EXPOSICIÓN DE MOTIVOS

DECRETO SUPREMO QUE APRUEBA EL REGLAMENTO DEL DECRETO DE URGENCIA N° 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO

I. ANTECEDENTES

El Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, señala en su artículo 8 que "La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital (hoy Secretaría de Gobierno y Transformación Digital - SGTD), es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, **seguridad digital** y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento" (énfasis añadido).

Asimismo, el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, establece en sus artículos 4 y 7 que el Sistema Nacional de Transformación Digital abarca de manera no limitativa, las materias de gobierno digital, economía digital, conectividad digital, educación digital, tecnologías digitales, innovación digital, servicios digitales, sociedad digital, ciudadanía e inclusión digital y **confianza digital;** y que la Presidencia del Consejo de Ministros, a través de la SGTD, es el ente rector del Sistema Nacional de Transformación Digital, constituyéndose en la autoridad técnico-normativa a nivel nacional sobre la materia.

A su vez, el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, tiene como objeto, según su artículo 1, 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.

En ese marco, el objeto que persigue este reglamento es desarrollar lo establecido en el Decreto de Urgencia N° 007-2020, a fin de lograr que las interacciones digitales de las personas con los servicios digitales prestados por las entidades públicas y organizaciones del sector privado en el territorio nacional, se desarrollen de tal forma que la información a la que estos accedan sea veraz, predecible, segura, inclusiva y confiable, fortaleciendo así la confianza de los usuarios en el entorno digital, promoviendo el avance de la transformación digital y fomentando el ejercicio de la ciudadanía digital.

Considerando lo mencionado en el párrafo anterior, se señala que la finalidad de este reglamento es regular las conductas que permitan alcanzar la prosperidad económica, garantizar la confianza digital de la ciudadanía y fortalecer la articulación de los ámbitos que integran el Marco de Confianza Digital, estas conductas abarcan el fortalecimiento de la seguridad digital en las entidades públicas, las organizaciones de la sociedad civil, ciudadanía, empresas y academia, así como la promoción de la participación activa de los

diferentes actores de nuestra ciudadanía y la permanente colaboración y articulación entre las autoridades a cargo de la protección y defensa de los consumidores, la protección de los datos personales y el seguridad Digital.

Así, el artículo 4 del mencionado Decreto de Urgencia establece que el Marco de Confianza Digital está constituido por tres (03) ámbitos:

a) **Seguridad Digital**, el cual es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la SGTD.
b) **Protección de datos personales y transparencia**, el cual es dirigido, supervisado y evaluado por la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos (MINJUSDH).
c) **Protección del consumidor,** el cual es dirigido, supervisado y evaluado por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

Asimismo, se establece que la Presidencia del Consejo de Ministros, a través de la SGTD, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos. De acuerdo con el artículo 6 del Decreto de Urgencia N° 007-2020, la SGTD, tiene competencias para formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento, así como 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.

En ese marco, la Primera Disposición Complementaria Final del Decreto de Urgencia N° 007-2020 establece que el Poder Ejecutivo elabora y aprueba el reglamento dentro de los noventa (90) días hábiles siguientes a la entrada en vigor del Decreto de Urgencia referido, el cual será publicado mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

Por otro lado, el Perú tomó la decisión de adherirse al Convenio de Budapest o Convenio contra la Ciberdelincuencia mediante Resolución Legislativa N° 30913, Resolución Legislativa que aprueba el Convenio sobre 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 firmantes[1].

Con relación a lo señalado, la SGTD dispuso la investigación y análisis en materia de confianza digital a cargo de la Subsecretaría de Política y Regulación Digital a fin de elaborar el proyecto de Reglamento del Decreto de Urgencia N° 007-2020. Posteriormente, a través de la plataforma Participa Perú, se recibieron comentarios y aportes de la ciudadanía hasta el 19 de abril de 2023.

En base a los insumos recibidos por parte de la ciudadanía, así como los aportes recibidos de la Subsecretaría de Tecnologías y Seguridad Digital, la Subsecretaría de Servicios e Innovación Digital de la Secretaría de Gobierno y Transformación Digital, la Dirección General

[1] El documento en detalle se ubica en https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del MINJUSDH e INDECOPI se ha permitido actualizar y mejorar la propuesta normativa.

II. MARCO JURÍDICO QUE HABILITA LA PROPUESTA NORMATIVA

a) La Constitución Política del Perú señala en su artículo 14 y en el numeral 4 de su artículo 2 que el Estado promueve el desarrollo científico y tecnológico del país y el uso de las tecnologías de la información y la comunicación, respectivamente. Asimismo, de acuerdo con su artículo 44, es deber primordial del Estado garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad, y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.
b) El inciso 6 del artículo 2 de la Constitución Política del Perú establece el derecho de los ciudadanos a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
c) El artículo 58 de la Constitución Política del Perú, la cual establece que la iniciativa privada es libre, y se ejerce en una economía social de mercado, además de señalar que el Estado orienta el desarrollo del país y actual en área de promoción de empleo, salud, educación, seguridad, servicios públicos e infraestructura.
d) El artículo 65 de la Constitución Política del Perú, señala que el Estado defiende el interés de los consumidores y usuarios, para tal efecto garantiza el derecho a la información sobre los bienes y servicios que se encuentra a su disposición en el mercado.
e) La Política 35 del Acuerdo Nacional, sobre Sociedad de la Información y Sociedad del Conocimiento señala en su literal b) que el Estado fomentará el pleno ejercicio y respeto de los Derechos Humanos en todo entorno digital. Además, en su literal h) que el Estado fomentará el uso transversal de las TIC en ámbitos tales como educación, salud, conservación del ambiente, seguridad ciudadana, prevención de riesgo de desastres, gobierno abierto, defensa nacional, innovación, investigación, transferencia de conocimiento y sectores productivos y sociales.
f) El Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno. Asimismo, en su artículo 8 establece que la Presidencia del Consejo de Ministros, a través de la SGTD, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad y arquitectura digital.
g) De igual manera, el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, establece que la Presidencia del Consejo de Ministros, a través de la SGTD, es el ente rector del Sistema Nacional de Transformación Digital, constituyéndose en la autoridad técnico-normativa a nivel nacional sobre la materia, el cual tiene como finalidades impulsar la innovación digital, el fortalecimientos de una sociedad digital inclusiva y el ejercicio de una ciudadanía digital con deberes y derechos digitales de los ciudadanos, así como fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital

fomentando la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital para la sostenibilidad, prosperidad y bienestar social y económico del país. Asimismo, de acuerdo con su artículo 4 el Sistema Nacional de Transformación Digital abarca de manera no limitativa, las materias de gobierno digital, economía digital, conectividad digital, educación digital, tecnologías digitales, innovación digital, servicios digitales, sociedad digital, ciudadanía e inclusión digital y confianza digital.

h) Asimismo, el Decreto de Urgencia Nº 007-2020, establece en su artículo 12 que 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.
i) El Decreto Supremo N° 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030, y establece como Objetivo Prioritario 5 "*Consolidar la seguridad y confianza digital en la sociedad*"; y, por ende, se hace hincapié en que, debido a la consolidación del proceso de transformación digital del país, las amenazas y riesgos se hacen también cada vez mayores, sin embargo, ello no puede representar una limitante para la interacción de la ciudadanía en el entorno digital.
j) El Decreto Supremo N° 255-2019-EF, que aprueba la Política Nacional de Inclusión Financiera y modifica el Decreto Supremo N° 029-2014-EF, que crea la Comisión Multisectorial de Inclusión Financiera, que busca promover y facilitar el proceso de inclusión financiera mediante la ejecución de acciones coordinadas que permitan un mayor acceso y uso responsable de servicios financieros de calidad. En este sentido, se busca que los servicios financieros resulten confiables, innovadores, accesibles y adecuados a las necesidades de la ciudadanía, con el fin de contribuir al desarrollo y estabilidad económica. Para ello, se determinó como Objetivo Prioritario 4 (OP4), que el Estado se compromete a "*Desarrollar infraestructura de telecomunicaciones y plataformas digitales para incrementar la cobertura de servicios financieros*", lo cual requiere de una regulación clara en las materias de economía digital, educación digital, tecnologías digitales, servicios digitales, seguridad digital y confianza digital, todas ellas objeto del Sistema Nacional de Transformación Digital.
k) El artículo 79 del Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Resolución Ministerial N° 224-2023-PCM, refiere que la SGTD es el órgano de línea con autoridad técnica normativa a nivel nacional responsable de proponer, articular, implementar, desarrollar, brindar asistencia técnica, supervisar y evaluar la Política Nacional de Transformación Digital y su estrategia, las políticas nacionales, planes nacionales, normas, lineamientos, estrategias, proyectos, plataformas y agendas digitales. Así, ejerce la rectoría del Sistema Nacional de Transformación Digital, el cual abarca las materias de tecnologías digitales, sociedad digital, talento digital, educación digital, seguridad digital, entre otras.

Los dispositivos constitucionales y legales antes enunciados nos permiten determinar que a la fecha existe un marco normativo que establece la rectoría de la SGTD como autoridad técnico normativa a nivel nacional sobre la confianza digital. Asimismo, existe un marco normativo que regula la seguridad digital en el país, entendiéndola como el estado de

confianza que aspiramos alcanzar en el entorno digital o ciberespacio, que nos permite ejercer nuestros derechos con seguridad, y gestionar la información de manera confiable.

