P/ 545.03.2026/DNPACG
Lima, 19 de marzo de 2026

CCL | CÁMARA DE COMERCIO LIMA
La Fuerza de los Empresarios
Presidencia

Señora
ARIANA MAYBEE ORUÉ MEDINA
Presidenta
Comisión de Ciencia, Innovación y Tecnología
Congreso de la República
Presente. -

Asunto: Dictamen recaído en los Proyectos de Ley 13415 Y 13511/2025-CR, que con texto sustitutorio propone la Ley que declara día nacional de la ciberseguridad el 30 de noviembre de cada año.

De nuestra consideración,

Es grato dirigirme a usted para saludarle a nombre del Consejo Directivo de la Cámara de Comercio de Lima (CCL) así como de la Presidencia del Gremio de las Tecnologías de la Información y de las Comunicaciones de la CCL; y, a su vez, remitirle nuestra opinión institucional sobre el Dictamen recaído en los Proyectos de Ley 13415 y 13511/2025-CR, que con texto sustitutorio propone la Ley que declara día nacional de la ciberseguridad el 30 de noviembre de cada año.

Al respecto, la CCL como gremio empresarial que agrupa a 16 gremios internos, 11 comisiones de trabajo y más de 20 sectores especializados dedicados al comercio, la producción y servicios, tiene el compromiso institucional de velar por los empresarios peruanos a través de proyectos y propuestas relacionados con el desarrollo del sector empresarial, facilitando oportunidades de negocio para fomentar el crecimiento económico y la generación de empleo que dinamice la economía peruana.

En ese sentido, adjuntamos el Informe DNPACG-029-2026/CCL de la Dirección Normatividad, Políticas y Articulación de Comisiones y Gremios, que contiene nuestros comentarios y sugerencias a la mencionada propuesta legislativa, las cuales ponemos a su consideración para los fines pertinentes.

Hacemos propicia la oportunidad para reiterarle los sentimientos de nuestra mayor consideración y estima personal.

Atentamente,

RAMIRO SALAS
Presidente (e)
Cámara de Comercio de Lima

JOSÉ ANTONIO CASAS
Presidente
Gremio de las Tecnología de la Información y de las Comunicaciones
Cámara de Comercio de Lima

Se adjunta: *Informe DNPACG-029-2026/CCL de la Dirección de Normatividad, Políticas y Articulación de Comisiones y Gremios.*
CC: Comisión de Descentralización, Regionalización, Gobiernos locales y Modernización de la gestión del Estado

INFORME DNPACG-029-2026/CCL

A	:	PRESIDENCIA DE DIRECTORIO
DE	:	DIRECCIÓN DE NORMATIVIDAD, POLÍTICAS Y ARTICULACIÓN DE COMISIONES Y GREMIOS
ASUNTO	:	OPINIÓN SOBRE EL DICTAMEN RECAÍDO EN LOS PROYECTOS DE LEY N° 13415 Y 13511/2025-CR, QUE CON TEXTO SUSTITUTORIO PROPONE LA LEY QUE DECLARA DÍA NACIONAL DE LA CIBERSEGURIDAD EL 30 DE NOVIEMBRE DE CADA AÑO
FECHA	:	LIMA, 06 DE MARZO DE 2026

Es grato dirigirme a usted, en atención al asunto y el documento de la referencia, para informar lo siguiente:

I. ANTECEDENTES

1.1. Con fecha 01 de diciembre de 2025, se presentó el Proyecto de Ley N°13415/2025-CR, Proyecto de Ley que declara el 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad". El 02 de diciembre de 2025, dicha iniciativa legislativa fue derivada a la Comisiones de Descentralización, Regionalización, Gobiernos Locales y Modernización de la Gestión del Estado, y a la Ciencia, Innovación y Tecnología del Congreso de la República para su análisis y dictamen correspondiente. Por medio del Oficio N° 00145-PO-2025- 2026-CCIT-AMOM-CR, de fecha 20 de enero de 2026, la Comisión de Ciencia, Innovación y Tecnología del Ministerio de la Producción solicitó a la Cámara de Comercio de Lima (CCL) sus aportes al referido Proyecto de Ley en mención.

1.2. Con fecha 11 de diciembre de 2025, se presentó el Proyecto de Ley N°13511/2025-CR, Proyecto de Ley que declara el Día Nacional de la Seguridad Informática – Ciberseguridad el 3 de diciembre de todos los años. En la misma fecha, dicha iniciativa legislativa fue derivada a la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República para su análisis y dictamen correspondiente. Posteriormente, con Oficio N°00152-PO/2025-2026-AMOM-CCIT/CR, de fecha 20 de enero de 2026, la Comisión de Ciencia, Innovación y Tecnología del Ministerio de la Producción solicitó a la Cámara de Comercio de Lima (CCL) sus aportes al referido Proyecto de Ley.

1.3. El 2 de marzo de 2026, la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República aprobó por unanimidad el Texto Sustitutorio recaído en el Dictamen de los Proyectos de Ley N° 13415 Y N°13511/2025-CR (en adelante, Texto Sustitutorio del Dictamen), que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año.

II. ANÁLISIS

2.1. De la revisión del Texto Sustitutorio del Dictamen en referencia, se advierte que propone lo siguiente: **(i)** declarar el 30 de noviembre como Día Nacional de la Ciberseguridad; y, **(ii)** promover la concientización de la ciberseguridad respecto a la importancia de la protección de la información.

2.2. Al respecto, del análisis del Dictamen recaído en los Proyectos de Ley N° 13415 y N°13511/2025-CR, que con texto sustitutorio propone la Ley que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año, emitimos nuestras **observaciones**, en atención a los fundamentos que se desarrollan en el presente informe.

A. RESPECTO A LA DETERMINACIÓN DE UNA FECHA CONMEMORATIVA SOBRE CIBERSEGURIDAD

2.3. De la revisión del dictamen en análisis se advierte que el establecimiento de una fecha conmemorativa para declarar el Día Nacional de la Ciberseguridad se establecerse con la finalidad de concientizar a la población, a las organizaciones de la sociedad civil y a las instituciones gubernamentales y privadas sobre la importancia de proteger la información. En el presente caso si bien valoramos que la misma constituye una medida orientada a visibilizar la importancia de la protección de la información y de los sistemas digitales en un contexto caracterizado por el creciente uso de las tecnologías de la información, lo cierto es que se requiere evaluar su viabilidad, y necesidad.

