



VÍCTOR SEFERINO FLORES RUIZ
Congresista de la República

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"



**PROYECTO DE LEY QUE MODIFICA EL
DECRETO DE URGENCIA N° 007-2020, DECRETO
DE URGENCIA QUE APRUEBA EL MARCO DE LA
CONFIANZA DIGITAL Y DISPONE MEDIDAS
PARA SU FORTALECIMIENTO, A FIN DE
REFORZAR EL CENTRO DE SEGURIDAD
DIGITAL Y PROMOVER LA CREACIÓN DE UN
CONSEJO NACIONAL DE CIBERSEGURIDAD O
SEGURIDAD DIGITAL**

El **Grupo Parlamentario Fuerza Popular**, a iniciativa del Congresista de la República, **Víctor Seferino Flores Ruiz** ejerciendo el derecho de iniciativa legislativa que le confiere el artículo 107° de la Constitución Política del Perú, en concordancia con lo establecido por los artículos 75° y 76° del Reglamento del Congreso de la República, presenta la siguiente propuesta legislativa:

El Congreso de La República;

Ha dado la ley siguiente:

FÓRMULA LEGAL

LEY QUE MODIFICA EL DECRETO DE URGENCIA N° 007-2020, DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE LA CONFIANZA DIGITAL Y DISPONE MEDIDAS PARA SU FORTALECIMIENTO, A FIN DE REFORZAR EL CENTRO DE SEGURIDAD DIGITAL Y PROMOVER LA CREACIÓN DE UN CONSEJO NACIONAL DE CIBERSEGURIDAD O SEGURIDAD DIGITAL

Artículo 1°. Objeto de la Ley

La presente Ley, tiene por objeto modificar el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, a fin de reforzar el Centro Nacional de Seguridad Digital en todo el territorio nacional, así como promover la creación de un Consejo Nacional de Ciberseguridad o Seguridad Digital en el marco de las competencias de la Presidencia del Consejo de Ministros y la Secretaría de Gobierno Digital, como ente rector de la materia en el país.

Artículo 2°. Modificación al artículo 7° del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento

Se modifica el artículo 7° del Decreto de Urgencia N° 007 -2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, en los siguientes términos:

"Artículo 7.- Centro Nacional de Seguridad Digital

7. 1. Créase el Centro Nacional de Seguridad Digital como plataforma digital **que deberá contar con infraestructura** y se encargará de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer y **asegurar la confianza en el entorno digital**. Asimismo, es responsable de identificar, **prevenir, reducir, tratar de manera inmediata**, proteger, detectar, responder, recuperar, y recopilar, información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

7. 2. El Centro Nacional de Seguridad Digital se encuentra **adscrito** a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, **y se constituye en el Centro Nacional de Operaciones en Seguridad Digital lo que incluye la creación de herramientas legales y técnicas para garantizar la confianza en el entorno digital, la gestión de la plataforma Digital, el equipo de expertos en el campo de la seguridad digital**, siendo único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

7. 3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano y el Marco de Confianza Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y el artículo 4 del presente Decreto de Urgencia.

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

7. 5 La Secretaría de Gobierno Digital, establece los protocolos de escalamiento, coordinación, intercambio y activación **inmediata** ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes."

Artículo 3°. Incorporación de los siguientes artículos al Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento

Se incorporan los siguientes artículos al Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, en los siguientes términos:

"Artículo 16°. - Funciones del Centro Nacional de Seguridad Digital

Las principales funciones son:

- a) Resguardar la seguridad de las personas en el ciberespacio.
- b) Proteger la seguridad digital del país.
- c) Promover la cooperación y coordinación entre instituciones tanto públicas como privadas.