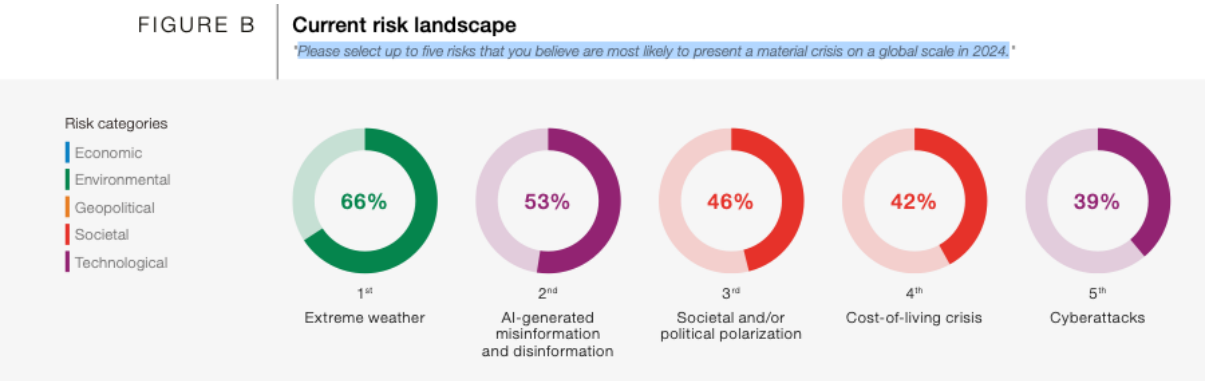
Contar con una norma con rango de Ley que establece un marco de articulación acorde con las necesidades y demandas de la transformación digital y uso de tecnologías digitales representa un avance significativo para nuestro país, el cual, al igual que otros países como, Reino Unido, Estados Unidos, Dinamarca, Estonia, incluyendo los de nuestra región (Colombia, Brasil, Uruguay y Chile) ha advertido esta necesidad. Frente a ello, es importante continuar con los esfuerzos de reglamentar el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, a fin de contar con un marco que sea suficiente para generar, asegurar y mantener la confianza en los entornos digitales.

III. FUNDAMENTO TÉCNICO DE LA PROPUESTA NORMATIVA

3.1. Análisis del estado situacional

3.1.1 Contexto Internacional

Es importante mencionar que el Foro Económico Mundial (FEM) señala en su "Informe Global de Riesgos 2024"[2] (Global Risk Report) que entre los cinco (05) riesgos con mayor probabilidad de presentar una crisis a gran escala se encuentran los **ciberataques**, y en segundo lugar la información falsa y la desinformación motivada por la inteligencia artificial.



Así, también se menciona en el reporte que, entre los 10 principales riesgos globales clasificados en corto y largo plazo, se encuentra la inseguridad digital o los ciberataques.

[2] Ver: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

FIGURE C

Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

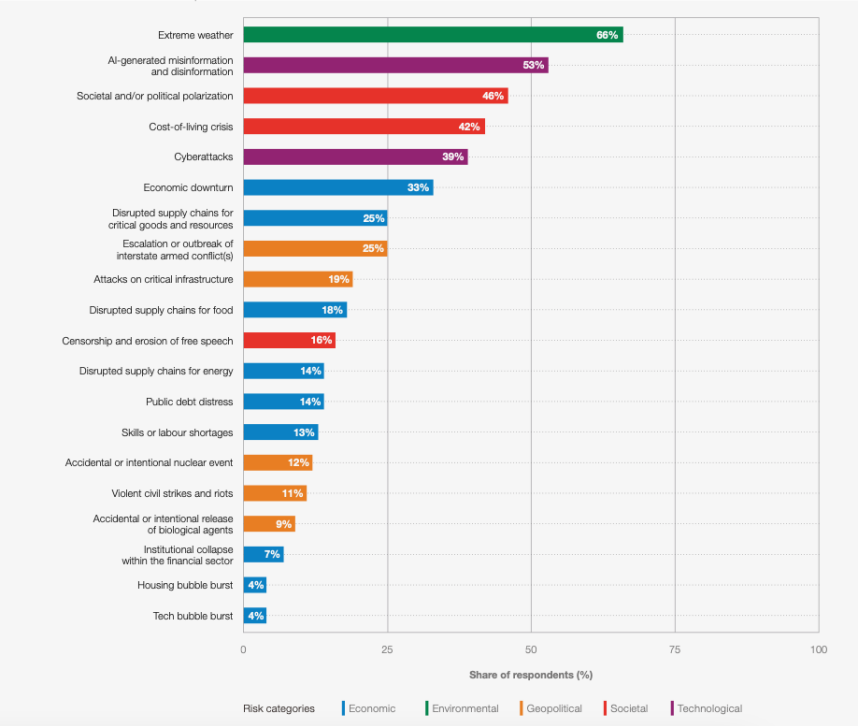
Source
World Economic Forum Global Risks Perception Survey 2023-2024.

Los ataques a las infraestructuras críticas nacionales son también considerados como un riesgo con probabilidad de presentar una crisis nacional.

FIGURE 1.2

Current risk landscape

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."



Conforme se advierte del Informe Global de Riesgos, el panorama internacional permite advertir que los ciberataques representan una probabilidad alta que genere un caos a nivel nacional, siendo importante establecer medidas que permitan garantizar la seguridad digital del país.

3.1.2 Reportes de ciberataques en el Perú

Conforme se mencionó en la Exposición de Motivos del Decreto de Urgencia N° 007-2020, el avance de las tecnologías digitales es exponencial, y en medio de ese 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 vigente aún continúa siendo insuficiente y revela la necesidad de emitir disposiciones que precisen el marco regulatorio, los actores intervinientes y las acciones que pueden realizar, siendo uno de estos dispositivos el reglamento del Decreto de Urgencia N° 007-2020.

Los ciberataques afectan la credibilidad y confianza de un país, impacta en la competitividad, la productividad, las condiciones para hacer negocios, 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, y hacen seguimiento a las víctimas rastreándolas maliciosamente. Por ello, al existir estos riesgos, se hace necesario establecer un marco regulatorio cuyo fin primario sea salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital, 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 seguridad, incluyendo aquellas que provienen por agentes perjudiciales en el referido entorno digital. Si bien la aprobación de la Ley de Gobierno Digital constituye un gran paso para este objetivo, el gobierno digital solo implica acciones al interior del Estado, lo cual resulta insuficiente. Para ello, la propuesta normativa establece disposiciones que promueven la articulación público privada con la finalidad de garantizar un desarrollo sostenible. Los cuales se sujetan a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas[3] y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables.

Según el informe de ESET 2022[4], el **Perú aparece liderando como uno de los países con mayor número de ataques de la región**. Seguido de México (17%), Argentina (11%) y Ecuador (9%). Así también, se muestra el resultado sobre el “spyware” que se encuentra relacionada al robo de datos y espionaje, siendo el Perú el país más afectado por la categoría de códigos maliciosos (40%).

En esta misma línea, según Kaspersky se señala que en el año 2023 se registraron al menos 9.6 millones de intentos de ataques de software maliciosos dirigidos a pequeñas y medianas empresas en el Perú[5].

3.2. Identificación del problema público

[3] El texto en su detalle se ubica en https://www.un.org/es/charter-united-nations/index.html
[4] Ver: https://web-assets.esetstatic.com/wls/2022/07/ESET-security-report-LATAM-2022.pdf
[5] Ver: https://gestion.pe/tecnologia/pymes-fueron-las-mas-afectadas-por-ciberataques-en-el-2023-por-que-empresas-peruanas-emprendimientos-negocios-noticia/

La pandemia de la COVID-19 ha permitido que el avance de las tecnologías digitales ascienda exponencialmente y su uso se globalice, por lo que su implementación se ha convertido en una pieza fundamental para el funcionamiento de nuestra sociedad y para la integración en la economía de las empresas, independientemente del tamaño y rubro en el que estas se desempeñen. En consecuencia, las redes como el internet y las infraestructuras de comunicaciones son cada vez más utilizadas de forma intensiva para el desarrollo de actividades productivas, educacionales, de la salud, entre otras, logrando su evolución, y en algunos casos su completa digitalización; ello coadyuva al fortaleciendo del ecosistema digital y el desarrollo de una economía digital en nuestro país.

Actualmente las entidades públicas y organizaciones del sector privado vienen haciendo un uso intensivo de las tecnologías para digitalizar sus procesos y servicios. Es así que, para el caso del comercio electrónico, una de las formas más utilizadas para realizar la compra y venta de productos y servicios, se ha incrementado debido al aumento de compradores online que pasó de 6 a 11.8 millones solo en el año 2020.

	Pre Cuarentena (Enero 2020)	Durante (Julio 2020)	Total Cierre 2020
Penetración del Ecommerce en el consumo a través de tarjeta	12.5%	45%	35%
Crecimiento del ecommerce (YTY)	43%	160%	50%
Compradores Online	6 millones	8.9 millones	11.8 millones
Ticket promedio	S/171	S/231	S/141
Penetración del ecommerce sobre el total del comercio	1.5%	3.5%	5%
N° de negocios que venden online	65,800	131,600	263,200
Penetración Ecommerce sobre el retail	2.8%	6%	8%

Fuente: CAPECE, Niubiz, Payu, Alignet

En ese contexto, si bien el uso de las tecnologías digitales trae múltiples beneficios para la sociedad puesto que permiten, entre otros, mejorar la prestación de servicios o generar nuevos, también pueden traer desventajas relacionadas con la seguridad o privacidad. Así, uno de los problemas más recurrentes en el entorno digital son la poca implementación de medidas de seguridad digital y protección de la identidad de los compradores online, dicha situación conlleva al crecimiento de los ciberataques, el robo de datos personales, los delitos contra niños y adolescentes, suplantación de identidad, ingeniería social, entre otros delitos en Internet. Lo que ha ocasionado pérdidas económicas tanto en el sector público como en el sector privado y, sobre todo, ha afectado a millones de ciudadanos, generando desconfianza en el entorno digital.