2.4. En atención a ello, debemos considerar que según el **Manual de Técnica Legislativa del Congreso de la República**[1], **todo proyecto de ley debe estar acompañado de un estudio que determine la viabilidad técnica, económica y jurídica de las medidas propuestas, así como su necesidad y coherencia con el ordenamiento vigente**. Esta exigencia no solo responde a una buena práctica normativa, sino también al principio de legalidad, racionalidad y eficiencia que rige la actividad legislativa del Estado. Asimismo, de acuerdo con el Decreto Supremo N°023-2025-PCM que aprueba el Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, el Análisis de Impacto Regulatorio Ex Ante es un proceso de análisis previo, sistemático e integral para identificar, evaluar y medir los probables resultados, beneficios y costos de distintas alternativas de solución para abordar un problema público y el impacto de la intervención pública. En ese sentido, tiene como objetivo *"garantizar que la propuesta de medida regulatoria que plantea la entidad como resultado del análisis correspondiente, sea la mejor opción para contribuir a solucionar o reducir los riesgos de un problema público identificado en base a evidencia; así como determinar que sus beneficios son superiores a sus costos (...)*

[1] Congreso de la República, Manual Técnica Legislativa. Aprobado por Acuerdo de Mesa Directiva 106-2020-2021/MESA-CR, 3era edición, 2021. Véase en: https://ial-online.org/wp-content/uploads/2022/11/manual-tecnica-legislativa-CongressoPeru.pdf

asegurando la coherencia con el ordenamiento jurídico (...)"[2]; a fin de que las nuevas regulaciones efectúen un análisis de impactos a nivel general.

2.5. Al respecto, de la revisión del referido Dictamen se advierte que: **i)** la fecha conmemorativa inicialmente propuesta en los Proyectos de Ley N° 13415 y N°13511/2025-CR fue el 3 de diciembre de cada año; **ii)** sustenta la nueva fecha de la declaración del Día Nacional de la Ciberseguridad (30 de noviembre de cada año) en virtud al Día Internacional de la Ciberseguridad o Día Internacional de la Seguridad de la Información; y, **iii)** no contiene acciones específicas que sustenten la necesidad de la declaración del Día Nacional de la Ciberseguridad.

2.6. Respecto al **primer punto**, referido a la fecha propuesta inicialmente (3 de diciembre), se advierte que en la sustentación del Dictamen en análisis se planteó la mencionada fecha en virtud de la realización de la cumbre de ciber amenazas SANS 2025 en la Unión Europea y la celebración del Día Internacional de las personas con discapacidad el celebrada en la misma fecha por parte la ONU[3].

2.7. Sin embargo, la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República identificó diversas cumbres internacionales desarrolladas en torno a la ciberseguridad, tales como Black Hat USA (01/08/2026 al 06/08/2026 en EEUU), Cumbre de Ciberseguridad 2026 (28/04/2026 y 29/04/2026 en Alemania), y Cyber Security World Asia (29/09/2026 y 30/09/2026 en Singapur); así como, 53 eventos relacionados al tema[4]. Por lo que, la referida Comisión determinó que *"no existe un sustento suficiente para la elección del 03 de diciembre como el día nacional de la ciberseguridad, ya que durante todo el año se están realizando eventos en torno a este importante tema"*[5].

2.8. Lo expuesto advierte inicialmente que la justificación para establecer el 03 de diciembre como Día Nacional de la Ciberseguridad resulta insuficiente, dado que los eventos internacionales vinculados a esta materia se desarrollan durante todo el año y no se concentran en una fecha específica.

2.9. Respecto al **segundo punto** de análisis, referido a la nueva fecha de la declaración del Día Nacional de la Ciberseguridad (30 de noviembre de cada año) en virtud al **Día**

---

2 Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria, aprobado por Decreto Supremo N° 023-2025-PCM (Artículo 32°).

3 Congreso de la República del Perú, Comisión de Ciencia, Innovación y Tecnología. (2026). Dictamen recaído en los Proyectos de Ley 13415 y 13511/2025-CR, que con texto sustitutorio propone la ley que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año. Congreso de la República del Perú. Página 6. Véase en: https://api.congreso.gob.pe/spley-portal-service/archivo/Mzc3NzE0/pdf. Consultado el 06/03/2026.

4 Véase en la página 7 del Dictamen recaído en los Proyectos de Ley 13415 y 13511/2025-CR, que con texto sustitutorio propone la ley que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año. Extraído de Global Cybersecurity Network. (2024, enero 21). Top cyber security conferences to attend in 2026. https://globalcybersecuritynetwork.com/blog/top-cyber-security-conferences/#:~:text=it%2Dsa%20Expo&Congress%202025%20es,y%20desaf%C3%ADos%20en%20seguridad%20inform%C3%A1tica

5 Congreso de la República del Perú, Comisión de Ciencia, Innovación y Tecnología. (2026). Dictamen recaído en los Proyectos de Ley 13415 y 13511/2025-CR, que con texto sustitutorio propone la ley que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año. Congreso de la República del Perú. Página 9.

Internacional de la Ciberseguridad o Día Internacional de la Seguridad de la Información, corresponde indicar que la Comisión sustentó la nueva fecha, *"conmemorando el ataque del gusano Morris en el año 1988, documentado en el portal oficial del Buró Federal de Estados Unidos (FBI) en la siguiente cita"*[6].

2.10. Sin embargo, esta nueva propuesta en virtud de lo expuesto por la Comisión determina un argumento lógicamente inconsistente, que paradójicamente invalida también la nueva fecha elegida (30 de noviembre de cada año); debido a que se constituye con un evento internacional que no requiere una conmemoración nacional.