- d) Identificación y jerarquización de las infraestructuras críticas de la información.
- e) Protección de las infraestructuras críticas de la información.
- f) Fomentar una cultura de la ciberseguridad o seguridad digital en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.
- g) Establecer relaciones de cooperación en ciberseguridad o seguridad digital con otros actores y participar activamente en foros y discusiones internacionales de la materia.
- h) Impulsar el desarrollo de la industria de ciberseguridad del país y el desarrollo digital, con foco en la provisión de la oferta de la industria nacional y la demanda del sector público de acuerdo con los intereses estratégicos del Estado.

Artículo 17°. - Promoción de la creación del Consejo Nacional de Ciberseguridad o Seguridad Digital

Promuévase la creación del Consejo Nacional de Ciberseguridad (CONACY), cuya conformación deberá contar con las siguientes entidades:

- a) Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital quien la preside.
- b) Poder Judicial
- c) Dirección Nacional de Inteligencia
- d) Ministerio de Defensa
- e) Ministerio del Interior
- f) Ministerio de Transportes y Comunicaciones
- g) Policía Nacional del Perú
- h) Asociación de Gobiernos Regionales
- i) Sociedad Nacional de Industrias
- j) Asociación de Bancos del Perú
- k) Asociación para el Fomento de la Infraestructura Nacional
- l) Red Científica Peruana
- m) Cámara de Comercio de Lima
- n) Cámara Nacional de Comercio, Producción, Turismo y Servicios – PERUCÁMARAS
- o) Colegio de Abogados de Lima
- p) Colegio de Ingenieros del Perú
- q) NAP (Network Access Point) Perú
- r) Confederación Nacional de Institucionales Empresariales Privadas

DISPOSICIÓN COMPLEMENTARIA FINAL

PRIMERA. – Financiamiento

La implementación de lo establecido en la presente Ley, se financia con cargo al crédito presupuestal de los sectores correspondientes, en el Presupuesto Público de cada Año Fiscal; sin demandar recursos adicionales al Tesoro Público.

SEGUNDA. – Vigencia y aplicación de la Ley

La presente ley rige a partir del día siguiente de su publicación en el diario oficial El Peruano.



Firmado digitalmente por:
CASTILLO RIVAS Eduardo
Enrique FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 12:15:57-0500



Firmado digitalmente por:
CHACON TRUJILLO Nilza
Merly FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 12:19:46-0500

05 de julio 2022



Firmado digitalmente por:
BARBARAN REYES Rosangella
Andrea FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 12:10:23-0500



Firmado digitalmente por:
FLORES RUIZ Victor
Seferino FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 13/07/2022 13:04:17-0500



Firmado digitalmente por:
INFANTES CASTAÑEDA Biana
Biana FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 12:07:49-



Firmado digitalmente por:
JUAREZ GALLEGOS Carmen
Patricia FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 22/08/2022 17:08:21-0500



Firmado digitalmente por:
OLIVOS MARTINEZ Leslie
Vivian FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 10:21:22-0500



Firmado digitalmente por:
AGUINAGA RECUENCO
Alejandro Aurelio FAU 2016174
soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 10:38:15-05



Firmado digitalmente por:
GUERRA GARCIA CAMPOS
Hermando FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 10:44:54-0500

Edificio Juan Santos Atahualpa Av. Abancay Cdra. 2 s/n Oficina N° 301 - Lima
Calle Marcelo Corne N° 161 Oficina N° 201 Urb. San Andres - Trujillo
Teléf.: +51 1 3117777 Anexo 7274



Firmado digitalmente por:
ZETA CHUNGA Cruz Maria
FAU 20161740126 soft
Motivo: Soy el autor del
documento
Fecha: 23/08/2022 11:53:11-

EXPOSICIÓN DE MOTIVOS

I. PROBLEMA QUE SE PRETENDE RESOLVER

En la actualidad, el mundo ha dado un gran paso mediante el acelerado desarrollo de sus tecnologías, herramientas y sistemas digitales, esta situación obliga a la sociedad a adaptarse de la manera más rápida posible a estos cambios, la velocidad con la que crecen los servicios digitales supera a veces la capacidad de respuesta por parte de la ciudadanía y de los entes encargados de fiscalizar el normal funcionamiento en la red. Esto se vio potenciado por efecto de la pandemia generada por el COVID-19, que supuso en su momento migrar de manera repentina e imprevista al entorno digital, a través de la imposición del trabajo remoto tanto en el sector público como privado.