Según un estudio de la firma de ciberseguridad Fortinet[6], el Perú ha sufrido más de 11.500 millones de intentos de ciberataques en el año 2021, 15.000 millones en el 2022[7] y 5.000

[6] Disponible en https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021

7 https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

millones en 2023[8]. Por ello, podemos señalar que nuestro país es por defecto un objetivo de ciberataques, lo que evidencia la insuficiencia de capacidades, organización y compromiso por incrementar los niveles de seguridad de la información en las organizaciones, así como la falta de compromiso con la necesidad de mantener un entorno digital seguro por parte de quienes promueven precisamente estos ataques.

Adicionalmente, es preciso señalar que entre enero y abril del 2021[9], se investigaron 1,188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú, y, entre enero y abril del 2024 el Registro de Identificación y Estado Civil (Reniec) anunció haber bloqueado más de 4.6 millones de ataques a su sistema de datos y diversas fuentes de información[10]. Los casos más frecuentes están relacionados al fraude informático y a la suplantación de identidad. Asimismo, de acuerdo con la información pública, el total de denuncias entre enero y agosto del 2024 se disgrega de la siguiente manera: Fraude informático (19.067), suplantación de identidad (6.196), acceso ilícito (724), fraude informático agravado (706) entre otros que en conjunto sumaban más de 1.000 denuncias solo en los primeros cuatro meses del año pasado[11].

En el entorno digital, como se viene explicando, uno de los factores vulnerables ante la falta de implementación de medidas de seguridad digital es el de la privacidad, los datos personales y la afectación del derecho a la autodeterminación informativa de las personas, la cual consiste en la capacidad de decisión y control por parte de la persona, como titular sobre sus datos personales, sobre el tratamiento de estos, aun cuando sean cedidos voluntariamente a las organizaciones titulares de aplicaciones de uso comunicacional, dispuestas para satisfacer distintas finalidades entre las que se encuentran laborales, educativas, o de cualquier otro tipo.

A causa de tal derecho y en el mencionado contexto del entorno digital que conlleva a un mayor uso de aplicaciones, sistemas, etc., se exige a los titulares de los bancos de datos personales que realizan tratamiento de datos personales eviten incurrir en incidentes de seguridad digital que perjudiquen los intereses de las personas, tales como el control sobre sus datos personales, su privacidad y el funcionamiento de la aplicación para su satisfacción. Con dicha exigencia, se contribuye a cumplir con la expectativa que se tiene respecto del uso de los datos personales cedidos: que dicho uso esté encaminado exclusivamente para la finalidad que fueron recabados y respetando la proporcionalidad de los datos.

La mencionada exigencia se traduce en la implementación obligatoria de medidas de seguridad por parte de las organizaciones, cuyo objetivo es evitar situaciones tales como la exposición no autorizada de los datos, el acceso a ellos por entes no autorizados o desconocidos, o su modificación o destrucción, preservando los tres pilares de gestión de la seguridad de la información: confidencialidad, disponibilidad e integridad.

En el Perú, la Ley N° 29733, Ley de Protección de Datos Personales, desarrolla tal obligación a través del principio de seguridad, establecido en su artículo 9 y complementariamente por

8 https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet

9 Disponible en: https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

10 https://www.gob.pe/institucion/reniec/noticias/940402-reniec-bloqueo-4-6-millones-de-ciberataques-en-lo-que-va-del-2024

11 https://ebiz.pe/noticias/el-alto-costo-de-la-cibercriminalidad-un-especial-de-ebiz-noticias/

medio del artículo 16. En virtud de tales disposiciones, las organizaciones que manejen datos personales deben evitar los riesgos e incidentes mencionados, adoptando medidas organizativas, legales y técnicas aplicables a todos los procesos de tratamiento de tales datos, involucrando no solo a especialistas de una determinada área, sino a la totalidad de la organización, desarrollando con ello una adecuada cultura de seguridad de la información.

Por otro lado, desde la perspectiva del consumidor, la adquisición de bienes y servicios a través de canales digitales permitió a las empresas seguir operando y reactivarse económicamente; no obstante, ello ha presentado algunas deficiencias que ha provocado el malestar de los consumidores.

Ante ello, en el año 2020, el INDECOPI pasó de tener 15 600 reportes, entre quejas y reclamos en junio a tener 60.000 en el mes de agosto del mismo año; siendo la demora en la entrega de productos una de las infracciones más frecuentes[12]. Asimismo, conforme lo señalado por la Autoridad Nacional de Protección del Consumidor del INDECOPI, las quejas más frecuentes de los consumidores relacionadas con compras en línea –comercio electrónico-, están vinculadas a la falta de entrega y/o la demora en la entrega de productos, errores en la entrega de un producto, productos defectuosos o incompletos, falta de reembolso del dinero pagado, cancelación del pedido sin previo aviso y los **cargos que no han sido aceptados por el consumidor**.

En ese sentido, al existir riesgos en el entorno digital, se hace necesario desarrollar a mayor detalle el marco regulatorio existente con el fin primario de salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital, 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 seguridad, incluyendo aquellas que provienen por agentes perjudiciales en el referido entorno digital.

3.3. Identificación de los objetivos relacionados con el problema público

La propuesta normativa busca lograr los siguientes objetivos:

a) Mejorar las condiciones que garanticen que las interacciones digitales de las personas con los servicios digitales prestados por las entidades públicas y organizaciones del sector privado en el territorio nacional se desarrollen de forma veraz, predecible, ética, proactiva, transparente, segura, inclusiva y confiable.
b) Garantizar el respeto de los derechos humanos, un uso y desarrollo seguro, sostenible, ético, transparente, responsable de las tecnologías digitales en favor del desarrollo económico y social del país.
c) Promover medidas en las organizaciones que permitan brindar la confianza a sus usuarios o consumidores finales, mediante mecanismos que ayuden a prevenir cualquier vulneración a los trámites digitales que realizan.
d) Fortalecer el marco institucional y la gobernanza de la seguridad digital en favor del desarrollo económico y social del país.

12 https://www.ecommercenews.pe/comercio-electronico/2020/indecopi-reclamos-ecommerce.html/

3.4. Análisis sobre la necesidad, viabilidad y oportunidad de la propuesta normativa

Con relación a la viabilidad, necesidad y oportunidad de la propuesta normativa se analiza lo siguiente:

- **Viabilidad política**, entendida como la consistencia de la propuesta normativa con las Políticas Nacionales. Al respecto, en la sección VI del presente Documento se desarrolla la vinculación de la propuesta con las políticas nacionales vigentes.

- **Viabilidad legal y administrativa**, que se refiere a la capacidad de gestión de la SGTD para implementar la propuesta normativa, para lo cual se realizará las gestiones necesarias para su viabilidad administrativa y se cuenta con los recursos necesarios; así como, la coherencia normativa se desarrolla en la sección VI del presente Documento.

- **Viabilidad de recursos,** conforme se establece en la sección V del presente documento, la propuesta regulatoria no genera gastos adicionales al tesoro público, se implementa con los recursos asignados a las entidades involucradas.

- **Necesidad y oportunidad de la propuesta normativa,** debido a la dación del Decreto de Urgencia N° 007-2020, que crea el Marco de Confianza Digital y establece medidas para su fortalecimiento, la misma que en su primera disposición complementaria final estableció un plazo de noventa (90) días hábiles, luego de la entrada en vigencia de dicha norma, para aprobar el reglamento del Decreto Supremo.
  Asimismo, en el Reglamento del Decreto Legislativo 1412, aprobado por Decreto Supremo N° 029-2021-PCM, se suele hacer mención al Decreto de Urgencia N° 007-2020 y su reglamento como las normas que establecerán las condiciones bajo las cuales se diseñarán, implementarán y prestarán los servicios brindados por los Proveedores de Servicios Digitales, remisiones que pueden advertirse en los artículos 25 (proveedores de servicios digitales), 68 (roles para la gobernanza y gestión de datos), 96 (modelo de seguridad digital), 102 (articulación de los ámbitos), 107 (referido a la comunicación de incidentes), 110 (gestión de riesgos de seguridad digital) y 114 (seguridad de los servicios digitales).

3.5. Nuevo estado pretendido

El presente reglamento realiza precisiones sobre el marco regulatorio vigente, con la finalidad de que estas disposiciones viabilicen la aplicación de lo dispuesto en el Decreto de Urgencia N° 007-2020, generando eficiencia en el sector público y privado a través de la digitalización de los servicios y la creación de entornos digitales seguros para aquellas personas que se desenvuelvan, ejerciendo su ciudadanía digital, en dicho ecosistema. Permitiéndoseles realizar trámites con entidades públicas y privadas, operaciones financieras, entre otros, aumentando la eficiencia tanto del sector público como del sector privado.

Además, se realizan precisiones sobre la forma en la que el Centro Nacional de Seguridad Digital, concebido en el Decreto de Urgencia N° 007-2020 como una plataforma digital, cumplirá con sus funciones y campos de acción asignados.

Finalmente, se precisa que se incluyen disposiciones que reafirman la facultad de regular por parte de la Secretaría de Gobierno y Transformación Digital en materia de Confianza Digital así como de aprobar un plan anual de operaciones del Centro Nacional de Seguridad Digital.

