"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

PROYECTO DE LEY QUE DECLARA EL DÍA NACIONAL DE LA SEGURIDAD INFORMÁTICA – CIBERSEGURIDAD EL 3 DE DICIEMBRE DE TODOS LOS AÑOS

Los Congresistas de la República que integran el Grupo Parlamentario Bloque Democrático Popular, a la iniciativa del congresista **Edgard Reymundo Mercado**, al amparo de lo establecido en el Artículo 107° de la Constitución Política del Perú y de los artículos 75° y 76° del Reglamento del Congreso de la República, proponen el Proyecto de Ley:

Proyecto de Ley

EL CONGRESO DE LA REPÚBLICA
HA DADO LA SIGUIENTE LEY:

PROYECTO DE LEY QUE DECLARA EL DÍA NACIONAL DE LA SEGURIDAD INFORMÁTICA – CIBERSEGURIDAD EL 3 DE DICIEMBRE DE TODOS LOS AÑOS

Artículo 1. Objeto de la ley

La presente Ley tiene por objeto declarar el Día Nacional de la Seguridad Informática – Ciberseguridad, con la finalidad de que el Estado concientice a las personas y organizaciones la importancia de ejercer buenas prácticas de seguridad al utilizar computadoras, Internet, o cualquier otro medio de almacenamiento de información, sensibilizar sobre las amenazas cibernéticas y promover prácticas que aseguren la confidencialidad, integridad y disponibilidad de los datos.

Artículo 2º.- De la Declaración

Declárase el Día Nacional de la Seguridad Informática – Ciberseguridad, el 3 de diciembre de todos los años.

DISPOSICIÓN COMPLEMENTARIA FINAL

Artículo Único. Ejecución de Acciones

El Ejecutivo, en el marco de sus competencias y funciones legalmente establecidas, realizará las acciones correspondientes para el cumplimiento de la presente ley.

Lima, diciembre de 2025

FIRMA DIGITAL
Firmado digitalmente por: REYMUNDO MERCADO Edgard Cornelio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/12/2025 18:00:12-0500

FIRMA DIGITAL
Firmado digitalmente por: ZEBALLOS MADARIAGA Carlos Javier FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 11/12/2025 10:42:28-0500

FIRMA DIGITAL
Firmado digitalmente por: REYMUNDO MERCADO Edgard Cornelio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/12/2025 18:00:17-0500

FIRMA DIGITAL
Firmado digitalmente por: LUQUE IBARRA Ruth FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 11/12/2025 09:46:24-0500

FIRMA DIGITAL
Firmado digitalmente por: BAZAN NARRO Sigrid Tesoro FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/12/2025 14:40:11-0500

I. EXPOSICIÓN DE MOTIVOS

1. JUSTIFICACIÓN DE LA PROPUESTA NORMATIVA

Los peruanos somos víctimas de ataques cibernéticos diariamente, según la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional quien señala que aproximadamente cada semana se registran entre 30 y 35 denuncias de delitos informáticos. Es decir, al menos 120 casos al mes. Del total, más del 50% de casos son de fraudes electrónicos, 20%, por pornografía infantil y 10%, por suplantación de identidad.

Asimismo, la perdida producto de estos ataques oscilan en 4 mil millones de dólares al año por ciberdelitos, según Digiware.

El informe sobre Ciberseguridad 2016, de la Organización de Estados Americano (OEA) y el Banco Interamericano de Desarrollo (BID), advierte que el Perú ha realizado destacados esfuerzos, pero aún presenta "la ausencia de una estrategia y una cadena de mando clara sigue impidiendo el fortalecimiento de la seguridad cibernética".

Esta situación se ha agravado pues no solo las personas naturales han sido víctimas de ciberataques, sino también entidades del Estado, como lo sucedido al Registro de identificación y Estado Civil (Reniec) que en el 2024 informó que han bloqueado más de 4.6 millones de ataques a su sistema de datos y diversas fuentes de información que tuvieron como intención acceder a los datos de todos los peruanos y provocar la saturación de sus servidores informáticos; además de afectar el normal desenvolvimiento de los servicios a la ciudadanía.

Conforme lo señala el medio informativo INFOBAE[1], el Perú registró 45 mil millones de ciberataques en 2024 y que durante la primera mitad del año 2025 se han detectado más de 748 millones de intentos de ciberataques. Esto demuestra un incremento exponencial en los últimos años, con un incremento del 35% en 2022 comparado con 2021.