El navegar dentro del mundo digital significa grandes avances en nuestro posicionamiento como país en aras de adaptarnos a la tecnología de las grandes potencias; sin embargo, nos trae también problemas de gran envergadura asociados con la seguridad digital o ciberseguridad, el constante acceso a datos personales y la facilidad con la que estos puedan encontrarse en el mercado, las distintas formas de ciberataques, nos obliga a analizar todo el conjunto normativo creado hasta la fecha y realmente verificar si funciona o no, así como determinar que aristas puedan ser materia de regulación para afianzar esta materia.

En nuestro país, han sido notable los esfuerzos por tratar de acoplar nuestra normativa a los cambios generados por la digitalización de procesos, incluso se ha suscrito el Convenio de Budapest en aras de fortalecer y prepararnos para los grandes retos que suponen la era digital. Muestra de ello podemos mencionar la siguiente normativa:

- Decreto Legislativo N° 1412 "Ley del Gobierno Digital"
- Decreto Supremo N° 29-2021 "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"
- Decreto de Urgencia 006-2020 "Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital"
- Decreto de Urgencia 007-2020 "Decreto de urgencia que aprueba el marco de confianza digital", que 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.

Las disposiciones antes expuestas han establecido definiciones, objetivos y estrategias sobre el campo tan relevante como es el de la seguridad digital; sin embargo, a la luz de nuevos hechos, vemos que el mismo debe fortalecerse, empezando por el Centro Nacional de Seguridad Digital, además se requiere del esfuerzo articulado tanto de las entidades públicas o privadas para afrontar los peligros y amenazas latentes en el ciberespacio.

Según Linares (2022) *"entre 2016 a 2020, los cibercrímenes causaron pérdidas de \$13.3 mil millones (INTERNET CRIME COMPLAINT CENTER, 2020) y los peligros online representan la segunda mayor preocupación de las empresas 2021."*¹

Además, conforme lo detallan algunos reportes, dentro de América Latina, el Perú es un país considerado como uno de los principales objetivos de ciberataques, tal cual citamos a continuación:

- El Panorama de Amenazas en América Latina 2021 de Kaspersky, informe anual realizado por nuestro Equipo de Investigación y Análisis, **revela un aumento del 24% en ciberataques en la región durante los primeros ocho meses del año, en comparación con el mismo periodo en 2020.** El informe toma en cuenta los 20 programas maliciosos más populares, los cuales representan más de 728 millones de intentos de infección en la región—un promedio de 35 ataques por segundo. La conclusión de los especialistas es clara: la seguridad de las tecnologías para el trabajo remoto debe ser prioridad y la piratería, tanto en dispositivos personales como profesionales, debe ser erradicada. (DiezGranados, 2021)²
- En el 2021 **Eset informó que el Perú volvió a tener el mayor nivel de detecciones de ransomware a nivel empresas en Latinoamérica durante 2020 al abarcar el 30% de las mismas. Superó a México (14.9%), Venezuela (13.2%) y Brasil (11.3%).** Además, fuimos el país con mayor actividad maliciosa relacionada con la criptominería de la región, con el 10,1% de detecciones y el segundo en el mundo, detrás de Tailandia. Por si fuera poco, según Eset, estamos a la cabeza de los países con la mayor cantidad de detecciones de spyware del mundo, seguidos de Israel y Rusia. Y en el caso de backdoors, despuntan Tailandia, Indonesia y Perú.(Ebiz Latinoamérica, 2022)³
- Un reciente estudio de Fortinet revela que Perú sufrió más de 11.5 mil millones de intentos de ciberataques en el 2021. Esta cifra equivale a 32 millones de intentos de ataques cibernéticos al día o 1.3 millones cada hora, en promedio. Así lo indica el informe FortiGuard Labs 2021 en América Latina y el Caribe, el cual registra más de 289 mil millones de amenazas cibernéticas, 600% más a lo registrado en el 2020. Los países de Latinoamérica más afectados por ataques cibernéticos en 2021 fueron, en orden según su volumen: México (156 mil millones), Brasil (88.5 millones), Perú (11.5 mil millones) y Colombia (11.2 mil millones).(Agencia Peruana de Noticias,2022)⁴

