva a cabo actividades de educación de forma periódica y sufrió incidentes de seguridad alcanzó un 18%, mientras que aquellas en las que no se realizan este tipo de actividades alcanzó un 40%.

Ahora bien, según los estudios en materia de ciberseguridad realizados por la Organización de Estados Americanos (OEA) las pérdidas para la administración pública en materia datos e información sustraída, robada, recuperada, o alterada alcanza los 17 millones de dólares aproximadamente. Cabe indicar que esto implica aspectos reputaciones, la imagen de la entidad o empresa, la infraestructura que se ve afectada, los procesos detenidos, etc. No obstante, el costo de recuperación de un incidente de seguridad digital en la administración pública es similar que en el sector privado en términos monetarios;

²⁸ Mayor información en <https://latam.kaspersky.com/blog/reporte-midiendo-el-impacto-financiero-de-la-seguridad-informatica-en-los-negocios/7711/>

103

sin embargo, el impacto es mayor al considerarse que la información que posee el sector público puede llegar a comprender información sensible, reservada, confidencial de lo peruanos y entidades a nivel nacional.

Las disposiciones referidas a la implementación del Centro Nacional de Seguridad Digital, Registro Nacional de Incidentes de Seguridad Digital, Centro Nacional de Datos y plataforma de aprendizaje en línea se encuentran contemplados como parte de los componentes del "Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional", que a la fecha viene ejecutando la Presidencia del Consejo de Ministros. El referido Proyecto tiene un monto de inversión de US\$ 60.9 millones, siendo el monto del préstamo de US\$ 50 millones y la contrapartida nacional de US\$ 10.9 millones, de este monto total el porcentaje destinado a dichas implementaciones es de 20% aproximadamente.

Con respecto a las obligaciones por parte de entidades públicas y privadas que prestan servicios digitales señalar lo siguiente:

Obligaciones	Inversión
Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.	PCM implementa el Registro Nacional de Incidentes de Seguridad Digital, por lo que los actores públicos y privados solo deben realizar el registro respectivo. Para ello, la SEGDI realizará capacitaciones para su registro.
Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.	Tanto las entidades públicas y privadas invertirán en por lo menos backup y antimalware con el presupuesto que manejan actualmente. Adicionalmente, la SEGDI realizará capacitaciones en línea.
Gestionar los riesgos de seguridad digital en su organización.	La PCM implementará una plataforma y lineamientos para la gestión de riesgos. Adicionalmente, la SEGDI realizará capacitaciones en línea.
Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.	Las entidades públicas usarán gratuitamente la plataforma de autenticación nacional de RENIEC, las organizaciones privadas implementarán mejoras
Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad que involucre datos personales.	Las acciones se encuentran a cargo del MINJUSDH quien a la fecha ya viene ejecutándolas.
Mantener una infraestructura segura, escalable e interoperable	Tanto las entidades públicas y privadas invertirán en por lo menos backup y antimalware con el presupuesto que manejan actualmente

Finalmente, concluir que una vez valorados los beneficios y posibles cargas que pudiera generar la implementación de la propuesta normativa, señalar que su implementación sería positiva, principalmente por promover la confianza digital en las interacciones que realizan el 59.8%²⁹ (más de

²⁹ Se realizó la consulta al "Sistema de Consulta de Base de Datos" de los "Censos Nacionales 2017: XII de Población, VII de Vivienda y III de Comunidades Indígenas" de la cual se obtuvo que la población de 0 a 18 años es de 9,704 850 personas a nivel nacional. Ver: <http://censos2017.nei.gob.pe/redatam/>. De la consulta realizada al "Sistema de Consulta de Base de Datos" de los "Censos Nacionales 2017: XII de Población, VII de Vivienda y III de Comunidades Indígenas" se obtuvo la cantidad de población niños de 06 a 11 años y adolescentes de 12 a 18 años a partir, la cual es de 6,699 288 personas. A partir de dicha cantidad se ha

16 millones de personas aproximadamente) de la población que accede a Internet en nuestro país, así como también a las empresas (grandes, medianas, pequeñas, micro) que utiliza las tecnologías digitales fomentando una cultura preventiva de seguridad y protección de datos e información, que permita minimizar los riesgos de seguridad digital.