A ello se suma que el Perú ha sido víctima de ataques cibernéticos con incidencia mundial: Las empresas peruanas fueron infectadas con ransomware (secuestro de datos), afectando también a otros países latinoamericanos como México, Brasil, Ecuador, Colombia y Chile. Según Dmitry Bestuzhev, Director de Investigación y Análisis para Kaspersky Lab en América Latina. En una entrevista dijo a la Agencia Andina que "decenas de compañías peruanas" fueron víctimas de este nuevo ataque, con origen desconocido y sin relación confirmada con el anterior. "Esto va a servir de precedente para cambiar la lucha internacional contra el crimen cibernético. Estén los gobiernos de acuerdo o no entre ellos, estos ataques cibernéticos de alcance mundial harán que trabajen juntos", advirtió.

Perú es el segundo país más vulnerable al cibercrimen, debajo de Brasil, debido a la falta de atención y acciones de prevención y promoción respecto a estas vulnerabilidades.

[1] https://www.infobae.com/peru/2025/05/22/peru-registro-45-mil-millones-de-ciberataques-en-2024-asi-puedes-proteger-tu-pyme-sin-ser-experto-en-tecnologia/

Según cifras de EY Perú, el robo de información confidencial se suma a los ataques de malware y phishing.

La DIVINDAT señala que realiza un trabajo de investigación de los delitos informáticos de la Ley 30096, pero que los ciudadanos no mantienen una cultura digital de denuncia, debido a que en muchos casos no lo reportan ante las autoridades, sin embargo, la responsabilidad no es únicamente de la población, sino que no cuentan con la información correcta y oportuna sobre la actuación frente a los delitos cibernéticos.

Los ciberdelitos más frecuentes en Latinoamérica en 2024, a los cuales el Perú nos ajeno:

- Phishing: el phishing sigue siendo el ciberataque más común en la región. Este método, que utiliza correos electrónicos, mensajes de texto o páginas web falsas para engañar a las víctimas y obtener datos confidenciales, representó 73% de los ataques registrados en 2024. Brasil y México son los países más afectados, con un aumento significativo en los intentos de este tipo de ataque en comparación con años anteriores. Empresas como ESET y Kaspersky han señalado que los ciberdelincuentes han perfeccionado estas técnicas gracias a herramientas de automatización y personalización impulsadas por inteligencia artificial.

- Ransomware: el ransomware, en el que los atacantes secuestran datos y exigen rescates para su liberación, sigue creciendo en la región. En 2024, el 23% de las empresas latinoamericanas fueron blanco de ataques de ransomware. Las industrias de salud y finanzas son las más impactadas, debido a la sensibilidad y criticidad de sus datos. Según informes de Sophos y el análisis global de Kaspersky, las demandas de rescate pueden llegar hasta los 10 millones de dólares, con un impacto devastador en empresas que no cuentan con medidas preventivas sólidas.

- Malware y troyanos bancarios: diseñados para robar credenciales financieras han registrado un alarmante incremento en Latinoamérica. Durante este año, se detectaron más de 2.6 millones de variantes de malware, con Brasil y Argentina como los principales afectados. Estas cifras provienen de reportes de empresas como Avast y ESET, que destacan cómo estos ataques aprovechan aplicaciones móviles no verificadas y redes Wi-Fi públicas vulnerables.

- Ataques a la cadena de suministro: los ataques a la cadena de suministro, donde los atacantes se infiltran a través de proveedores o socios de confianza, afectan al 18% de las empresas en la región. Esto se debe a la interconexión entre empresas y sus proveedores tecnológicos, lo que los convierte en un objetivo atractivo. Firmas como Palo Alto Networks y Trend Micro han destacado el crecimiento de esta amenaza, especialmente en sectores críticos como manufactura y telecomunicaciones.

- Exploits de vulnerabilidades: más del 81% de los ataques en la región explotaron vulnerabilidades conocidas en software que no había sido actualizado. Estas brechas, especialmente en sistemas como Microsoft Office y Windows, son una puerta abierta para los atacantes. ESET y Kaspersky han subrayado que este tipo de ataque es particularmente prevalente en empresas pequeñas y medianas, que suelen carecer de políticas de actualización rigurosas.

Los sectores más golpeados y vulnerables por los ciberataques son:

- Finanzas y banca: los bancos han sido blanco constante de ransomware y troyanos bancarios debido a la alta concentración de datos sensibles.
- Salud: las organizaciones de salud han experimentado un incremento del 37% en ataques cibernéticos, según el informe de Kaspersky, afectando tanto datos médicos como operaciones críticas.
- Gobiernos y entidades públicas: infraestructuras críticas, como servicios públicos y sistemas de transporte, han sido objeto de ataques disruptivos que buscan desestabilizar operaciones esenciales.

Ante esas situaciones que seguirán ocurriendo y afectando al país se requiere que el Estado actúe de manera más efectiva a través de las entidades y direcciones como la Secretaría de Gobierno y Trasformación Digital de la Presidencia del Consejo de Ministros, quienes deben fortalecer las acciones de gestión promoción e impulso para dictar políticas y estrategias en materia de transformación digital en el país.

