San Borja, 16 de Abril del 2025

INFORME N° 000079-2025-DPRC/OSIPTEL

Firmado digitalmente por QUISO CORDOVA Lennin Frank FAU 20216072155 soft
Cargo: Director De Politicas Regulatorias Y Competencia
Motivo: Soy el autor del documento
Fecha: 16.04.2025 18:41:04 -05:00

A	:	SERGIO CIFUENTES CASTANEDA **GERENTE GENERAL (e)**
CC	:	CARMEN CARDENAS DIAZ **DIRECTOR DE LA OFICINA DE COMUNICACIONES Y RELACIONES INSTITUCIONALES** RAFAEL MUENTE SCHWARZ **PRESIDENTE EJECUTIVO**
ASUNTO	:	Comentarios al Proyecto de Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital.
REFERENCIAS	:	Resolución Ministerial Nº 071-2025-PCM, publicada en el Portal Institucional de la PCM

	CARGO	NOMBRE
ELABORADO POR	ESPECIALISTA TECNOLÓGICO	PERCY PURAY CHAVEZ
	ABOGADO EN TEMAS DE GESTIÓN PÚBLICA	RENZO CHIRI MARQUEZ
REVISADO POR	SUBDIRECTOR DE ANÁLISIS REGULATORIO (e)	DANIEL ARGANDOÑA MARTINEZ
	DIRECTORA DE LA OFICINA DE ASESORÍA JURÍDICA (e)	ZARET MATOS FERNÁNDEZ
APROBADO POR	DIRECTOR DE POLÍTICAS REGULATORIAS Y COMPETENCIA	LENNIN QUISO CORDOVA

Firmado digitalmente por MATOS FERNANDEZ Zaret FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 16.04.2025 17:16:05 -05:00

Firmado digitalmente por CHIRI MARQUEZ Renzo Leonardo FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 16.04.2025 15:36:59 -05:00

Firmado digitalmente por ARGANDOÑA MARTINEZ Felipe Daniel FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 16.04.2025 12:42:43 -05:00

Firmado digitalmente por PURAY CHAVEZ Percy Faustino FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 16.04.2025 12:36:36 -05:00

I. OBJETO

El presente informe tiene por objeto emitir opinión sobre el Proyecto de Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº 007-2020, que establece disposiciones para el fortalecimiento del Marco de Confianza Digital.

II. ANTECEDENTES

2.1. Mediante la Resolución Ministerial Nº. 071-2025-PCM, la Presidencia del Consejo de Ministros publicó el proyecto de Reglamento del Decreto de Urgencia Nº 007-2020, con el objeto de recibir comentarios de las entidades competentes.

2.2. El citado proyecto desarrolla las disposiciones necesarias para fortalecer la confianza en las interacciones digitales entre personas, empresas, y entidades del Estado, promoviendo la seguridad digital, la protección de datos personales y los derechos del consumidor.

III. ANÁLISIS

3.1. Sobre el marco legal y las competencias del Osiptel

El OSIPTEL, en su calidad de organismo regulador de los servicios públicos de telecomunicaciones, tiene entre sus funciones promover la competencia, supervisar la calidad del servicio y proteger los derechos de los usuarios, conforme a la Ley Nº 27336[(1)], Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, y al TUO de la Ley de Telecomunicaciones, aprobado por Decreto Supremo Nº 013-93-TCC.

Dado que el Reglamento del DU Nº 007-2020 considera a los servicios de telecomunicaciones como "actividades críticas" (art. 8.1 y 13.1 del Reglamento), corresponde emitir una opinión técnica y legal sobre las implicancias del mismo en el ámbito de competencia del OSIPTEL.

3.2 Cuestión preliminar: sobre la base normativa y procedimiento de publicación

En cumplimiento del artículo 75[(2)] del Reglamento del Congreso y del artículo 9[(3)] del Reglamento de la Ley Nº 26889 aprobado mediante Decreto Supremo N° 007-