IV. EFECTO DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

El presente proyecto de Decreto de Urgencia se ha elaborado en cumplimiento de lo dispuesto en el artículo 74 de la Constitución Política del Estado y está en concordancia con lo dispuesto por la Ley General.

Asimismo, el proyecto de Decreto de Urgencia propuesto, no deroga ni modifica ninguna norma con rango legal vigente de nuestro ordenamiento jurídico, en razón que, lo expresado en el Decreto de Urgencia en mención, establece el Marco de la Confianza Digital y medidas adicionales para su fortalecimiento. En vista de ello, la presente exposición de motivos, promueve el crecimiento de entornos digitales seguros, íntegros y confiables, a fin de reducir la brecha entre las expectativas de las entidades de la Administración Pública y las necesidades o intereses del ciudadano, personas y empresas.



105

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

Única.- Norma derogatoria

Deróganse las disposiciones contenidas en el Decreto Legislativo 604 relativas al Sistema Nacional de Informática que se opongan al presente Decreto de Urgencia. Entiéndase, para todos sus efectos, que el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

MARÍA ANTONIETA ALVA LUPERDI
Ministra de Economía y Finanzas y
Encargada del Despacho del Ministerio de
Relaciones Exteriores

FLOR AIDEÉ PABLO MEDINA
Ministra de Educación

ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos

ROCÍO INGRED BARRIOS ALVARADO
Ministra de la Producción

EDMER TRUJILLO MORI
Ministro de Transportes y Comunicaciones

1844001-1

DECRETO DE URGENCIA
Nº 007-2020

DECRETO DE URGENCIA QUE APRUEBA EL
MARCO DE CONFIANZA DIGITAL Y DISPONE
MEDIDAS PARA SU FORTALECIMIENTO

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia de los que da cuenta a la Comisión Permanente para que los examine y los eleve al Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo Nº 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, mediante Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece 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;

Que, 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;

Que, mediante Decreto Supremo Nº 237-2019-EF, se aprueba el Plan Nacional de Competitividad y Productividad, el cual presenta un conjunto de medidas consensuadas entre el sector público y privado con miras a establecer un entorno favorable y competitivo que permita generar bienestar para todos los peruanos sobre la base de un crecimiento económico sostenible con enfoque territorial;

Que, del precitado Plan Nacional se entiende que las tecnologías digitales tienen un valor estratégico para reducir brechas, impulsar la innovación y apoyar en el crecimiento del país; más aún, señala que los cambios tecnológicos por los cuales atraviesa el mundo actual serían mucho más fáciles de adoptar si es que realizamos una transformación digital a lo largo del país;

Que, mediante Decreto Supremo Nº 086-2015-PCM se declara de interés nacional las acciones, actividades e iniciativas desarrolladas en el marco del proceso de vinculación del Perú con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) e implementación del Programa País, en esa línea, cobra relevancia las Recomendaciones para la Gestión de Riesgos de Seguridad Digital realizadas por la OCDE, entre las cuales se señala la importancia del establecimiento de Equipos de Respuestas a Incidentes de Seguridad Digital a nivel de los Estados;

Que, en el documento Gobierno Digital en el Perú "Trabajando con los ciudadanos" la OCDE señala como recomendación que el Estado Peruano debe "considerar establecer un Centro Nacional de Seguridad Digital" que busque articular acciones con los actores relevantes para gestionar incidentes de seguridad digital y fortalecer la confianza;

Que, la confianza digital es un estado que emerge como resultado de cuán veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital. La confianza digital es un componente de la Transformación Digital y tiene como ámbitos la protección de datos, transparencia, seguridad digital y protección del consumidor en el entorno digital;

Que, ante ello como parte de nuestro proceso de vinculación, resulta necesario dictar medidas en materia de confianza y seguridad digital, estableciendo los mecanismos de colaboración y articulación con actores públicos, privados y sociedad civil en el entorno digital, a través de un enfoque sistémico e integral que asegure el fortalecimiento de la confianza en los servicios digitales por las personas, entidades y sociedad en general;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;

Con el voto aprobatorio del Consejo de Ministros; y,
Con cargo a dar cuenta a la Comisión Permanente para que lo examine y lo eleve al Congreso, una vez que éste se instale;

DECRETA:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Decreto de Urgencia tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

104

Artículo 2. Alcance

Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia.