2.11. En ese sentido, en virtud a los términos expuestos, adoptar la nueva fecha que ya cuenta con un reconocimiento global **resulta redundante** debido a que no explica la necesidad específica para que en el contexto peruano se replique la referida conmemoración internacional.

2.12. En relación al **tercer punto**, referido a la falta de acciones específicas que sustenten la necesidad de la declaración del Día Nacional de la Ciberseguridad. De lo expuesto en el artículo único del Dictamen, si bien se establece la finalidad de concientizar a la población, a las organizaciones de la sociedad civil y a las instituciones gubernamentales y privadas sobre la importancia de proteger la información, **se constituye únicamente como un proyecto declarativo**, **que limita su alcance y efectividad,** debido a que no determina las acciones necesarias que implementará para cumplir con la mencionada finalidad.

2.13. De acuerdo a la Dirección General de Desarrollo Normativo y Calidad Regulatoria del Ministerio de Justicia y Derechos Humanos en la Consulta Jurídica N° 024-2018-JUS/DGDNCR de fecha 12 de junio de 2018, tales leyes generan una vinculación política mas no jurídica, que no imponen ningún tipo de efecto jurídico. En consecuencia, tratándose de la declaración de un Día Nacional de la Ciberseguridad, debería orientarse no sólo a resaltar la importancia de la materia y promover su visibilización, sino establecer disposiciones específicas que impliquen la adopción de acciones concretas por parte de las entidades de la administración pública. Lo referido a las acciones necesarias para mejorar la seguridad digital será desarrollado en el tercer acápite del presente informe.

2.14. De lo expuesto, se advierte que el Dictamen no desarrolla una justificación suficiente que sustente la viabilidad y necesidad de instituir una fecha conmemorativa a nivel nacional, toda vez que tanto la elección inicial del 3 de diciembre y posterior adopción del 30 de noviembre carecen de sustento técnico, y se limita a replicar una conmemoración internacional existente, sin explicar de qué manera su declaración en el ámbito nacional contribuiría de forma concreta al fortalecimiento o la promoción de acciones para alcanzar la finalidad planteada (concientización sobre la importancia de

[6] Congreso de la República del Perú, Comisión de Ciencia, Innovación y Tecnología. (2026). Dictamen recaído en los Proyectos de Ley 13415 y 13511/2025-CR, que con texto sustitutorio propone la ley que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año. Congreso de la República del Perú. Página 9.

proteger la información). Desde esa perspectiva, la justificación presentada resulta principalmente declarativa, al no profundizar los posibles efectos jurídicos, sociales o institucionales que podría generar la implementación de la norma.

B. RESPECTO A LOS IMPACTOS DE LA CIBERSEGURIDAD EN EMPRESAS Y CIUDADANÍA

2.15. En este punto, es importante indicar que el concepto de "ciberseguridad" tiene una variedad de definiciones, y en algunos países es conocida como seguridad digital, que es la práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero[7]. Asimismo, debemos señalar que la ciberseguridad se entiende como el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos[8].

2.16. En el marco de la normativa peruana, **la ciberseguridad se define como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital.** Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país[9]. Y como señalamos anteriormente, también está relacionado con la "**seguridad digital**", el cual es el *"estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno"*[10]. Este marco de seguridad digital se encuentra establecido en la Ley de Gobierno Digital mediante el Decreto Legislativo N° 1412, particularmente en sus artículos: 30° y 33° este último, en concordancia con la *"Seguridad de la Información"* de acuerdo al *"Capítulo VI: Seguridad Digital"* del *"Título II. Gobierno Digital"* de la mencionada ley[11].

2.17. En esa línea, el contexto actual evidencia un incremento significativo de los riesgos y amenazas en el entorno a la seguridad digital que afectan tanto a las instituciones públicas y privadas como a la ciudadanía. En efecto, diversos reportes recientes dan

---

7 Microsoft. (s. f.). ¿Qué es la ciberseguridad? Microsoft Support. Véase en: https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390. Consultado el 05/03/2026.

8 International Telecommunication Union. (2018). "Guía para la elaboración de una estrategia nacional de Ciberseguridad - Participación estratégica en la Ciberseguridad". Véase en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf. Consultado el 05/03/2026.

9 Presidencia de la República del Perú. (2020, 9 de enero). Decreto de Urgencia N.° 007-2020, Decreto de Urgencia N° 007-2020. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Véase en: https://cdn.www.gob.pe/uploads/document/file/2790485/Decreto%20de%20Urgencia%20N%C2%BA%20007-2020.pdf?v=1643322610. Consultado el 05/03/2026.

10 Presidencia de la República del Perú. (2018, 13 de septiembre). Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital. Véase en: https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n1412-1691026-1.pdf?v=1566312763

11 Presidencia del Consejo de Ministros. (2025). Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (ESNACIB). Gobierno del Perú. Véase en: https://cdn.www.gob.pe/uploads/document/file/8499082/7046161-propuesta_-estrategia-nacional-de-ciberseguridad.pdf?v=1759424724. Consultado el 05/03/2026.

cuenta del problema que se evidencia en los reportes recientes sobre incidentes de seguridad informática. A modo de ejemplo, en **América Latina**[12] se registra un promedio de 2,716 ciberataques por semana, un 38% por encima de la media global. Asimismo, durante la primera mitad del 2025, FortiGuard Labs detectó 748.2 millones de intentos de ciberataques en el **Perú** y más de 374,000 millones de eventos maliciosos en los países de la región[13]. Con ello, los sectores telecomunicaciones, manufactura y público concentran la mayor cantidad de eventos maliciosos debido a la naturaleza crítica de sus operaciones y la sensibilidad de la información que manejan[14].

2.18. En esa línea, los ciberataques particularmente representan una de las principales amenazas para la estabilidad económica y operativa de las organizaciones, debido a las pérdidas financieras directas e indirectas que se pueden generar. En un contexto de creciente digitalización y dependencia de los sistemas informáticos, la ocurrencia de ciberataques puede comprometer gravemente la sostenibilidad financiera y la capacidad operativa de las empresas.