1 Publicada: 08 de julio de 2000.

2 El Artículo 75 del Reglamento del Congreso señala lo siguiente:

"Requisitos y presentación de las proposiciones
Artículo 75. Las proposiciones de ley deben contener una exposición de motivos donde se exprese el problema que se pretende resolver y los fundamentos de la propuesta; los antecedentes legislativos; el efecto de la vigencia de la norma que se propone sobre la legislación nacional, precisando qué artículos o partes de artículos se propone modificar o derogar; el análisis costo-beneficio de la futura norma legal que incluya la identificación de los sectores que se beneficiarían o perjudicarían con el proyecto de ley, los efectos monetarios y no monetarios de la propuesta, su impacto económico y, cuando corresponda, su impacto presupuestal y ambiental.
(…)"
[Subrayado agregado]

3 el Artículo 9. Análisis de impactos cuantitativos y/o cualitativos de la norma señala lo siguiente:

"Artículo 9.- Análisis de impactos cuantitativos y/o cualitativos de la norma
9.1 El análisis de impactos cuantitativos y/o cualitativos es empleado para conocer en términos cuantitativos y/o cualitativos los efectos que tiene una propuesta normativa sobre diversas variables que afectan a los actores, la sociedad y el bienestar general, de tal forma que permite cuantificar los costos y beneficios, o en su defecto posibilita apreciar analíticamente beneficios y costos no cuantificables. (…)
9.2 La necesidad de la norma debe estar debidamente justificada dada la naturaleza de los problemas existentes, los costos y beneficios probables de la aprobación y aplicación de la norma y los mecanismos alternativos que existan para solucionar dichos problemas.

2022-JUS, Ley Marco para la Producción y Sistematización Legislativa, toda propuesta normativa debe contener una Exposición de Motivos con análisis de impactos cuantitativos y cualitativos.

La Exposición de Motivos revisada se sustenta en instrumentos como el Informe Global de Riesgos 2024 (Foro Económico Mundial), datos de ciberataques registrados por ESET y Kaspersky, y la necesidad de armonizarse con compromisos internacionales como el Convenio de Budapest.

No obstante, se recomienda que en los futuros lineamientos técnicos o directivas operativas se incorporen indicadores clave de desempeño (KPI) y matrices de riesgo diferenciadas por sector, con el fin de facilitar el monitoreo y la evaluación continua del cumplimiento regulatorio, especialmente en sectores críticos como telecomunicaciones. Ello permitiría aplicar enfoques proporcionales, medibles y adaptados a las particularidades de cada sector.

Asimismo, se advierte que el proyecto no establece mecanismos de coordinación entre la Secretaría de Gobierno y Transformación Digital (SGTD-PCM) y los reguladores sectoriales como el OSIPTEL. Esta omisión podría generar conflictos de competencias en materia de supervisión de servicios digitales críticos. Se recomienda incorporar dicha coordinación en la reglamentación futura.

3.3 Respecto a las disposiciones contenidas en el Proyecto de Ley

a. Sobre las definiciones contempladas

El artículo IV[4] del Reglamento omite una definición clara de "proveedores de servicios de Internet" (ISP), no obstante que este término se emplea en el art. 18, lo que puede generar interpretaciones divergentes sobre el alcance de las obligaciones. Se recomienda incluir una definición expresa según el marco legal vigente, y que diferencie entre prestadores de servicios públicos de telecomunicaciones (provisión del servicio de Internet) que brindan las operadoras de telecomunicaciones, y servicios y plataformas digitales (OTT), las cuales se soportan sobre la Internet; ello, para garantizar seguridad jurídica.

Al respecto, cabe señalar que tanto el Decreto de Urgencia N° 007-2020, como el proyecto de Reglamento tienen como objetivo "*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 este sentido, una referencia general a los proveedores de servicios de internet resultaría imprecisa dado que, en la actualidad, las empresas operadoras que brindan servicios públicos de internet fijo y móvil pueden también brindar, además, servicios de plataformas digitales.

Por lo tanto, la definición que se adopte en el marco de esta normativa debe permitir la delimitación adecuada del alcance de las obligaciones establecidas en dicho marco, de manera que estas se apliquen únicamente a los servicios digitales ofrecidos por los proveedores de servicios de Internet.

9.3 El análisis de impactos cuantitativos y/o cualitativos de la norma es obligatorio en todos los proyectos normativos, (…).”