¹Linares, F. (28 de marzo de 2022). *Vulnerabilidad en el sector público y la urgencia de pensar en ciberseguridad.* <https://ciup.up.edu.pe/analisis/vulnerabilidad-en-sector-publico-la-urgencia-de-pensar-ciberseguridad>.

² DiezGranados, H. (31 de agosto de 2021). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021.* <https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/>

³ Perú está entre los países con más incidentes de seguridad del continente. (04 de abril de 2022). <https://noticias.ebiz.pe/peru-esta-entre-los-paises-con-mas-incidentes-de-seguridad-del-continente/>

⁴ Perú sufrió más de 11.5 mil millones de intentos de ciberataques en 2021 (16 de febrero de 2022). <https://andina.pe/agencia/noticia-peru-sufrio-mas-115-mil-millones-intentos-ciberataques-2021-881221.aspx>

Incluso mencionamos los ciberataques más relevantes que sufrió nuestro país:

- En el año 2018, se consumó uno de los ataques más trascendentes a las entidades del sistema financiero, el servicio atacado fue el de cajeros automáticos, que maneja la mayoría de la población, que pudo ser inmediatamente repelido gracias a la activación de protocolos de seguridad por parte de las entidades bancarias.
- Y recientemente fuimos objeto de una filtración de datos personales administrado por entidades públicas conforme advirtió la Asociación de Bancos del Perú (Asbanc), quien emitiera una alerta poniendo en conocimiento que distintas personas habrían estado ofertando esta información por distintos medios, principalmente en redes sociales. *"Esto es motivo de profunda preocupación para nuestro gremio en la medida que se pone en serio riesgo el desarrollo de las operaciones financieras que diariamente se realizan en el país y que compromete el patrimonio de todos los peruanos"*⁵, indicó el presidente de la Asbanc.

Según informaron los medios de prensa peruanos, el Registro Nacional de Identificación y Estado Civil (RENIEC), también habrían sido objeto de ataque por estos delincuentes cibernéticos ocasionando que en el mercado negro exista la oferta de datos sensibles que almacena dicha institución (huellas digitales, fichas RENIEC, números de DNI's).⁶

Este panorama nos obliga a replantear si es que nuestro marco normativo es el adecuado para afrontar este tipo de situaciones, si el grado de respuesta por parte de las instituciones encargadas es el más óptimo, pues del hecho antes mencionado, es una realidad que la Presidencia del Consejo de Ministros (PCM) y la Secretaría de Gobierno y Transformación Digital, si bien actuaron dentro de lo que le corresponde, mitigando los efectos, aún no han podido establecer estrategias para evitar y reforzar los sistemas de entidades públicas para evitar este tipo de ataques.

Como vemos, los sectores público y privado se han transformado digitalmente y se encuentran aplicando nuevas tecnologías, que si bien son necesarias también traen como consecuencia que busquen mejorar sus requerimientos en seguridad de Tecnologías de Información(TI), que muchas veces no son las más idóneas.