Cuadro 1. Por tamaño de empresa, el golpe económico es el siguiente:

Tamaño de empresa		
Grande	**1% - 3% de los ingresos anuales**	**Caída en el valor de la acción y crisis de confianza**
Mediana	5% - 10% de los ingresos anuales	Problemas severos de flujo de caja y pérdida de contratos clave
Pequeña (PYME)	> 20% de los ingresos anuales.	Riesgo de quiebra: el 60% de las pymes que sufren un ataque grave cierran en los siguientes 6 meses

Fuente: Según TIVIT Perú[15]. Extraído de Redacción Gestión.

2.19. El cuadro evidencia que el **impacto económico de los ciberataques varía según el tamaño de las empresas**, siendo las pequeñas y medianas empresas (pymes) las más vulnerables frente a este tipo de incidentes. Mientras que en las grandes empresas las

12 Redacción Gestión. (2025, 4 de septiembre). Mercado de ciberseguridad en Perú alcanzó US$ 220 millones: los sectores que lideran la inversión. Gestión. Véase en: https://gestion.pe/economia/empresas/mercado-de-ciberseguridad-en-peru-alcanzo-us-220-millones-los-sectores-que-lideran-la-inversion-noticia/?ref=gesr. Consultado el 05/03/2026.

13 Espinoza Castro, L. (2025, 3 de septiembre). Ciberataques en Perú superan los 748 millones en seis meses. Diario Oficial El Peruano. Véase en: https://www.elperuano.pe/noticia/278133-ciberataques-en-peru-superan-los-748-millones-en-seis-meses. Consultado el 05/03/2026.

14 Ibidem.

15 Cuadros Concha, F. (2026, enero 27). Por ciberataques, 6 de cada 10 pymes cierran: el impacto en los ingresos. Gestión. Véase en: https://gestion.pe/tu-dinero/por-ciberataques-6-de-cada-10-pymes-cierran-el-impacto-en-los-ingresos-noticia/?ref=gesr. Consultado el 05/03/2026.

pérdidas suelen oscilar entre el 1% y el 3% de sus ingresos anuales, principalmente asociadas a efectos reputacionales y la pérdida de confianza, en las empresas medianas el impacto puede alcanzar el 5% y el 10%, afectando el flujo de caja y la continuidad de contratos. En el caso de las pymes, las pérdidas pueden superar el 20% de sus ingresos anuales, incrementando el riesgo de quiebra, lo que evidencia que los ciberataques se han convertido en un riesgo creciente para la sostenibilidad financiera de las organizaciones en un contexto de mayo digitalización y sofisticación de la amenaza.

2.20. Sumado a ello, estos incidentes relacionados con la vulneración de la ciberseguridad **suelen ocasionar el robo de información sensible, la interrupción de servicios, el pago de rescates en ataques de *ransomware*[16] y elevados costos a la recuperación de sistemas y fortalecimiento de medidas de seguridad**. Respecto a los elevados costos, las grandes empresas en Perú incrementaron su presupuesto en ciberseguridad del 5% al 12% durante el segundo semestre de 2024. Por otro lado, se estima que las pequeñas empresas, con menos recursos, destinarán hasta un 10% de su presupuesto a Tecnología de la Información[17]. El sector financiero encabeza la lista, impulsado por iniciativas que integran inteligencia artificial para fortalecer la seguridad y optimizar costos"[18].

2.21. En otro ámbito, surgen **amenazas adicionales para la ciberseguridad que afecta directamente a la ciudadanía**, el cual consiste en la vulnerabilidad de la privacidad y la protección de los individuos cuyos datos personales han sido comprometidos. La divulgación de información sensible, como direcciones, números de contacto, datos financieros y documentos de identificación, puede derivar en situaciones de robo de identidad, acoso y otros riesgos asociados a la exposición de datos[19]. Esta situación podría provocar una disminución en la adopción de nuevas tecnologías en el futuro.

---

16 El ransomware es un tipo de malware capaz de bloquear un dispositivo o cifrar su contenido con el fin de extorsionar al propietario. A cambio, los operadores del código malicioso prometen (por supuesto, sin ninguna garantía) restaurar el acceso a la máquina o los datos afectados. Extraído de ESET. (s. f.). Ransomware: qué es, cómo ataca y cómo evitarlo. ESET. Véase en: https://www.eset.com/pe/ransomware/?srsltid=AfmBOor-q1_f0ZHO6E-8I5i3baSon9BZufUCKoxfo_VzwRndHTCI_7bL Consultado el 05/03/2026.

17 ICEX España Exportación e Inversiones. (2025). El mercado de la ciberseguridad en Perú 2025: Resumen ejecutivo del estudio de mercado. Oficina Económica y Comercial de España en Lima. Véase en: https://www.icex.es/content/dam/icex/centros/peru/documentos/2025/estudio-mercado-ciberseguridad-peru-2025-resumen.pdf?utm. Consultado el 05/03/2026.

18 Redacción Gestión. (2025, 4 de septiembre). Mercado de ciberseguridad en Perú alcanzó US$ 220 millones: los sectores que lideran la inversión. Gestión. Véase en: https://gestion.pe/economia/empresas/mercado-de-ciberseguridad-en-peru-alcanzo-us-220-millones-los-sectores-que-lideran-la-inversion-noticia/?ref=gesr. Consultado el 05/03/2026.

19 Centro Nacional de Planeamiento Estratégico (CEPLAN). (2025, abril). Ruptura de la ciberseguridad. Observatorio CEPLAN. Véase en: https://observatorio.ceplan.gob.pe/ficha/r39_2025. Consultado el 05/03/2026.

Cuadro 2. Los impactos negativos de una ruptura en la ciberseguridad.