Artículo 3. Definiciones

Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:

a) Confianza Digital.- Es 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.

b) Economía digital.- Es la innovación y la transformación de la economía basada en el uso estratégico y disruptivo de las tecnologías digitales. Desarrolla la capacidad de incrementar la eficiencia, productividad, transparencia, seguridad y eficacia de los procesos y actividades económicas y sociales, sustentada en el uso intensivo de tecnologías digitales, redes de datos o comunicación y plataformas digitales. Conlleva a la generación de beneficios económicos y sociales, prosperidad y bienestar para la sociedad.

c) Entorno Digital.- Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes e infraestructuras de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, plataformas que sirven como base para la interacción entre personas, empresas, entidades públicas o dispositivos.

d) Actividad crítica.- Es la actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, en el funcionamiento efectivo de los servicios esenciales que rigen la economía, sociedad y el gobierno, o afectan la prosperidad económica y social en general.

e) Incidente de seguridad digital.- Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

f) Gestión de incidentes de seguridad digital.- Proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

g) Riesgo de seguridad digital.- Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.

h) Ciberseguridad.- Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

i) Servicio digital.- Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo, al menos

una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.

j) Proveedor de servicios digitales.- Comprende a cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional.

CAPÍTULO II

MARCO DE CONFIANZA DIGITAL

Artículo 4. Marco de Confianza Digital

4.1 El Marco de Confianza Digital se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital.

4.2 El Marco de Confianza Digital tiene los siguientes ámbitos:

a) Protección de datos personales y transparencia.- El Ministerio de Justicia y Derechos Humanos (MINJUSDH), quien ejerce las autoridades nacionales de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.

b) Protección del consumidor.- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.

c) Seguridad Digital.- La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de seguridad digital en el país, norma, dirige, supervisa y evalúa la materia de seguridad digital.

Artículo 5. Ente rector del Marco de Confianza Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos.

Artículo 6. Atribuciones del Ente rector

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la Confianza Digital, tiene las siguientes funciones:

a) Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.

b) Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.

c) Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.

d) Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.

e) Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.

Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias.

Artículo 7. Centro Nacional de Seguridad Digital

7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige,

162

articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

7.2 El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

7.3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional responsable de: i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y, ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital.

7.5 La Secretaría de Gobierno Digital establece los protocolos de escalamiento, coordinación, intercambio y activación ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes.

CAPÍTULO III MEDIDAS PARA FORTALECER LA CONFIANZA DIGITAL

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

8.1 Créase el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

8.2 El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad.

8.3 El Centro Nacional de Seguridad Digital brinda información sobre los registros de incidentes de seguridad digital, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, y del Marco de Confianza Digital debiendo observar para tal efecto la normatividad vigente en materia de protección de datos personales.

Artículo 9. Obligaciones del Proveedor de servicios digitales

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

- Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
- Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.
- Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que

permitan proteger la confidencialidad, integridad y disponibilidad de la información.

d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.

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

f) Mantener una infraestructura segura, escalable e interoperable.

9.2 Las organizaciones privadas toman como referencia las normas emitidas por la Secretaría de Gobierno Digital en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

9.3 Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

9.4 Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Artículo 10. Articulación internacional

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias.

Artículo 11. Articulación en Materia de Comunicaciones

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Transportes y Comunicaciones las acciones vinculadas a la materia de comunicaciones en el marco de sus competencias.

CAPÍTULO IV USO ÉTICO DE LAS TECNOLOGÍAS DIGITALES Y DE LOS DATOS

Artículo 12. Datos como activos estratégicos

12.1 Las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, acceden, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad en materia de protección de datos personales, gobierno digital y seguridad digital.