IV. CONTENIDO DE LA PROPUESTA NORMATIVA

El Decreto de Urgencia N° 007-2020 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. El presente Reglamento desarrolla las disposiciones normativas del citado Decreto de Urgencia.

4.1 Título Preliminar: Disposiciones Generales

El Título Preliminar establece el objeto de la norma, el cual está enmarcado en lo dispuesto en el Decreto de Urgencia N° 007-2020, además de su finalidad y principios; asimismo, se establece el ámbito de aplicación 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 del sector privado, la sociedad civil, la academia y ciudadanía en general, que integran el Sistema Nacional de Transformación Digital conforme lo previsto en el Decreto de Urgencia N° 006-2020.

La confianza en el entorno digital se ha convertido en uno de los factores clave en los que se sustenta las relaciones económicas y sociales en las sociedades, ya que cuanto más aumenta el involucramiento de las personas mayor es el riesgo que pueda generarles daños económicos o de su privacidad. Por ello, la confianza digital se convierte en un componente de la transformación digital en el país, siendo importante que el Estado, las entidades públicas y privadas, y la sociedad civil desarrollan un papel estratégico a fin de fomentar el desarrollo digital en un entorno confiable.

En ese sentido, el Poder Ejecutivo, mediante el presente Reglamento, regula el Marco de Confianza Digital para promover 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, además de reafirmar la facultad de la Secretaría de Gobierno y Transformación Digital para establecer los protocolos y lineamientos, y regular en esta materia en su calidad de ente rector.

Además, en este extremo se señala que el ámbito de aplicación de la norma alcanza a las entidades comprendidas en el artículo I del Título Preliminar del Texto único ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General aprobado por el Decreto Supremo Nº 004-2019-JUS, las empresas del Estado que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) y las empresas públicas de los gobiernos regionales y locales, además de las

organizaciones de la sociedad civil, ciudadanos, empresas y la academia que integran el Sistema Nacional de Transformación Digital en lo que corresponda y establezca el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

Así, dicho Título incorpora los principios que rigen el Marco de Confianza Digital: colaboración y cooperación, gestión de riesgos, integridad, privacidad y seguridad desde el diseño, recuperación y resiliencia digital, respeto de los derechos humanos, responsabilidad y transparencia.

Así también, en el artículo IV se desarrollan los acrónimos de algunas palabras contenidas en la propuesta normativa, que permiten facilitar su lectura y comprensión de las disposiciones reguladas.

4.2 Título I: Confianza Digital

De acuerdo a lo señalado el Decreto de Urgencia N° 006-2020, la Confianza Digital es una de las materias de articulación de los sectores públicos y privados; en ese marco, la Confianza Digital fue desarrollada en el Decreto de Urgencia N° 007-2020, precisándose que esta abarcaba tres ámbitos: la protección de datos personales y transparencia, la protección del consumidor y la seguridad digital.

El Título I del presente Reglamento desarrolla la Confianza Digital, el que a su vez se subdivide en dos (2) Capítulos. Por un lado, el Capítulo I que regula el Marco de Confianza Digital, donde se abordan aspectos sobre la rectoría del Marco de Confianza Digital, recayendo este sobre la Presidencia del Consejo de Ministros, a través de la SGTD. En esta línea, se desarrolla las atribuciones que tiene el ente rector, entre las que se encuentran: promover una cultura de confianza digital en la ciudadanía y fortalecer el desarrollo de capacidades y competencias en materia de confianza digital en el marco del impulso del talento digital en el país.

Asimismo, se precisa que las acciones de las entidades señaladas en el numeral 9.1. del artículo 9 del Decreto de Urgencia, es decir, las entidades de la administración pública, proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud, transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, se orientan a fortalecer la continuidad, disponibilidad y resiliencia frente a incidentes de seguridad digital, accidentales o intencionadas en los procesos y servicios digitales.

El desarrollo del marco de confianza digital responde a una de las principales necesidades urgentes que se deben de atender para el desarrollo de la Transformación Digital en el país, y que fue identificada mediante la "Encuesta Nacional de Satisfacción Ciudadana a nivel regional 2021"[13], realizada a pedido de la Presidencia del Consejo de Ministros a través de la Secretaría de Gestión Pública, en donde se obtuvo lo siguiente:

[13] Presentación de los resultado de la encuesta en el siguiente enlace: https://cdn.www.gob.pe/uploads/document/file/3792943/Encuesta%20Regional%202021.pdf.pdf?v=1666800634

Confianza en el Estado Peruano	El 68% de los encuestados “solo confía” en el Estado Peruano mientras el 10% “confía mucho”. El 29% considera que el motivo de desconfianza es porque no es seguro y hay estafas.
Trámites a través de página web y/o aplicaciones de entidades públicas	8 de cada 10 personas no ha realizado trámites de manera virtual en entidades públicas durante período de pandemia de la COVID-19. 5% ha realizado algún trámite a través de la página web y/o aplicaciones de entidades públicas
Razón principal por la que no han realizado trámites	19% indica que no es seguro y pueden filtrarse datos personales

Fuente: Encuesta Nacional de Satisfacción Ciudadana a nivel regional 2021(Elaboración propia)

Por su parte OCDE, en su informe sobre la “Perspectivas económicas de América Latina 2019: Desarrollo en transición”[14], menciona en uno de sus párrafos lo siguiente:

> *«(…) El acceso a las **tecnologías digitales** también sigue siendo un reto, pues **apenas 57% de los latinoamericanos tienen acceso a Internet**. Además, alrededor de 40% de los latinoamericanos están en riesgo de regresar a la condición de pobreza y tienen empleos informales y una protección social deficiente. Por otra parte, **cerca de 64% de la población no tiene confianza en sus gobiernos nacionales**. (…)» (énfasis añadido)*.

En el mismo informe, se hace referencia a que **todo país en vías de desarrollo**, atraviesa por algunos obstáculos (**riesgos potenciales**) que se deben de identificar y superar para no limitar su capacidad de alcanzar mayores grados de desarrollo. Uno de estos cuatro **principales “nuevos” obstáculos del desarrollo** es el siguiente:

> *«(…)*
> ***Institucional**: La expansión de la clase media vino acompañada de mayores expectativas y aspiraciones sociales. Pese a los avances de años anteriores, **las instituciones aún no logran responder a las crecientes exigencias de los ciudadanos. La desconfianza y la poca satisfacción se están***

[14] OCDE et al. (2019), Perspectivas económicas de América Latina 2019: Desarrollo en transición, OECD Publishing, Paris, https://doi.org/10.1787/g2g9ff1a-es

> ***agravando**. Esto lleva a que los ciudadanos den menor valor a cumplir con sus obligaciones sociales, como la de pagar impuestos. Esto, a su vez, dificulta la recaudación de ingresos tributarios para financiar mejores servicios públicos y responder a las exigencias de la sociedad. (…)» (énfasis añadido)*

Por otro lado, se complementan definiciones que resultan de suma relevancia para el desarrollo del Reglamento en la medida que las obligaciones establecidas en la propuesta normativa se aplican a los Proveedores de Servicios Digitales (PSD) además, conforme podrá advertirse en la misma norma, se desarrollan obligaciones que impliquen la coordinación entre los PSD y los terceros que les brinden servicios

Asimismo, se debe tener presente que los PSD independientemente del sector y localización geográfica donde se desempeñen son responsables por el diseño, prestación y/o acceso a los servicios digitales que se brindan en el territorio nacional, los cuales ponen a disposición de los ciudadanos o consumidores finales. Así, el cumplimiento de las disposiciones contenidas en el Decreto de Urgencia N° 007-2020 y en la propuesta normativa no los exonera de la observancia de las obligaciones establecidas en las normas especiales de los ámbitos que integran el Marco de Confianza Digital.

Además, es necesario mencionar la relevancia que, en este caso asume la Subsecretaría de Tecnologías y Seguridad Digital en la implementación y el desarrollo de las disposiciones establecidas en el Decreto de Urgencia N° 007-2020 y el presente reglamento, asumiendo el rol de gestionar y administrar el funcionamiento del Centro Nacional de Seguridad Digital y las plataformas que, a su vez, se deriven de estas disposiciones y del Reglamento de Organización y Funciones de la PCM, aprobado por Resolución Ministerial N° 224-2023-PCM.

De otro lado, el Capítulo II del Título I del presente Reglamento regula sobre los ámbitos del marco de confianza digital, que comprende los ámbitos de seguridad digital, protección al consumidor, y protección de datos personales y transparencia, y que se necesita desplegar esfuerzos de articulación entre los actores competentes en las acciones, políticas, estrategias, instrumentos, lineamientos y planes necesarios para fortalecer la confianza digital en el país. Dicha articulación se realiza bajo el enfoque de múltiples partes interesadas y conforme con los mecanismos de articulación previstos para el Sistema Nacional de Transformación Digital.

Asimismo, de conformidad con lo previsto en el artículo 4 del Decreto de Urgencia N° 007-2020, y el artículo 7 del presente Reglamento, cabe precisar que el MINJUSDH y el INDECOPI cumplen funciones rectoras en materia de protección de datos personales y de protección al consumidor, respectivamente, conforme a lo siguiente:

<u>Ámbito de protección de datos personales y transparencia</u>

En el ámbito nacional, la Constitución Política del Perú, en el inciso 6 de su artículo 2, dispone que toda persona tiene derecho a que los servicios informáticos, computarizados o no públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

En el afán de lograr una adecuada tutela de este derecho constitucional, en el año 2011, se publicó la Ley Nº 29733, Ley de Protección de Datos Personales en la que, además de desarrollarse las garantías vinculadas a este derecho, también se creó la Autoridad Nacional de Protección de Datos Personales, ejercida por el MINJUSDH a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Además, en el año 2013, se aprueba su Reglamento, por Decreto Supremo N° 013-2013-JUS.