Impactos negativos	Descripción
Pérdida de datos críticos	Pérdida de información valiosa y sensible
Robo de identidad	Suplantación de identidad de una persona con fines fraudulentos
Interrupción de servicios	Fallo o interrupción de servicios en línea como consecuencia de un ataque cibernético
Mayores costos financieros	Aumento de los costos financieros debido a la necesidad de invertir en medidas de seguridad cibernética
Disminución en la reputación	Reducción de la percepción positiva de la marca o empresa afectada
Diminución de la seguridad	Perdida de seguridad informática y aumento de la vulnerabilidad ante futuros ataques
Vulnerabilidad en la seguridad	Debilidad en los sistemas de seguridad que pueden ser explotados por atacantes
Paralización de negocios	La interrupción de las operaciones comerciales debido a un ataque cibernético
Disminución de la confianza	Reducción de la confianza en la seguridad cibernética y en los servicios en línea que utilizan los usuarios
Disminución de la privacidad	Pérdida de privacidad y exposición de información personal y sensible
Tensiones diplomáticas	Aumento de las tensiones entre países debido a los ataques cibernéticos
Disminución de la libertad	Disminución de la libertad individual como resultado de medidas de seguridad más estrictas en línea.

Fuente: Elaboración Cornejo, Verdezoto, Villacis & Ospina & Sanabria y Minería & Energía. Extraído de Observatorio CEPLAN[20].

2.22. A partir de este cuadro, se evidencia que las consecuencias de una ruptura en la ciberseguridad van más allá de la pérdida inmediata de datos o interrupción de servicios, sino que **impacta profundamente en la confianza de los usuarios, la reputación de las organizaciones, estabilidad de los negocios y afectación de derechos fundamentales como la privacidad y libertad individual**.

2.23. Este contexto, la propuesta normativa debería orientarse prioritariamente al **fortalecimiento de políticas públicas, capacidades institucionales y mecanismos de prevención y respuesta oportuna en materia de ciberseguridad, antes de la creación de nuevas efemérides**, más aún cuando ya existe una fecha de reconocimiento internacional destinada a la sensibilización sobre la seguridad de la información.

[20] Ibidem.

Asimismo, debe considerarse que la conmemoración de una fecha conmemorativa a nivel nacional no debe afectar, en ningún caso, el normal desarrollo de actividades institucionales ni generar interrupción en el funcionamiento regular de las organizaciones públicas y privadas.

2.24. En efecto, el incremento de la inversión en ciberseguridad por parte de las empresas en el Perú si bien evidencia la magnitud de estos riesgos y la necesidad de promover una cultura de seguridad digital. No obstante, también pone de manifiesto que **se requiere acciones concretas que se constituyan como una respuesta efectiva a dichos riesgos**, que deberían desarrollarse principalmente a través estrategias tecnológicas nacionales u organizacionales y de gestión; lo que sugiere que las acciones orientadas al fortalecimiento de capacidades y políticas públicas contribuyan a la protección de la información y al uso responsable de las tecnologías que resultan más pertinentes que la creación de nuevas efemérides.

2.25. Por lo expuesto, si bien resulta fundamental prevenir y mitigar amenazas informáticas que pueden comprometer el funcionamiento de los sistemas digitales y la seguridad de la información —que afectan tanto a empresas como a la ciudadanía—, lo cierto es que el establecimiento de una fecha conmemorativa no constituye necesariamente una medida eficaz para alcanzar el objetivo de la propuesta, debido a que se limita a un acto declarativo que, aunque es concordante con el Acuerdo Nacional[21], carece de mecanismos operativos necesarios para materializar el objetivo de la propuesta.

C. AUSENCIA DEL ESTABLECIMIENTO DE MEDIDAS ESPECÍFICAS PARA EL FOMENTO DE LA CONCIENTIZACIÓN DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN.

2.26. Teniendo presente el contexto planteado, en este acápite vamos a desarrollar algunas acciones necesarias que deberían contemplarse en el texto sustitutorio del referido Dictamen para lograr el objetivo planteado en la propuesta. Sobre el particular, en torno al sustento del Dictamen en referencia se advierte que si bien se reconoce la relevancia de promover la importancia de fomentar la concientización en ciberseguridad[22] como una herramienta esencial para la protección de la información en todos los niveles de la sociedad; no obstante, no establece ninguna disposición que permitan materializar

---

[21] A través de las siguientes Políticas de Estado, como: "20. Desarrollo de la ciencia y la tecnología", la "18. Búsqueda de la competitividad, productividad y formalización de la actividad económica"; y la "35: Sobre la sociedad de la información y sociedad del conocimiento". Acuerdo Nacional. (s. f.). *Acuerdo Nacional*.https://acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/definicion/

[22] La **concientización en ciberseguridad constituye un componente fundamental para fortalecer la seguridad digital**, en la medida en que no solo busca sensibilizar a la población sobre los riesgos asociados al uso de las tecnologías de la información, sino también promover la participación de las organizaciones públicas y privadas en la adopción de prácticas responsables que minimicen riesgos y fortalezcan la seguridad digital.
En este contexto, se vuelve especialmente relevante promover una cultura de ciberseguridad, entendida como *"la comprensión colectiva de lo que es normal y valorado en el entorno laboral en materia de ciberseguridad"*. El fomento de la cultura de ciberseguridad resulta fundamental para garantizar la protección de la información en un contexto caracterizado por el uso intensivo de tecnologías digitales y el intercambio constante de datos; en ese sentido, es necesario que se promueva la adopción de buenas prácticas en el uso de las tecnologías de la información por parte de empresas, instituciones y ciudadanía en general. National Cyber Security Centre (UK). (s. f.). Cyber security culture principles. Véase en: https://www.ncsc.gov.uk/collection/cyber-security-culture-principles. Consultado el 06/03/2026.

dicho propósito. Esta omisión constituye la deficiencia más crítica de la propuesta, en tanto lo reduce a un proyecto declarativo.

2.27. A modo ilustrativo corresponde indicar que en el Proyecto de Ley N°13415/2025-CR[23], que dio origen al Dictamen en análisis, se precisó **medidas de implementación** tales como: *i) campañas nacionales de sensibilización sobre buenas prácticas digitales; ii) simulacros nacionales de ciberataques orientados a mejorar la capacidad de respuesta institucional, iii) Programas educativos en coordinación con el Ministerio de Educación (Minedu) y la Autoridad Nacional del Servicio Civil (Servir), para incluir contenidos de ciberseguridad en todos los niveles de enseñanza y capacitación pública; y, iv) Reconocimiento anual "Perú Ciberseguro", a las instituciones que demuestren buenas prácticas y políticas efectivas de ciberseguridad.* Asimismo, se contempló la participación interinstitucional de las entidades públicas, empresas privadas, universidades y organizaciones civiles. En contraste, el Proyecto de Ley N°13511/2025-CR no contempló la implementación de acciones en el marco de la declaración de la fecha nacional.