12.2 Las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

12.3 El tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

Artículo 13. Centro Nacional de Datos

13.1 Créase el Centro Nacional de Datos como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de datos a nivel nacional, a fin de fortalecer la confianza y bienestar de las personas en el entorno digital en el marco de la presente norma.

13.2 El Centro Nacional de Datos se encuentra a cargo de la Presidencia del Consejo de Ministros, a través

108

de la Secretaría de Gobierno Digital y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

13.3 El Centro Nacional de Datos intercambia información y articula acciones con las entidades públicas, academia, sociedad civil y sector privado y con las entidades responsables de los ámbitos del Marco de Confianza Digital para la gobernanza de datos.

13.4 La Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos, establece los protocolos y mecanismos en materia de gobierno de datos y emite los lineamientos y las directivas correspondientes.

Artículo 14. Financiamiento

La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 15. Refrendo

El presente Decreto de Urgencia es refrendado por el Presidente del Consejo de Ministros y la Ministra de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Reglamentación

El Poder Ejecutivo, dentro de los noventa (90) días hábiles siguientes a la entrada en vigencia de la presente norma, aprueba su reglamento mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

Segunda. Registro Nacional de Incidentes de Seguridad Digital

En un plazo no mayor a noventa (90) días hábiles, posterior a la publicación del presente Decreto de Urgencia, la Presidencia del Consejo de Ministros implementa el Registro Nacional de Incidentes de Seguridad Digital y dicta normas, lineamientos y directivas para su correcto funcionamiento.

Tercera. Gestión e Impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE)

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, se encarga de la gestión e impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE) a las que se refiere la Ley N° 29904 a fin de coadyuvar al logro de las políticas nacionales, el fortalecimiento de una sociedad digital y la transformación digital del Estado. La contratación de los servicios para la conectividad de la REDNACE es realizada por cada entidad de la Administración Pública, de conformidad con lo dispuesto en el artículo 19 de dicha Ley.

Cuarta. Aplicación de la Norma

La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

Dado en la Casa de Gobierno, en Lima, a los ocho días del mes de enero del año dos mil veinte.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

VICENTE ANTONIO ZEBALLOS SALINAS
Presidente del Consejo de Ministros

ANA TERESA REVILLA VERGARA
Ministra de Justicia y Derechos Humanos

1844001-2

DECRETO DE URGENCIA N° 008-2020

DECRETO DE URGENCIA QUE ESTABLECE NUEVOS SUPUESTOS DE CONVERSIÓN DE PENA EN LOS CASOS DE PERSONAS PRIVADAS DE LIBERTAD POR EL DELITO DE OMISIÓN DE ASISTENCIA FAMILIAR PARA PROMOVER EL PAGO DE LA REPARACIÓN CIVIL Y LA DEUDA ALIMENTICIA

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de conformidad con el artículo 135 de la Constitución Política del Perú, durante el interregno parlamentario, el Poder Ejecutivo legisla mediante decretos de urgencia, de los que da cuenta a la Comisión Permanente para que los examine y los eleve al nuevo Congreso, una vez que éste se instale;

Que, mediante Decreto Supremo N° 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso, se revocó el mandato parlamentario de los congresistas, manteniéndose en funciones la Comisión Permanente;

Que, la Constitución Política del Perú señala en su artículo 4 que el Estado protege especialmente al niño, al adolescente y a la familia, reconociendo a esta última como un instituto natural y fundamental de la sociedad. Una disposición sobre la protección de niños y adolescentes que es ratificada en el artículo IX del Título Preliminar de la Ley N° 27337, Código de los Niños y Adolescentes, que establece que, en toda medida concerniente al niño y al adolescente, adoptada por el Estado, se considere el Principio del Interés Superior del Niño y del Adolescente y el respeto a sus derechos;

Que, ante las dificultades de cumplimiento de obligaciones alimentarias respecto a niños, niñas y adolescentes ocasionadas por la reclusión de los obligados; y la necesidad de atender prioritariamente los intereses y las oportunidades que requieren los niños, las niñas y los adolescentes en su condición de población vulnerable, resulta conveniente promover egresos penitenciarios de internos condenados por omisión de asistencia familiar, siempre que su otorgamiento esté expresamente condicionado al pago íntegro de las deudas pendientes; que se establezca una revocatoria inmediata por incumplimiento posterior del pago; y que el egresado continúe sancionado con una pena alternativa que permita resocializarlo. Esta medida, a su vez, logrará contrarrestar el hacinamiento penitenciario que aqueja al Sistema Penitenciario peruano a nivel nacional;