La Autoridad Nacional de Protección de Datos Personales tiene funciones orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras a efectos de garantizar el cumplimiento del objeto de la Ley N° 29733 y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS. También tiene a su cargo el Registro Nacional de Protección de Datos Personales, en el que las personas naturales, entidades públicas y privadas inscriben los bancos de datos personales que administran.

Por ello, el inciso b) del artículo 4 del Decreto de Urgencia N° 007-2020, señala que el ámbito de Protección de Datos Personales y Transparencia, es dirigido, supervisado y evaluado por la Autoridad Nacional de Protección de Datos Personales del MINJUSDH. Conforme a ello, a fin de fortalecer la confianza digital, cuando los proveedores de servicios digitales traten datos personales, dicho ámbito ya se encuentra desarrollado de acuerdo al marco legal existente en materia de protección de datos personales, y que es supervisado y fiscalizado por el MINJUSDH.

Así también, la SGTD, en su calidad de ente rector del Marco de Confianza Digital en el país, brinda asistencia y acompañamiento técnico al MINJUSDH, para el cumplimiento de sus funciones y desarrollo de acciones conjuntas para el diseño de campañas de difusión que involucren la materia de protección de datos personales en el entorno digital, y propondrán protocolos de colaboración e intercambio de información sobre notificaciones de incidentes de seguridad digital cuando estos involucren datos personales.

Ámbito de protección de protección al consumidor

Los artículos 58 y 65 de la Constitución Política del Perú, establecen una economía social de mercado, resaltando la defensa de los derechos de los consumidores y usuarios. Así, se destaca la defensa de los intereses de los consumidores y usuarios, garantizando el derecho a la información de los bienes y servicios disponibles y velando por la salud y la seguridad de la población.

En línea con lo anterior, la Ley N° 29571, que aprueba el Código de Protección y Defensa del Consumidor (en adelante, el Código), instituye que la protección de los derechos de los consumidores constituye un principio rector de la política social y económica del Estado y que dichas políticas deben ser transversales con la finalidad que involucren a todos los poderes públicos y a la sociedad. Además, establece como finalidad que los consumidores accedan a productos y servicios idóneos y gocen de los derechos y mecanismos efectivos para su protección, reduciendo la asimetría

informativa, corrigiendo, previniendo o eliminando las conductas y prácticas que afecten sus legítimos intereses.

Así mismo, el Código estableció que el INDECOPI es la autoridad con competencia primaria y de alcance nacional para conocer presuntas infracciones a las disposiciones en materia de consumo, así como para interponer las sanciones y medidas correctivas que correspondan.

En este sentido, el inciso c) del artículo 4 del Decreto de Urgencia N° 007-2020, señala que el ámbito de protección al consumidor, es dirigido, supervisado y evaluado por el INDECOPI. Conforme a ello, a fin de fortalecer la confianza digital, cuando se adviertan hechos que podrían constituir una presunta afectación a los intereses de los consumidores en el marco de una relación de consumo con proveedores de servicios digitales, serán aplicables las disposiciones de protección del consumidor establecidos en el Código, siendo en esos casos el Indecopi la entidad encargada de supervisar y fiscalizar estos hechos.

De esta forma, a fin de establecer en el Reglamento disposiciones que permitan la articulación entre los ámbitos del Marco de Confianza Digital, se han incluido artículos específicos que establecen el desarrollo de acciones conjuntas para el diseño de campañas de difusión que involucren la materia de protección de datos personales y protección al consumidor en el entorno digital, así como el apoyo y asesoramiento técnico a dichos ámbitos.

Ámbito de seguridad digital

La propuesta normativa reafirma que la SGTD es el ente rector en materia de seguridad digital en el país. Asimismo, dirige, evalúa, promueve, orienta, articula y supervisa su operación y correcto funcionamiento.

De igual forma se precisa que la SGTD es la encargada de coordinar y promover actividades de concientización en las que se promueva el desarrollo del ámbito de seguridad digital y el Marco de Confianza Digital.

4.3 Título II: Seguridad Digital

En el presente Título se desarrollan cinco (05) Capítulos. En el Capítulo I sobre medidas para la seguridad digital en la administración pública, se establece que para las entidades de la Administración Pública las disposiciones de seguridad digital establecidas en el Marco de Confianza Digital se articulan conforme con lo en el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y su Reglamento, aprobado por Decreto Supremo N° 029-2021-PCM, el mismo que, dicho sea de paso, hace remisiones en sus disposiciones a la reglamentación del Decreto de Urgencia N° 007-2020. Dichas disposiciones son de obligatorio cumplimiento para fortalecer la confianza digital de la ciudadanía.

Asimismo, respecto a las actividades críticas y funciones críticas, en el artículo 8.3 se señala que la SGTD es la encargada de elaborar y aprobar la lista que clasifica a las mismas, labor que ejercerá a través de la emisión de Resoluciones de Secretaría de Gobierno y Transformación Digital; al respecto, dicha labor tiene su sustento en el numeral 9.3 del artículo 9 del Decreto Legislativo N° 1412 señala que la SGTD tiene facultades para elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital. Así como en el inciso b) del artículo 6 del Decreto de Urgencia N° 007-2020 establece que la SGTD emite lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de confianza digital.

Asimismo, en el Capítulo II, se hace mención expresa a las medidas para la seguridad digital en las entidades del sector privado, lo cual se circunscribe a aquellas que presten sus servicios en un entorno digital, siendo de carácter orientador y referencial en cuanto le genere valor para los objetivos estratégicos de negocio, salvo aquellas que presente los servicios señalados en el numeral 9.1 del Decreto de Urgencia N° 007-2020.

En los artículos siguientes se desarrollan recomendaciones para la gestión de riesgos de seguridad digital para las actividades críticas, resiliencia de las actividades críticas, desarrollo de alianzas sostenibles para asegurar la cooperación ante la gestión de riesgos de seguridad digital de actividades críticas.

Por otro lado, en el marco de la gestión de riesgos de seguridad digital se establece que tanto las entidades públicas como las privadas, alcanzadas por el numeral 9.1 del artículo 9 del Decreto de Urgencia N° 007-2020, implementen el proceso de gestión de riesgos de seguridad digital, el cual está integrado a la gestión de riesgos operativos u operacionales establecido conforme a las normas sobre la materia. Las organizaciones del sector privado, como integrantes del Sistema Nacional de Transformación Digital, pueden tomar como referencia e implementar las mejores prácticas y estándares de gestión de riesgos ampliamente reconocidos, las cuales serán consideradas válidas para su uso y adopción, no siendo de obligatorio cumplimiento.

Sobre el mismo, el capítulo de la Gestión de riesgos de seguridad digital de la OCDE[15], hace mención que, pese a que en el 75% de los países en la región aún no dispone de una estrategia de seguridad digital, un gran número de países, entre ellos Argentina, Brasil, Chile, México y Paraguay, cuentan con entidades del gobierno y del sector público encargadas de coordinar y proteger la seguridad nacional y la infraestructura crítica.

Asimismo, en un estudio de ciberseguridad (BID y OEA, 2016) se evaluó el estado de preparación de 32 países de la región utilizando 49 indicadores divididos en cinco dimensiones: políticas y estrategia; educación; cultura y sociedad; marco jurídico, y tecnologías. Uruguay, Brasil, México, Argentina, Chile, Colombia y Trinidad y Tobago

[15] OCDE, capítulo 11: Gestión de riesgos de seguridad digital, https://www.oecd-ilibrary.org/docserver/9789264259027-17-es.pdf?expires=1592073880&id=id&accname=guest&checksum=A1E5A5B23D2DEBABD07014F2F55352CE

ya han alcanzado un nivel intermedio de preparación, pero aún van por detrás de países avanzados como Estados Unidos, Israel, Estonia y Corea.

En esta línea, se establecen disposiciones para el establecimiento de alianzas estratégicas para fines de colaboración y cooperación con el Centro Nacional de Seguridad Digital. Como actor clave se dispone que el Oficial de Seguridad y Confianza Digital es el rol responsable de coordinar acciones para fortalecer la seguridad digital en la entidad, así como también coordinar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Además, es responsable de coordinar con el CSIRT institucional el registro y notificación al CNSD de cualquier incidente de seguridad digital, e intercambio de información en materia de seguridad digital

Aunado a ello, se precisa que el Oficial de Seguridad y Confianza Digital es integrante del Marco de Confianza Digital y coordina con el Oficial de Datos Personales cuando se refiera a cuestiones relativas a la protección de datos a fin de fortalecer la confianza digital en el entorno digital.

Por último, se indica que organizaciones del sector privado, que conforman el Sistema Nacional de Transformación Digital, pueden tomar como referencia las mejores prácticas, normas técnicas peruanas y estándares internacionales ampliamente reconocidos en materia de seguridad de la información, para contar con un Oficial de Seguridad y Confianza Digital o rol similar, a fin de generar valor para el logro de sus objetivos estratégicos y contribuir a la implementación del Marco de Confianza Digital.