2.28. Estas disposiciones, en el texto sustitutorio aprobado por el Dictamen en análisis lamentablemente, han sido eliminadas en su totalidad, lo que impide determinar los mecanismos bajo los cuales el Estado promovería la concientización y la protección de la información. En ese sentido, si bien el Dictamen no incorpora mecanismos concretos que permitan materializar dichas acciones, es importante reconocer que el Estado peruano ha venido impulsando diversas iniciativas orientadas a fortalecer la seguridad digital y la protección de la información.

2.29. En esa línea, el Gobierno, a través de la Secretaría de Gobierno y Transformación Digital (SGTD-PCM), ha reconocido que la ciberseguridad sigue siendo una preocupación constante y, al mismo tiempo, una prioridad dentro de las agendas de las entidades públicas y privadas del país. En ese sentido, resulta fundamental continuar fortaleciendo las **acciones de capacitación y promover mayores inversiones en medidas preventivas que permitan consolidar los avances alcanzados**[24].

[23] Congreso de la República del Perú. (2024). Proyecto de Ley N°13415/2025-CR, Proyecto de Ley que declara el 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad". Artículo 3. Véase en: https://api.congreso.gob.pe/spley-portal-service/archivo/MzUzNTg5/pdf. Consultado el 06/03/2026.

[24] Presidencia del Consejo de Ministros. (2025). Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (ESNACIB). Gobierno del Perú. Véase en: https://cdn.www.gob.pe/uploads/document/file/8499082/7046161-propuesta_-estrategia-nacional-de-ciberseguridad.pdf?v=1759424724. Consultado el 05/03/2026.

Figura 1. Ciberseguridad en Perú, desempeño del país, según el IGC 5ta Edición

Fuente: Elaboración propia, adaptada y traducida al español del "Global Cybersecurity Index 2024". Extraído de la Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026–2028.

2.30. Sobre el particular, de acuerdo al informe del **Índice Global de Ciberseguridad (GCI)**, cabe indicar que el Perú ha alcanzado avances en materia de ciberseguridad, especialmente en el ámbito de **medidas legales y organizacionales**, lo que refleja el fortalecimiento del marco normativo y de las estructuras institucionales destinados a la gestión de seguridad. No obstante, el país aún presenta oportunidades de mejora en áreas como las medidas técnicas, la cooperación y el desarrollo de capacidades, aspectos fundamentales para consolidar un ecosistema digital más seguro. Por consiguiente, **el Perú ocupa el 5° puesto en el GCI en la región, superando a países como Chile y Argentina.** A nivel mundial, está en el Nivel 3 (Establishing) de 5 y se encuentra en la denominada "etapa formativa"[25].

2.31. Como parte de este avance, se puede evidenciar el **desarrollo del marco normativo orientado a fortalecer la seguridad digital**, reflejado en el compendio de la normatividad del Centro Nacional de Seguridad Digital[26] y el compendio de normativa sobre Transformación Digital[27]. Algunas de esas normativas son el Decreto de Urgencia N° 007-2020, Decreto de urgencia que aprueba el marco de confianza digital

[25] ICEX España Exportación e Inversiones. (2025). El mercado de la ciberseguridad en Perú 2025: Resumen ejecutivo del estudio de mercado. Oficina Económica y Comercial de España en Lima. Véase en: https://www.icex.es/content/dam/icex/centros/peru/documentos/2025/estudio-mercado-ciberseguridad-peru-2025-resumen.pdf?utm. Consultado el 05/03/2026.

[26] Presidencia del Consejo de Ministros. (s. f.). Normatividad del Centro Nacional de Seguridad Digital. Plataforma Digital Única del Estado Peruano. Véase en: https://www.gob.pe/institucion/pcm/colecciones/3422-normatividad-del-centro-nacional-de-seguridad-digital. Consultado el 05/03/2026.

[27] Presidencia del Consejo de Ministros. (s. f.). Normativa sobre transformación digital. Plataforma Digital Única del Estado Peruano. Véase en: https://www.gob.pe/institucion/pcm/colecciones/147-normativa-sobre-transformacion-digital. Consultado el 05/03/2026.

y dispone medidas para su fortalecimiento; el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital[28] y su reglamento aprobado mediante Decreto Supremo N° 029-2021-PCM; y, la Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición". Asimismo, se cuenta con la implementación y evaluación de la Política Nacional de Transformación Digital al 2030, aprobado mediante Decreto Supremo Nº 085-2023-PCM[29].

2.32. En esa misma línea, como parte de las acciones en ciberseguridad desde *"la SGTD – PCM mediante el Centro Nacional de Seguridad Digital se gestionaron y emitieron 2,320 alertas de Seguridad Digital durante el año 2024; esto ha generado que se cree una mediana conciencia en cuanto a la protección y los riesgos relacionados con la Ciberseguridad"*[30]. Asimismo, hasta el momento la PCM ha emitido ciento sesenta y seis (166) alertas integradas documento que organiza en coordinación con diversas instituciones del Estado y del sector privado, con el fin de que los responsables de la Seguridad Digital, puedan conocer sobre las amenazas y las vulnerabilidades que aquejan al entorno digital y así advertir las situaciones que pudieran afectar la continuidad de los servicios y operaciones en favor de la población[31].

2.33. Sumado a ello, también se ha visualizado la **implementación de campañas y actividades orientadas a fortalecer la conciencia y educación en seguridad digital dirigidas tanto a ciudadanos como a entidades públicas y privadas**. Entre estas destacan campañas de sensibilización como **"Cuidarte es digital"**[32], una iniciativa para fortalecer la cultura del cuidado y la seguridad en el entorno digital. y **"Conectate Seguro"**[33], el cual es una plataforma que brinda información clara y recomendaciones prácticas para navegar de forma más segura.