4 Artículo IV. Definiciones y Acrónimos
Para efectos del presente Reglamento se aplican las siguientes definiciones y acrónimos:
(…)

b. Sobre la cobertura de plataformas digitales críticas

El artículo 12 del Proyecto de Reglamento establece lo siguiente:

> *"**Artículo 12. Marco de Seguridad Digital en el Sector Privado***
>
> *12.1. Las disposiciones de seguridad digital establecidas en el presente Reglamento son aplicables a las organizaciones del sector privado que presten los servicios señalados en el numeral 9.1 del artículo 9 del DU 007-2020 en un entorno digital.*
>
> *12.2. Las organizaciones del sector privado que no se encuentren comprendidas en los alcances del DU 007-2020 considerarán como referenciales estas disposiciones y aquellos protocolos y lineamientos que se emitan en base al presente Reglamento."*
> [subrayado propio]

En este contexto, plataformas digitales como Netflix, Max, Spotify, entre otras, solo considerarían como referenciales las disposiciones del futuro Reglamento, a pesar que procesan datos personales sensibles.

Desde un enfoque constitucional, el inciso 6[(5)] del artículo 2 de la Constitución Política del Perú garantiza que los servicios informáticos no deben suministrar informaciones que afecten la intimidad personal y familiar. Permitir que estas plataformas queden fuera del cumplimiento obligatorio puede generar un tratamiento desigual en la protección de los derechos digitales de los ciudadanos, debilitando el alcance efectivo del marco normativo.

Por ello, se recomienda ampliar el ámbito de aplicación del Reglamento o, en su defecto, establecer criterios objetivos que permitan incluir a dichas plataformas cuando cumplan condiciones como volumen de usuarios, tipo de datos tratados o nivel de criticidad del servicio digital ofrecido.

c. Sobre las competencias de supervisión

En relación a nuestras funciones como órgano fiscalizador, se advierte que el Reglamento de la referencia estaría incluyendo a los servicios de telecomunicaciones dentro del concepto de "actividades críticas" en el ecosistema digital, conforme se desprende de la lectura realizada en los artículos 8[(6)] y 18[(7)]. En

---

5 El artículo 2 inciso 6 de la Constitución Política del Perú establece lo siguiente:

Artículo 2.- Toda persona tiene derecho:
(...)
6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
(…)"
[Subrayado agregado]

6 Artículo 8. Actividades Críticas y Funciones Críticas en la Administración Pública

8.1 Las actividades críticas se soportan en las funciones críticas, que comprenden al conjunto de personas, procesos, recursos, datos y activos que interactúan articuladamente para soportar el funcionamiento continuo y efectivo de actividades críticas y servicios básicos. Estas actividades son prestadas por entidades públicas u organizaciones privadas relacionadas con la IOFE, con el CNSD, con el SNTD y con el ecosistema de pagos digitales
Para efectos del presente Reglamento se aplican las siguientes definiciones y acrónimos:

8.2 Los PSD que participan en la prestación de los servicios básicos descritos en el artículo 9 del DU 007-2020 son responsables de establecer medidas para la ejecución continua y efectiva de las actividades críticas de dichos servicios; así como, de identificar, valorar y gestionar adecuadamente los riesgos de seguridad digital que los afecten.

8.3 La SGTD-PCM elabora y aprueba la lista de las actividades y funciones críticas para el CNSD y la SNTD, a través de Resoluciones de Secretaría de Gobierno y Transformación Digital

7 Artículo 18. Obligaciones de los Proveedores de Servicios Digitales

ese sentido, tanto el OSIPTEL como las empresas operadoras que supervisamos formaríamos parte del grupo de entidades públicas y proveedores de servicio digitales, respectivamente, que estarían obligadas a implementar medidas de seguridad digitales y a reportar incidentes al Centro Nacional de Seguridad Digital (CNSD)

Así mismo el artículo 19[8] establece que la SGTD-PCM realizará acciones de supervisión y monitoreo sobre proveedores de servicios digitales. Al respecto, siendo el OSIPTEL el ente regulador del sector telecomunicaciones, se recomienda que se disponga, en la parte reglamentaria o en los futuros lineamientos, la necesidad de coordinación interinstitucional a fin de evitar duplicidad o interferencia normativa, conforme al principio de especialidad regulatoria.

d. Sobre implicancias operativas y técnicas para el OSIPTEL

Por otro lado, se identifican disposiciones que, si bien no están relacionadas con competencias de supervisión, deben ser tomadas en cuenta en la planificación y ejecución de proyectos institucionales:

El artículo 17[9] establece que los niveles de autenticación en servicios digitales deben adecuarse al nivel de riesgo asociado al servicio, lo que implica el uso de mecanismos reforzados de validación, como el doble factor de autenticación. Esta disposición es relevante para entidades que gestionan datos personales sensibles o información crítica, por lo que podría tener efectos en el diseño técnico y normativo de sus servicios digitales.