En el Capítulo III se desarrollan un conjunto de medidas que adoptan los prestadores de servicios digitales para fortalecer la confianza en el entorno digital, dichas medidas abordan aspectos sobre:

a) Adopción de normas técnicas y estándares internacionales en materia seguridad digital, ciberseguridad, accesibilidad, protección de datos personales y prácticas de protección al consumidor.
b) Niveles de Confianza en la Autenticación.
c) Obligaciones de los PSD en base a lo definido en el Decreto de Urgencia N° 007-2020.

En esta línea, siendo la SGTD el ente rector de la Seguridad Digital encargado de supervisar y evaluar dicha materia, se establece que realizan acciones de supervisión sobre el cumplimiento de obligaciones de los proveedores de servicios digitales a fin de cumplir con lo establecido en el artículo 9 del Decreto de Urgencia N° 007-2020. Las acciones de supervisión se realizan de forma presencial o digital y tienen un enfoque basado en riesgos que permitan la adopción de medidas correctivas y preventivas. Para tal fin, elabora los lineamientos para la supervisión del cumplimiento de las obligaciones de seguridad digital establecidas en el presente reglamento.

Por otro lado, el Capítulo IV de la propuesta normativa desarrolla aspectos relacionados con el Centro Nacional de Seguridad Digital (CNSD), el cual será el punto único de contacto, a través de la SSTSD y de la SGTD, para la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional, de conformidad con

el Decreto de Urgencia N° 007-2020 y Decreto Legislativo N° 1412. En ese marco se establece que los roles a desarrollar, a través de la Subsecretaría de Tecnologías y Seguridad Digital - SSTSD de la SGTD (órgano que, de acuerdo a lo establecido en el Texto Integrado del Reglamento de Organización y Funciones de la PCM, se encuentra a cargo de dicha plataforma).

Así, los roles que cumpliría el CNSD a través de la gestión de la Subsecretaría antes mencionada son las de: articulador, supervisor y capacitador, así como se encargará de elaborar los lineamientos que aseguren el cumplimiento de dichos roles.

Asimismo se precisa que las líneas de acción del CNSD son ejecutadas a través de la SSTSD, teniendo como parte de una de sus responsabilidades, el establecer y promover relaciones de cooperación en materia de seguridad digital con CSIRTs, SOCs, CERTs y otros actores del sector privado, academia, centros de investigación, sociedad civil del ámbito nacional y, con organismos internacionales de similar naturaleza, a través del intercambio de información y buenas prácticas y experiencias sobre investigación y desarrollo.

De esta forma se establece un conjunto de acciones bajo su cargo, así como los procesos operativos a su cargo (gestión de alertas digitales, gestión de incidentes, gestión de riesgos de seguridad digital, entre otros) que permitirán una adecuada interacción con las entidades públicas y organizaciones del sector privado.

Asimismo, respecto a la creación de la Plataforma Nacional de Talento Digital se debe considerar que el artículo 7 del Decreto de Urgencia N° 007-2020, ha asignado a la plataforma CNSD, a cargo de la SSTSD, la labor de articular y supervisar la operación, educación, promoción, colaboración y cooperación de la seguridad digital, en ese marco la labor como promotor de la educación digital que debe cumplir el Estado en el contexto de la confianza digital, la cual a su vez es una materia de la transformación digital es abordado en el objetivo prioritario 4 (OP4) de la Política Nacional de Transformación Digital al 2030, denominado, “Fortalecer el talento digital en todas las personas”, el cual advierte sobre la necesidad de desarrollar habilidades sociales, emocionales y cognitivas que permitan a las personas utilizar las tecnologías digitales para interrelacionarse, además de resaltarse la necesidad de una presencia multicanal de la Educación Digital.

Asimismo, el artículo 4 del Reglamento de la Ley de Gobierno Digital establece que el laboratorio de gobierno y transformación digital del Estado es el mecanismo de gobernanza e innovación abierta para co-crear, producir, innovar, prototipar y diseñar plataformas digitales, soluciones tecnológicas y servicios digitales con las entidades públicas, fomentar el desarrollo del talento digital, el uso de tecnologías emergentes, con colaboración de la academia, el sector privado, la sociedad civil y los ciudadanos. En ese marco, considerando las facultades que se desprenden del Decreto de Urgencia N° 007-2020 de la SGTD para emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza Digital, en el artículo 24 del presente Reglamento se señala que la SGTD emite los lineamientos para regular el CNSD y la Plataforma Nacional de Talento Digital.

En el capítulo V se establecen disposiciones sobre incidentes de seguridad digital, así como del Equipo de Respuesta a Incidentes de Seguridad Digital Nacional (CSIRT Nacional), componente del CNSD, responsable de prevenir, detectar, manejar, analizar, recopilar información y desarrollar soluciones para contener, articular y atender los incidentes de seguridad digital en el ámbito nacional, de conformidad con lo establecido en el artículo 7 del Decreto de Urgencia N° 007-2020.

El Perú cuenta actualmente con un **Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional (PeCERT),** creado por Resolución Ministerial N° 360-2009-PCM[16], siendo parte de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, el cual desde algunos años atrás, se ha encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los CiberDesafíos y coordinar la defensa ante los Ciberataques, con el fin de proveer a la Nación de una postura segura en el ámbito de la Seguridad Digital. Asimismo, tiene como parte de sus funciones, el coordinar y articular acciones con otros CSIRTs, CERTs o equipos de similar naturaleza locales, nacionales e internacionales para atender los incidentes de seguridad digital.

Asimismo, se desarrollan aspectos relacionados sobre el Registro Nacional de Incidentes de Seguridad Digital, el cual fue creado en el numeral 8.1 del artículo 8 del Decreto de Urgencia N° 007-2020, cuyo objetivo es el de recibir, consolidar y centralizar datos e información sobre los incidentes de seguridad digital comunicados por los PSD que puedan servir de evidencia o insumo para su análisis, investigación y solución. Adicionalmente se señala que las organizaciones del sector privado que presten servicio en entornos digitales deben notificar los incidentes de seguridad digital al Registro Nacional de Incidentes de Seguridad Digital en tanto estas pueden servir para generar datos, evidencias e insumos para el análisis, investigación y solución de incidentes de seguridad digital. Así, el Registro Nacional de Incidentes de Seguridad se constituye en el medio para conocer los incidentes relacionados con la seguridad digital.

El PeCERT como parte de las responsabilidades asignadas en el artículo 3 de la Resolución Ministerial N° 360-2009-PCM, dispuso el "Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas de la Administración Pública Nacional y facilitar el intercambio de información para afrontarlos".

Así, las entidades comprendidas en el artículo 9 del Decreto de Urgencia N° 007-2020 comunican al CNSD, los incidentes de seguridad digital reportados por sus administrados mediante los Protocolos y Canales para la comunicación de incidentes de seguridad digital. Asimismo, se precisa que los protocolos deben ser legibles para humanos y adecuados para su uso mediante plataformas digitales o aplicaciones informáticas que automaticen el intercambio de información.

Adicionalmente, se establecen disposiciones sobre los protocolos, canales, clasificación de los incidentes de seguridad y plazos para la notificación de incidentes de seguridad digital. Complementariamente se establecen disposiciones que regulan la notificación de los incidentes de seguridad digital al CNSD y su adecuada gestión.

[16] Ver resolución en https://cdn.www.gob.pe/uploads/document/file/357307/RM_360-2009-PCM.pdf

4.4 Título III: Medidas para fortalecer la confianza digital

La propuesta normativa establece dos (2) Capítulos en el Título III del presente Reglamento.

El Capítulo I incluye los instrumentos que permiten fortalecer la confianza digital, entre los que se encuentran:

a) Confianza digital de nombres de dominio; y,
b) Sellos de confianza digital

Por último, el Capítulo II de la propuesta normativa busca promover el uso ético de las tecnologías digitales y de los datos, considerando que el uso ético está orientado en asegurar que estos se encuentren al servicio de las personas y el medio ambiente, garantizando un progreso científico y tecnológico centrado en la persona, la transparencia y que asegure el respeto de los derechos fundamentales previstos en la Constitución Política del Perú y en los tratados internacionales de derechos humanos.

Por tal motivo se hace la precisión, por ejemplo, de que los proveedores implementan la protección de la privacidad el cual se incorpora en cada acción realizada y medida implementada durante el desarrollo y la prestación de servicios digitales.

Al respecto, el derecho internacional de derechos humanos establece las obligaciones que deben cumplir los Estados. Al pasar a formar parte de tratados internacionales, los Estados asumen deberes y obligaciones en virtud del derecho internacional, y se comprometen a respetar, proteger y promover los derechos humanos. La obligación de proteger exige que los Estados protejan a las personas o grupos de personas de las violaciones de los derechos humanos. La obligación de promover significa que los Estados deben adoptar medidas positivas para facilitar la realización de los derechos humanos básicos.

Asimismo, el Derecho Internacional Humanitario (DIH) prevé la obligación de los estados de “respetar” y “hacer respetar” sus normas (art. 1 común a los cuatro Convenios de Ginebra de 1949). La relación jurídica que se genera convencionalmente, vincula a los estados entre sí. Cada estado parte en los Convenios de Ginebra de 1949 se obliga a respetar y a hacer respetar a los demás estados parte la plena vigencia de sus enunciados normativos. En la práctica, los estados han sido renuentes a manifestar su intención de cuestionar a los estados violadores del DIH. En este sentido la posición asumida por terceros estados respecto de los conflictos armados ha sido generalmente la de impulsar la prevención de nuevas o reiteradas violaciones.