2.34. Como se mencionó anteriormente, la ausencia de disposiciones efectivas orientadas a la capacitación, sensibilización o coordinación institucional en el Dictamen, limita el alcance de la finalidad perseguida y dificulta la promoción efectiva en una cultura de seguridad digital. Ello resulta particularmente relevante, si se considera que el fortalecimiento de la ciberseguridad no solo requiere el reconocimiento de su

---

28 Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. Véase en: https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf?v=1566312763. Consultado el 05/03/2026.

29 Presidencia del Consejo de Ministros del Perú. (2023). Política Nacional de Transformación Digital al 2030. Véase en: https://cdn.www.gob.pe/uploads/document/file/4932850/Pol%C3%ADtica%20Nacional%20de%20Transformaci%C3%B3n%20Digital%20al%202030.pdf?v=1691014709. Consultado el 05/03/2026.

30 Presidencia del Consejo de Ministros. (2025). Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (ESNACIB). Gobierno del Perú. Véase en: https://cdn.www.gob.pe/uploads/document/file/8499082/7046161-propuesta_-estrategia-nacional-de-ciberseguridad.pdf?v=1759424724. Consultado el 05/03/2026.

31 Ibidem.

32 Presidencia del Consejo de Ministros. (2025). Cuidarte es digital. Plataforma Digital Única del Estado Peruano. Véase en: https://www.gob.pe/institucion/pcm/campa%C3%B1as/122782-cuidarte-es-digital. Consultado el 06/03/2026.

33 Presidencia del Consejo de Ministros. (2026, 5 de febrero). Conéctate seguro. Plataforma Digital Única del Estado Peruano. Véase en: https://www.gob.pe/institucion/pcm/campa%C3%B1as/137765-conectate-seguro. Consultado el 06/03/2026.

importancia, sino también la adopción de acciones concretas y sostenidas que contribuyan al desarrollo de capacidades y a la prevención de riesgos en el entorno digital.

2.35. En virtud a lo expuesto, toda regulación que promueva la concientización en materia de ciberseguridad debería contemplar las siguientes acciones de materialización:

a) **Fortalecer la normativa existente y establecer una política específica en materia de ciberseguridad**[34], que permita articular de manera coherente las acciones del Estado, el sector privado y la ciudadanía frente a los crecientes riesgos en el entorno digital. En ese sentido, resulta necesario impulsar la elaboración del Plan Nacional de Continuidad o de Contingencia[35] para gestionar crisis de Ciberseguridad con la debida resiliencia, que considere diversos escenarios de riesgo, con la colaboración de las entidades, y proporcione una visión integral de los mecanismos nacionales de respuesta ante incidentes y clasifique los incidentes de Ciberseguridad según su impacto en los activos y servicios críticos de las entidades del Estado Peruano.

b) **Fortalecer medidas legales y organizacionales** que respondan al carácter transversal de la ciberseguridad y a su impacto en diversos sectores, con el fin de fortalecer la gestión de riesgos y la protección de la información. A modo de ejemplo, en cuanto a las medidas legales, se propone materializar **la propuesta de Estrategia Nacional de Ciberseguridad Perú 2026-2028**[36] en el que se desarrollan ocho pilares (principios rectores) y se establecen acciones estratégicas determinadas que permiten el paso del cumplimiento normativo a la gestión operativa relacionados con esta materia. Por otro lado, como medida organizacional que se puede impulsar es una cultura orientada a mitigar riesgos cibernéticos y responder eficazmente ante incidentes[37].

c) **Fomentar el uso de estándares internacionales reconocidos junto con marcos normativos**, como, por ejemplo: la NTP-ISO/IEC 27001:2022, Seguridad de la información, Ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3º Edición, y la NTP-ISO/IEC 27002:2022, Seguridad de la información, Ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2º Edición[38]. Esto permitirá garantizar la gestión efectiva de riesgos cibernéticos, la protección de la información crítica y la coordinación institucional.

---

[34] Presidencia del Consejo de Ministros del Perú. (2025, 15 de agosto). Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026-2028 (ESNACIB). Gobierno del Perú. Página 106. Véase en: https://cdn.www.gob.pe/uploads/document/file/8499082/7046161-propuesta_-estrategia-nacional-de-ciberseguridad.pdf?v=1759424724. Consultado el 06/03/2026.

[35] Cabe indicar que en la ESTRATEGIA NACIONAL DE CIBERSEGURIDAD PERÚ, 2026-2028, se contempla como una de las acciones estratégicas de ciberseguridad a la siguiente: *AEC4.2.3: Elaborar un Plan Nacional de Continuidad o de Contingencia para gestionar crisis de Ciberseguridad con la debida resiliencia.*

[36] Presidencia del Consejo de Ministros del Perú. (2025, 15 de agosto). Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026-2028 (ESNACIB). Gobierno del Perú. Página 88. Véase en: https://cdn.www.gob.pe/uploads/document/file/8499082/7046161-propuesta_-estrategia-nacional-de-ciberseguridad.pdf?v=1759424724. Consultado el 06/03/2026.

[37] Ibidem. Página 88.

[38] Ibidem. Página 21 y 22.

d) **Promover acciones permanentes de capacitación y sensibilización capacitación y sensibilización** dirigidos a operadores de infraestructuras críticas y usuarios estratégicos[39], así como mayores inversiones en medidas preventivas, que contribuyan al desarrollo de capacidades y a la consolidación de los avances alcanzados en materia de seguridad digital

e) **Medidas de innovación en ciberseguridad** para que se promuevan *"startups y empresas tecnológicas a través de participación de subvenciones, beneficios tributarios, becas, programas de incubación y fondos concursables, con el objetivo de desarrollar soluciones tecnológicas nacionales y potenciar el talento especializado. Todo ello con el respaldo estratégico de instituciones como CONCYTEC, la Cámara de Comercio, PRONABEC, universidades, centro de investigación, etc., que fomentan la I+D+i para consolidar una industria digital segura y competitiva"*[40].