Una de esas acciones es impulsar mediante la difusión y la sensibilización a los ciudadanos, la misma que se concretiza mediante las declaraciones de los días nacionales, que concientizan los riesgos y la necesidad de atender diversas situaciones que viene afectado a la colectividad.

- **NECESIDAD DE DECLARAR EL DÍA NACIONAL DE LA SEGURIDAD INFORMÁTICA – CIBERSEGURIDAD EL 3 DE DICIEMBRE DE TODOS LOS AÑOS**

Cada 30 de noviembre desde 1988, de manera mundial se busca concienciar sobre la importancia de proteger nuestra vida digital frente a amenazas como phishing, ransomware y ataques a cadenas de suministro.

Fue propuesto en 1988 por la Association for Computing Machinery (ACM) tras el incidente del gusano Morris, considerado el primer malware ampliamente propagado en la incipiente Internet. Este evento afectó aproximadamente al 10% de las computadoras conectadas a ARPANET, la red precursora de Internet, y evidenció la vulnerabilidad de los sistemas digitales de la época.

Esta fecha se conmemoró por primera vez en el 2004, como parte de un esfuerzo global para sensibilizar sobre las amenazas cibernéticas y promover prácticas que aseguren la confidencialidad, integridad y disponibilidad de los datos.

Es importante que el Estado impulse y fortalezca la seguridad de la información, porque respecto a la ciberseguridad es el activo más valioso de las organizaciones y personas. Asimismo, garantiza la confidencialidad, integridad y disponibilidad de la información y protege los datos sensibles de los ciudadanos e implementa medidas de seguridad, ayuda a identificar, evaluar y reducir los riesgos asociados con la información, previene ciberataques, asegura la continuidad de los servicios públicos digitales y mantiene la confianza de los ciudadanos en la entidad.

Tal como lo orienta la conmemoración mundial, es necesario educar sobre los peligros asociados con el robo de datos, los ataques informáticos y la falta de medidas preventivas, incentivando la adopción de prácticas seguras tanto en el ámbito personal como en el corporativo, pues no solo la ciberseguridad es una necesidad global sino es una oportunidad para miles de jóvenes que estudian carreras técnicas especializadas y se preparan para enfrentar los desafíos del ecosistema digital.

En el Perú no existe un día nacional específico para la seguridad informática – ciberseguridad, por lo que considerando que día el 3 de diciembre de 2025 se llevó a cabo uno de los eventos anuales más esperados anualmente sobre ciberseguridad consideramos oportuno que dicho día sea considerado para que nuestro país declare un día nacional de la seguridad informática, con la finalidad de que el Estado concientice a las personas y organizaciones la importancia de ejercer buenas prácticas de seguridad al utilizar computadoras, Internet, o cualquier otro medio de almacenamiento de información, sensibilizar sobre las amenazas cibernéticas y promover prácticas que aseguren la confidencialidad, integridad y disponibilidad de los datos.

II. ANÁLISIS COSTO – BENEFICIO

La presente iniciativa no conlleva gastos al erario nacional, toda vez que, al ser una norma declarativa fortalecerá las acciones que el Estado viene ejecutando respecto a la seguridad informática en el país.

Los impactos que originará la dación de esta norma serán positivas para los ciudadanos, toda vez que tiene como finalidad orientar a la ejecución de acciones estratégicas para recomendar, prevenir y atender de manera prioritaria los delitos cibernéticos que afectan directamente en la economía y desarrollo del país.

III. EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACION NACIONAL

La iniciativa legislativa no se contrapone con ninguna norma de nuestro sistema legislativo, por el contrario, garantiza los derechos constitucionales en ciberseguridad que se encuentran contenidos en la Constitución Política (Art. 2) que protegen la privacidad, intimidad, honor y propia imagen, extendiéndose al derecho al acceso a internet (Art. 14, incorporado en 2024) y la protección de datos personales (Ley 29733), garantizando el anonimato, el olvido y el control sobre la información. Asimismo, no colisiona con leyes específicas como la Ley de Delitos Informáticos (N° 30096) y normativas sectoriales (SBS) sancionan ataques y exigen medidas de seguridad robustas, entre otras relacionadas a la materia.

IV. VINCULACIÓN CON EL ACUERDO NACIONAL

La presente iniciativa se enmarca en la siguiente política del Acuerdo Nacional:

9. Política de Seguridad Nacional[2]
24. Afirmación de un Estado eficiente y transparente[3]

Asimismo, tiene vinculación con los objetivos de Agenda Legislativa para el periodo anual de sesiones 2024 -2025.

[2] https://acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado/politicas-de-estado-castellano/
[3] https://acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado/politicas-de-estado-castellano/