Asimismo, se busca promover la transparencia en los algoritmos de los servicios digitales a fin de verificar el uso adecuado de la información, así como también se proponen algunos criterios para promover la calidad de los datos, la publicación de datos de valor estratégico para el desarrollo de una economía basada en datos y se establecen condiciones sobre las capacidades y servicios del Centro Nacional de Datos, el cual al igual que el CNSD es una plataforma gestionada por la SSTDS tal y como se desprende del artículo 85 del ROF de la PCM..

4.5 Disposiciones Complementarias Finales

El proyecto normativo establece nueve (09) disposiciones complementarias finales en las que se aborda la emisión de normas complementarias que permitan asegurar la aplicación de las disposiciones establecidas en la propuesta normativa; la aprobación de lineamientos y protocolos propuestos por otras Entidades de la Administración Pública; la aprobación de los lineamientos para la gestión del Centro Nacional de Datos; la aprobación de la Estrategia Nacional de Confianza Digital; la clasificación nacional de incidentes de seguridad digital; los protocolos, canales y plazos para la notificación de incidentes de seguridad digital; la presentación del informe sobre la situación en seguridad y confianza digital en el país; y los recursos críticos de internet.

Asimismo, se establece la obligación de elaborar anualmente un Plan de Operaciones a fin de poder cumplir de forma adecuada con las obligaciones establecidas para el CNSD en el Decreto de Urgencia N° 007-2020, cómo, por ejemplo, gestionar, dirigir, articular y supervisar el cumplimiento de las disposiciones de Seguridad Digital.

En ese marco, hay que señalar que el mismo Texto Integrado del Reglamento de Organización y Funciones de la PCM establece que la SGTD tiene facultades para elaborar las estrategias, políticas nacionales, planes nacionales, normas, lineamientos, estrategias, proyectos, plataformas y agendas digitales.

Al respecto, es preciso señalar que la Trigésima Quinta Disposición Complementaria Final del Reglamento de la Ley de Gobierno Digital indica que la SGTD aprueba la Estrategia Nacional de Seguridad y Confianza Digital.

Finalmente, conforme se ha señalado en el Informe N° D000002-2025-PCM-SSPRD-AZH se precisa que la SGTD llevó a cabo talleres de co-creación y reuniones de trabajo con organizaciones del sector privado y entidades públicas, así como también con representantes de la sociedad civil a fin de dar a conocer la propuesta normativa, recibir aportes y realizar las adecuaciones correspondientes. Los aportes permitieron actualizar y mejorar la propuesta normativa.

V. ANÁLISIS DE IMPACTOS CUANTITATIVOS Y/O CUALITATIVOS DE LA NORMA

En cuanto a los principales beneficios, podemos señalar:

a) Respecto a la ciudadanía:

- 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, 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 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.

b) Respecto a las entidades de la Administración Pública:

- Contar con funcionarios y servidores públicos capacitados en materia de seguridad digital, ya que la implementación del CNSD comprende acciones para el fortalecimiento de capacidades en los aspectos técnicos, legales, organizacionales de la seguridad digital.
- Contar con disposiciones que permitan a las entidades públicas gestionar los riesgos de seguridad digital.
- Fortalecer los roles para la gestión digital, estableciendo como actor clave al Oficial de Seguridad y Confianza Digital como el rol responsable de coordinar la gestión de riesgos e incidentes de seguridad digital en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

c) Respecto a las organizaciones privadas:

- 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.
- Promover la interacción de los ciudadanos con los servicios digitales al establecer medidas para fortalecer la confianza digital, lo cual impacta en el desarrollo de la economía.

Así, se indicó que la propuesta normativa citada es de alto impacto y sumamente beneficiosa para los ciudadanos y sociedad en general, toda vez, que permitirá establecer y desarrollar el marco legal para el diseño e implementación de servicios digitales seguros, así como lo necesario para dar una atención adecuada y oportuna a los incidentes de seguridad digital que afecten a nivel nacional.

En cuanto a los costos, se prevé que no existe costo alguno para los administrados; por el contrario, estos se verán beneficiados con su aplicación.

Asimismo, es necesario indicar que la referida propuesta normativa no irrogará gastos adicionales a las entidades de la Administración Pública, puesto que se financia con el presupuesto institucional del Pliego presupuestario aprobado por las entidades de los tres niveles de gobierno, sin demandar recursos adicionales al Tesoro Público. Ello por cuanto su finalidad es, con miras a impulsar la transparencia, confianza y transformación digital del país y el desarrollo de una sociedad digital.

Finalmente, podemos advertir que en un análisis costo-beneficio ciertamente los beneficios que genera el Reglamento en materia de confianza digital superan largamente los costos que implicaría su implementación; razón por la cual, resulta pertinente su aprobación.

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

6.1. Análisis de la concordancia de la norma con la Constitución y la legislación nacional

La propuesta normativa no contraviene la Constitución Política del Perú ni la Ley Orgánica del Poder Ejecutivo, da estricto cumplimiento al mandato establecido en la Primera Disposición Complementaria Final del Decreto de Urgencia N° 007-2020, y guarda vinculación y coherencia con las normas vigentes del ordenamiento jurídico nacional. Así, dicha propuesta es concordante con las siguientes disposiciones normativas, para mantener la congruencia en el ordenamiento jurídico:

- Constitución Política del Perú.
- Ley Nº 29158, Ley Orgánica del Poder Ejecutivo.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado por Decreto Supremo N° 029-2021-PCM.
- Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, aprobado por Decreto Supremo N° 157-2021-PCM.
- Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Resolución Ministerial N° 224-2023-PCM.

Asimismo, la propuesta normativa es concordante con los siguientes instrumentos de política:

- El Acuerdo Nacional que, como compromiso entre las fuerzas políticas presentes en el Congreso, la sociedad civil, instituciones religiosas y el Gobierno, se suscribiera en marzo de 2002, a fin de entablar un diálogo para lograr que a través de la formulación de políticas de Estado se estableciera la base para la transición y consolidación de la democracia, la afirmación de la identidad nacional y el diseño de una visión compartida del país a futuro. Específicamente en relación con la Política 35 del Acuerdo Nacional sobre Sociedad de la Información y Sociedad del Conocimiento en su literal b) que el Estado fomentará el pleno ejercicio y respeto de los Derechos Humanos en todo entorno digital y en su literal h) que el Estado fomentará el uso transversal de las TIC en ámbitos tales como educación, salud, conservación del ambiente, seguridad ciudadana, prevención de riesgo de desastres, gobierno abierto, defensa nacional, innovación, investigación, transferencia de conocimiento y sectores productivos y sociales.
- La Política Nacional de Inclusión Financiera aprobada por Decreto Supremo N° 255-2019-EF, relacionado al Objetivo Prioritario 4 (OP4), referido a que el Estado se compromete a "*Desarrollar infraestructura de telecomunicaciones y plataformas digitales para incrementar la cobertura de servicios financieros*", lo cual requiere de una regulación clara en las materias de economía digital, educación digital, tecnologías digitales, servicios digitales, seguridad digital y confianza digital, todas ellas objeto del Sistema Nacional de Transformación Digital.

- La Política Nacional de Transformación Digital aprobada por Decreto Supremo N° 085-2023-PCM, relacionado con el OP5: "*Consolidar la seguridad y confianza digital en la sociedad*"; y, por ende, se hace hincapié en que, debido a la consolidación del proceso de transformación digital del país, las amenazas y riesgos se hacen también cada vez mayores, sin embargo, ello no puede representar una limitante para la interacción de la ciudadanía en el entorno digital.

- En relación con su impacto normativo, la propuesta normativa no deroga ni modifica ninguna norma con rango legal ni norma de menor jerarquía vigente de nuestro ordenamiento jurídico, en razón que, lo expresado en el Decreto de Urgencia N° 007-2020.

  Asimismo, tanto el Reglamento y la presente Exposición de Motivos han sido elaborados en el marco de la Ley N° 26889 Marco para la Producción y Sistematización Legislativa y su Reglamento aprobado por Decreto Supremo N° 007-2022-JUS.

6.2. Referentes en la legislación comparada

El Reglamento busca desarrollar lo establecido en el Decreto de Urgencia N° 007-2020, y su desarrollo se fundamenta principalmente en las recomendaciones realizadas por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en materia de seguridad y confianza digital. Asimismo, se consideraron los estudios y reportes realizados por organismos internacionales sobre dichas materias, entre ellos podemos mencionar, a la Unión Internacional de Comunicaciones (UIT), la Unión Europea.

Al respecto, la OCDE emitió un documento denominado “Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social”, el cual busca guiar la formulación de estrategias en materia de gestión de riesgos de seguridad digital, considerando los ámbitos económicos y sociales[19]. En dicho documento la OCDE indica que:

“La seguridad digital se puede abordar desde al menos cuatro perspectivas diferentes, cada una derivada de una cultura y antecedentes diferentes, prácticas reconocidas y objetivos:

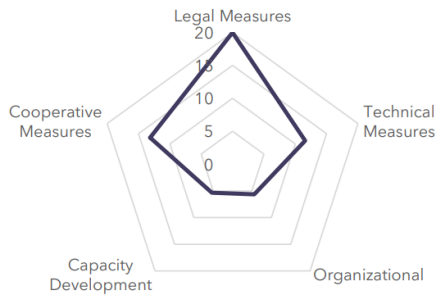
- *Tecnología, es decir, centrándose en el funcionamiento del entorno digital (a menudo llamado "seguridad de la información", "seguridad informática" o "seguridad de la red" por expertos)*
- *Aplicación de la Ley y, en general, aspectos legales (por ejemplo, cibercrimen)*
- *Seguridad nacional e internacional, incluidos aspectos como el papel de las TIC con respecto a la inteligencia, la prevención de conflictos, la guerra, etc.*
- *Prosperidad económica y social, que abarca creación de riqueza, innovación, crecimiento, competitividad y empleo en todos los sectores económicos, así como aspectos como las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso.”*

En el referido documento se reconoce que las diversas perspectivas están interrelacionadas en el entorno digital como lo están fuera de él, por lo que, los gobiernos deben esforzarse por un enfoque integral que involucre dichas perspectivas con las políticas y medidas de seguridad digital, aspirando a la coherencia, la complementariedad y el refuerzo mutuo. Así, la seguridad digital tiene un enfoque más amplio que comprende a la ciberseguridad, ciberdefensa, lucha contra la ciberdelincuencia; por lo tanto, las economías encuentran en este enfoque una perspectiva más amplia e integral.