2.36. La incorporación de estas acciones permitiría abordar la ciberseguridad desde un **enfoque integral**, que no solo contemple la respuesta frente a incidentes, sino también el fortalecimiento de capacidades institucionales, la prevención de riesgos y la consolidación de buenas prácticas a nivel organizacional y social. Como señala Genghis Ríos, experto en transformación digital: *"A medida que el Perú avanza en su crecimiento y se convierte en un país más digital, la ciudadanía emplea cada vez más plataformas digitales, como es el caso del e-commerce. Entonces, tenemos que estar un paso adelante capacitando no solamente al personal técnico, sino al público en general, porque se tiene que desarrollar una cultura de ciberseguridad. Si no lo hacemos, los casos de ciberdelincuencia seguirán creciendo y las personas pueden volverse reacias a usar medios de pago digitales, afectando el desarrollo del e-commerce en el país"*[41].

2.37. En esa línea, es importante a su vez que se impulsen **medidas de autorregulación empresarial**[42], orientadas al fortalecimiento de la ciberseguridad dentro de las organizaciones, que requiere una formación y concientización continua que permite mantener actualizados los conocimientos frente a la constante evolución de las amenazas digitales. Este enfoque no solo promueve una cultura de seguridad en la que todos los colaboradores asumen responsabilidad en la protección de la información,

---

39 Al respecto, en la ESTRATEGIA NACIONAL DE CIBERSEGURIDAD PERÚ, 2026-2028, se contempla como una de las acciones estratégicas de ciberseguridad a la siguiente: *AEC7.2.1: Impulsar programas especializados de capacitación y sensibilización dirigidos a operadores de infraestructuras críticas y usuarios estratégicos, promoviendo una cultura robusta de Ciberseguridad.*

40 Presidencia del Consejo de Ministros del Perú. (2025, 15 de agosto). Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026-2028 (ESNACIB). Gobierno del Perú. Página 106. Véase en: https://cdn.www.gob.pe/uploads/document/file/8499082/7046161-propuesta_-estrategia-nacional-de-ciberseguridad.pdf?v=1759424724. Consultado el 06/03/2026.

41 Innovapucp. (2024, diciembre 18). La importancia de la ciberseguridad en el entorno digital. INNOVAPUCP. Véase en: https://innovapucp.pucp.edu.pe/la-importancia-de-la-ciberseguridad-en-el-entorno-digital/. Consultado el 05/03/2026.

42 Waqas, M., & Hania, A. (2023). Enhancing Cybersecurity: The Crucial Role of Self-Regulation, Information Processing, and Financial Knowledge in Combating Phishing Attacks. SAGE Open. Véase en: https://journals.sagepub.com/doi/10.1177/21582440231217720. Consultado el 05/03/2026.

sino que también fomenta la identificación de comportamientos de riesgo y la adopción de prácticas seguras[43].

2.38. En virtud de ello, resulta fundamental la implementación de las **medidas de ciberseguridad** que tienen como propósito proteger los datos tanto individuales como organizacionales, centrándose en prevenir filtraciones, detectar amenazas, responder eficazmente y recuperarse de incidentes cibernéticos. En un mundo cada vez más conectado, una estrategia sólida de ciberseguridad es esencial para mantener la privacidad, la confianza y la seguridad. Asimismo, la capacitación interna resulta más efectiva cuando se adapta a las funciones y responsabilidades de cada trabajador, ya que cada rol enfrenta distintos niveles de exposición a riesgos y manejo de información sensible, lo que permite una gestión más eficiente de la seguridad digital[44].

2.39. Por lo expuesto, el fomento de la concientización en ciberseguridad se presenta como un elemento estratégico para garantizar la protección de la información en un país cada vez más digitalizado; por lo que, resulta fundamental establecer medidas específicas orientadas al desarrollo de acciones de capacitación, sensibilización y difusión dirigidas a la ciudadanía y las organizaciones públicas y privadas. Ello permitirá promover una cultura de seguridad digital que contribuya a reducir comportamientos de riesgo, mantenga actualizado los conocimientos frente a nuevas amenazas y fortalezca la confianza en el uso de plataformas digitales, favoreciendo así un entorno digital más seguro.

III. CONCLUSIONES

3.1 Del análisis del Dictamen recaído en los Proyectos de Ley N° 13415 y N°13511/2025-CR, que con texto sustitutorio propone la Ley que declara día nacional de la ciberseguridad el 30 de noviembre de cada año, emitimos nuestras **observaciones**: **(i)** la propuesta legislativa no desarrolla un sustento técnico suficiente que sustente la necesidad de instituir el Día Nacional de la Ciberseguridad, limitándose a replicar una conmemoración internacional existente sin explicar de qué manera su declaración a nivel nacional contribuiría de forma concreta al fortalecimiento de la concientización y protección de la información; **(ii)** el establecimiento de una fecha conmemorativa constituye principalmente un acto declarativo que no garantiza la prevención y mitigación de amenazas informáticas, por lo que resulta necesario priorizar el fortalecimiento de políticas públicas, capacidades institucionales y acciones de capacitación y sensibilización en materia de ciberseguridad; y, **(iii)** se requiere incorporar medidas específicas orientadas al desarrollo de acciones permanentes de capacitación, sensibilización y difusión que fortalezcan la cultura de ciberseguridad en la ciudadanía y en las organizaciones públicas y privadas, a fin de reducir

[43] Mendoza Silva, L. F. (2025, 14 de agosto). La concientización en ciberseguridad. Instituto para la Calidad – Pontificia Universidad Católica del Perú. Véase en: https://calidad.pucp.edu.pe/la-concientizacion-en-ciberseguridad/. Consultado el 05/03/2026.

[44] United Nations. (s. f.). Basic facts about the global cybercrime treaty. Véase en: https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty. Consultado el 05/03/2026.

comportamientos de riesgo, actualizar los conocimientos frente a nuevas amenazas y promover un uso responsable de las tecnologías en un entorno digital cada vez más complejo.

IV. RECOMENDACIÓN

4.1. Se recomienda remitir el presente informe a la Presidencia de Directorio para que, de corresponder, se ponga a consideración de las autoridades competentes.

Atentamente.