Que, la Constitución Política del Perú señala en el inciso 22 de su artículo 139, que el objeto del régimen penitenciario es la reeducación, rehabilitación y reincorporación del penado a la sociedad. Lamentablemente, la situación penitenciaria actual presenta condiciones críticas por las que, a través del Decreto Supremo N° 013-2018-JUS, Decreto Supremo que proroga la emergencia dispuesta por el Decreto Legislativo N° 1325, para la reestructuración del Sistema Nacional Penitenciario y el Instituto Nacional Penitenciario, se prorrogó el periodo de emergencia del Sistema Nacional Penitenciario y del Instituto Nacional Penitenciario, por veinticuatro meses adicionales, en razón a asuntos de seguridad, salud, deficiente infraestructura y hacinamiento, siendo este último el factor que problematiza integralmente el funcionamiento regular del modelo penitenciario;

Que, actualmente nuestros establecimientos penitenciarios albergan aproximadamente 2900 internos por el delito de omisión de asistencia familiar, cuya condición de reclusión no asegura el cumplimiento de las obligaciones alimenticias impuestas y, por el contrario, lo dificulta, repercutiendo directamente en la situación de carencia o desabastecimiento que padecen los niños, niñas o adolescentes que son destinatarios legítimos de dicho pago;

En uso de las facultades conferidas por el artículo 135 de la Constitución Política del Perú;

109

COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA

Lima, 19 de febrero de 2020

En cumplimiento del segundo párrafo del artículo 135 de la Constitución Política del Perú, el congresista Neyra Olaychea, designado como coordinador para la elaboración del informe de evaluación del **Decreto de Urgencia 007-2020**, presentó el 17 de febrero de 2020, con el congresista Palma Mendoza el informe de evaluación sobre el **Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento**.-----

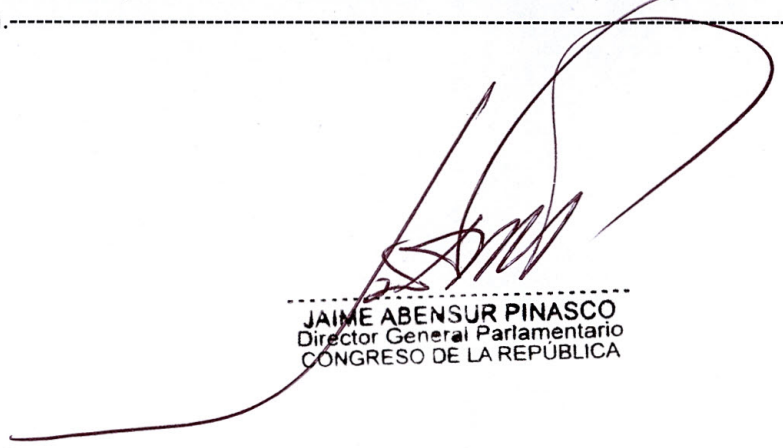
Seguidamente, la Presidencia dio cuenta del mencionado informe y lo puso a debate.-----

Finalizado el debate, se sometió a votación nominal el Informe de evaluación del **Decreto de Urgencia 007-2020**, el cual se aprobó por 7 votos a favor, 3 votos en contra y 11 abstenciones.-----

Posteriormente, la Presidencia dejó constancia del voto a favor de la congresista Salazar De La Torre.-----

La Presidencia manifestó que dicho informe será elevado al nuevo Congreso, una vez instalado este, para que proceda conforme a lo establecido en el segundo párrafo del artículo 135 de la Constitución Política del Perú.-----

Se acordó la dispensa del trámite de sanción del Acta para ejecutar lo acordado en la presente sesión.-----



JAIME ABENSUR PINASCO
Director General Parlamentario
CONGRESO DE LA REPÚBLICA