Por otro lado, la UIT[17] realiza evaluaciones periódicas sobre el desarrollo de la ciberseguridad en sus países miembros, siendo una de las medidas técnicas a evaluar el disponer de un CNSD o Equipo de Respuestas ante incidentes de seguridad digital (CSIRT/CERT) activo, ello como parte de la articulación y atención diligente de los incidentes de seguridad digital que afecten la seguridad y confianza en el entorno digital.

[17] Puede ser consultado en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Peru

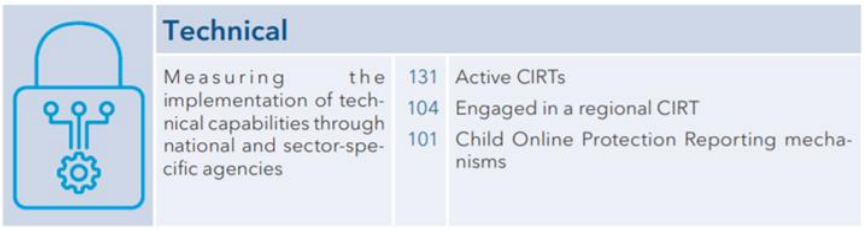


Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational, Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
55.67	20.00	11.58	5.63	5.32	13.15

Source: ITU Global Cybersecurity Index v4, 2020



Fuente: Global Cybersecurity Index 2020. UIT

Asimismo, en el año 2019, Perú firmó las “Recomendaciones del Consejo de Inteligencia Artificial” de la OCDE, las cuales tienen por objeto velar porque el diseño de los sistemas de Inteligencia Artificial se haga robustos, seguros, imparciales y fiables. Entre las recomendaciones para los países firmantes para el uso responsable de la IA se encuentran:

- Crecimiento inclusivo, desarrollo sostenible y bienestar, donde las partes interesadas, que incluyen a los que crean la IA, busquen beneficios de la IA para reducir desigualdades económicas, sociales y de género, protegiendo entornos naturales.
- Valores y equidad centrados en el ser humano, donde los desarrolladores de IA deben de respetar las leyes, derechos humanos y valores democráticos, durante el ciclo de vida del desarrollo de sistemas basados en IA.
- Transparencia y explicabilidad, donde los desarrolladores de IA deben comprometerse con la transparencia y la divulgación responsable con respecto a los sistemas de IA.
- Robustez, seguridad y protección, donde los sistemas de IA deben ser robustos, seguros durante todo su ciclo de vida, y que, en condiciones de uso normal, uso previsible o mal uso, u otras condiciones adversas, funcionen adecuadamente y no presenten riesgos de seguridad irrazonables.
- Responsabilidad, donde los desarrolladores de la IA deben ser responsables del correcto funcionamiento de los sistemas de IA y del respeto de los principios anteriores, en función de sus roles, el contexto y de conformidad con el estado del arte.

Además, la OCDE recomienda a los gobiernos se adopten las siguientes acciones:

- Promover la inversión pública y privada en investigación y desarrollo que estimule la innovación en una IA fiable.
- Fomentar ecosistemas de IA accesibles con tecnologías e infraestructura digitales, y mecanismos para el intercambio de datos y conocimientos.

- Desarrollar un entorno de políticas que allane el camino para el despliegue de unos sistemas de IA fiables.
- Capacitar a las personas con competencias de IA y apoyar a los trabajadores con miras a asegurar una transición equitativa.

En esta línea, el Decreto de Urgencia N° 007-2020 establece un capítulo mediante el cual dispone que 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. Y por ello, resulta de especial atención, la reglamentación del referido capítulo a fin de disponer las medidas necesarias para el uso ético de los datos y las tecnologías emergentes como la inteligencia artificial.

VII. PUBLICACIÓN DEL PROYECTO NORMATIVO

Finalmente, con relación a la publicación de la propuesta normativa, ésta resulta necesaria dado que se está estableciendo medidas para fortalecer la seguridad digital en las entidades públicas, las organizaciones de la sociedad civil, ciudadanos, empresas, y academia. Por consiguiente, se dispone la difusión del proyecto normativo de acuerdo con lo establecido en el artículo 19 del Reglamento que establece disposiciones sobre publicación y difusión de normas jurídicas de carácter general, resoluciones y proyectos normativos, aprobado por Decreto Supremo N° 009-2024-JUS.

VIII. ANÁLISIS DE IMPACTO REGULATORIO

Es importante mencionar que la propuesta normativa es de carácter multisectorial, dado que contiene disposiciones transversales que competen a otros sectores, así se requiere contar con el refrendo de la Presidencia del Consejo de Ministros y del Ministerio y del Ministerio de Justicia y Derechos Humanos, pero no requiere el voto aprobatorio del Consejo de Ministros.

Por otro lado, dado que la propuesta normativa no crea ni modifica procedimientos administrativos no pasa por el Análisis de Calidad Regulatoria según lo dispuesto en el numeral 33.4 del artículo 33 del Decreto Supremo N° 023-2025-PCM que aprobó el Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de la Calidad Regulatoria (en adelante, el Reglamento del DL 1565), vigente desde febrero del 2025.

Dado que la propuesta normativa no incorpora exigencias diferentes a las ya establecidas en la normativa vigente como el Decreto Legislativo 1412 y el Decreto de Urgencia 007-2020, lo cual implica que no haya una variación de costos en el cumplimiento por parte de las entidades de la administración pública, las empresas o ciudadanos, ni se advierte que este proyecto limite el otorgamiento o reconocimiento de derechos para el desarrollo de actividades económicas y sociales. En ese escenario se debe considerar que la propuesta se encuentra exceptuada de la aplicación del Análisis de Impacto Regulatorio Ex Ante, en tanto no regula ninguno de los supuestos establecidos en el artículo 33 del Reglamento del DL

1565 que desarrolla el marco institucional que rige el proceso de mejora de la calidad regulatoria y establece los lineamientos generales para su aplicación[18].

Por último, debido de que la propuesta normativa regula disposiciones referidas a la seguridad digital la cual, como ya se ha señalado, constituye un ámbito del Marco de Confianza Digital, conjuntamente con la protección al consumidor y la protección de los datos personales y transparencia; y, considerando, además que el objeto de la propuesta normativa es garantizar las interacciones digitales confiables a través del fortalecimiento de la seguridad digital en las entidades públicas, las organizaciones de la sociedad civil, ciudadanos, empresas, y academia, procurando con ello, el logro de la prosperidad económica y social del país, es que se debe señalar que la propuesta normativa se encuentra en el supuesto de excepción regulado en el inciso o) del párrafo 41.1 del artículo 41 del Reglamento del DL 1565[19], dada la relevancia de su implementación a garantizar la continuidad de la prestación de los servicios públicos, además de los ya señalados en el artículo 9 del Decreto de Urgencia 007-2020.

FIRMA DIGITAL
PCM
PRESIDENCIA DEL CONSEJO DE MINISTROS
Firmado digitalmente por VILCHEZ INGA Cesar FAU 20168999926 soft
Motivo: Doy V° B°
Fecha: 31.03.2025 16:34:33 -05:00

[18] **Decreto Supremo N° 023-2025-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley general de mejora de la calidad regulatoria**

"Artículo 33.- Ámbito de aplicación del AIR Ex Ante
(…)
33.2 Las entidades públicas tienen la obligación de aplicar un AIR Ex Ante como herramienta de análisis previo, cuando el proyecto normativo de carácter general establezca y/o modifique una obligación, condición, requisito, responsabilidad, prohibición, limitación y/o cualquier otra regla que imponga exigencia(s):
a) Que genere(n) o modifique(n) costos en su cumplimiento por parte de las personas; y/o,
b) Que limite(n) el ejercicio, otorgamiento y/o reconocimiento de derechos de las personas, restringiendo el desarrollo de actividades económicas y sociales que contribuyan al desarrollo integral, sostenible, y al bienestar social.
(…)"

[19]
"Artículo 41.- Supuestos que están fuera del alcance de la obligación de presentar expediente AIR Ex Ante a la CMCR

41.1 Las entidades públicas están exceptuadas de presentar expediente AIR Ex Ante a la CMCR, por lo que se encuentran fuera de lo dispuesto en el numeral 33.2 del artículo 33 del presente Reglamento, en los siguientes supuestos:
(…)
o) Disposiciones normativas que regulen aspectos vinculados a garantizar la seguridad o evitar el desabastecimiento para la continuidad de la prestación de servicios públicos cuando se presenten situaciones de eminente desabastecimiento o de alto riesgo ocasionados por eventos inesperados e impredecibles que pueden producir un daño a la vida o al ambiente.
(…)".