El artículo 38[10] introduce la figura de los sellos de confianza digital, como mecanismo de reconocimiento a buenas prácticas en la provisión de servicios

18.1 Las entidades públicas, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas, entre otros), salud y transporte de personas, proveedores de servicios de Internet, proveedores de actividades críticas y de servicios educativos que lo brindan en el entorno digital, tienen las siguientes obligaciones:

8 Artículo 19. Monitoreo y Supervisión del Cumplimiento de las Obligaciones del ámbito de Seguridad Digital

La SGTD-PCM realiza acciones de monitoreo y supervisión sobre el cumplimiento de obligaciones de los proveedores de servicios digitales, de conformidad con lo establecido en el artículo 9 del DU 007-2020 y el artículo 18 del presente Reglamento.

Las acciones de supervisión se realizan de forma presencial o digital y tienen un enfoque basado en riesgos, que permitan las recomendaciones de mejoras o 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.

9 Artículo 17. Niveles de Confianza en la Autenticación

17.1 Los NCA pueden ser:

a) Nivel 1: Provee un nivel de confianza básico respecto de la identidad de una persona autenticada. Para este nivel se requiere el uso de por lo menos un (01) factor de autenticación.
b) Nivel 2: Provee un nivel de confianza razonable respecto de la identidad de una persona autenticada. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí.
c) Nivel 3: Provee un nivel de confianza alto respecto de la identidad de una persona autenticada. Para este nivel se requiere el uso de dos (02) factores de autenticación diferentes entre sí, debiendo uno de ellos estar basado en un módulo criptográfico resistente a manipulaciones.

17.2 Los PSD, para autenticar digitalmente a las personas naturales, implementarán los NCA considerando el nivel de riesgo del servicio digital.

10 Artículo 38.- Sellos de confianza digital

38.1 Los sellos de confianza digital se constituyen en el reconocimiento a las buenas prácticas que miden los niveles de confiabilidad de un servicio digital prestado por una entidad pública. Se consideran como criterios, el cumplimiento de los requisitos establecidos en la normativa vigente, los estándares tecnológicos y de seguridad digital implementados y los mecanismos de mitigación y respuesta ante contingencias.

digitales por parte de entidades públicas. Resulta pertinente evaluar, en coordinación con la Oficina de Seguridad de la Información, la posibilidad de diseñar un plan de trabajo institucional orientado a cumplir los criterios necesarios para la obtención de dicho sello.

e. Otros comentarios: Sobre la Exposición de Motivos

- Se recomienda incluir un artículo en el Título Preliminar que sistematice la base normativa del Gobierno Digital (D. Leg. 1412, DU 006-2020 y DU 007-2020).

- Se sugiere establecer un canal digital unificado de denuncias para los usuarios, como parte de la estrategia de transparencia y acceso al derecho.

IV. CONCLUSIONES

Por las consideraciones expuestas, este Organismo Regulador emite opinión favorable con observaciones respecto al Proyecto de Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº 007-2020.

No obstante, se considera necesario que se atiendan las observaciones formuladas, en especial sobre:

- La definición precisa de "proveedores de servicios de internet".
- La coordinación de competencias de supervisión con el OSIPTEL.
- La cobertura de plataformas digitales relevantes.

Las observaciones están orientadas a reforzar la seguridad jurídica, mejorar la coherencia institucional en las competencias de supervisión, e incorporar herramientas que viabilicen la evaluación del impacto regulatorio en el entorno digital.

V. RECOMENDACIÓN

Se recomienda remitir el presente Informe a la Secretaría de Coordinación de la PCM, para que considere las observaciones formuladas por el OSIPTEL en el marco de sus competencias regulatorias en materia de telecomunicaciones.

Atentamente,

LENNIN FRANK QUISO CORDOVA
DIRECTOR DE POLITICAS REGULATORIAS
Y COMPETENCIA

38.2 La SGTD-PCM promueve y establece los criterios para la participación, selección y reconocimiento de las entidades públicas a través del sello de confianza digital.