Por ejemplo de un total de 2,429 entidades del Estado, solo 164 cumplen con la implementación de equipos de respuesta; lo que significa que 9 de cada 10 simplemente no cumplen.⁷

⁵ Asbanc: ¿qué datos personales se habrían filtrado y se estarían comercializando en la web? (20 de mayo de 2022). *La República*. <https://larepublica.pe/sociedad/2022/05/20/asbanc-violacion-de-datos-posible-filtracion-de-datos-personales-de-que-plataformas-del-estado-se-filtro-datos-personales/>

⁶ Filtración de datos personales. qué dijo Asbanc y las medidas que ha tomado frente a este problema (22 de mayo de 2022). *El Comercio*. <https://elcomercio.pe/lima/sucesos/filtracion-de-datos-personales-conoce-que-dijeron-asbanc-reniec-y-las-medidas-que-ha-tomado-la-pcm-frente-a-este-problema-rmmn-noticia/?ref=ecr>

⁷ Miñán, W. (07 de enero de 2022). El 93% de entidades del Estado sin equipos ante incidentes de seguridad digital. *Diario Gestión*. <https://gestion.pe/tecnologia/el-93-de-entidades-del-estado-sin-equipos-ante-incidentes-de-seguridad-digital-noticia/>

Esta estadística también ha sido consignada por la página web oficial del Gobierno:

Tabla 1

Porcentaje de implementación del marco de confianza digital en distintos órganos del Estado

	Ministerios	Gobiernos Regionales	Organismos Constitucionales Autónomos	Gobiernos Locales
Oficial de seguridad y confianza digital	100 %	100 %	60%	16%
Equipo de respuesta ante incidentes de seguridad digital	100%	36 %	90%	20%
Sistema de Gestión de Seguridad de Información	53%	48 %	50%	13

Nota: Tomado de la Presentación sobre Marco de Seguridad y Confianza Digital en el Perú remitido por la Secretaría de Gobierno y Transformación Digital, ante la Comisión de Descentralización, Regionalización, Gobiernos Locales y Modernización de Gestión del Estado, de fecha 24 de mayo de 2022.

Claramente se observa que aún existe deficiencia en la organización por parte del sector público para implementar los principales ejes para una adecuada gestión de la ciberseguridad o seguridad digital. Lo que nos indica que aún no estamos debidamente preparados y ello parte por no solo instalar sistemas tecnológicos más seguros sino educar a la población en el tema y procurar la creación de un Consejo Nacional de Ciberseguridad y reforzar el Centro Nacional de Seguridad Digital.

Para entender el tema, citamos la importancia de definir algunos términos, entre ellos el del ciberataque:

El ciberataque es una operación cibernética, ya sea ofensiva o defensiva, que busca dañar o destruir a la víctima (Arts, 2019). Por otro lado, la seguridad es un bien público y la ciberseguridad es un activo colectivo (Brangetto y Kert-Saint Abuyn, 2015). Entonces, bajo estos conceptos, la ciberseguridad debe considerarse como un aspecto fundamental, no sólo para los gobiernos, sino que también para las organizaciones privadas que deben incorporarlo en sus planes estratégicos. (Citado por Consultoría Group, s.f.)⁸

⁸ Consultoría Group (s.f) LA CIBERSEGURIDAD Y SU RELEVANCIA EN EL FUTURO DE LAS ORGANIZACIONES EN EL PERÚ <https://www.consultoriagroup.com/blog/la-ciberseguridad-y-su-relevancia-en-el-futuro-de-las-organizaciones-en-el-peru/>

Los ataques más utilizados en la web conforme informan los expertos son: Malware, Virus, Gusanos, Troyanos, Spyware, AdWare, Ransomware, Doxing , Phishing y Denegación de servicio distribuido (DDoS).⁹

Entre los nuevos frentes que se encuentran en la mira de los delincuentes informáticos, se encuentra la "nube", que es una red sistematizada en donde se almacena la información de un determinado usuario a través de un servidor externo y que funciona a través del internet, evitando así colocar nuestra data dentro del almacenamiento local. Esta modalidad se encuentra implementada en los usuarios, entidades públicas, para citar un ejemplo: La Corte Superior de Justicia de todos los distritos judiciales implementaron la nube a fin de guardar data sobre procesos judiciales-en el caso concreto- procesos laborales, en donde se cuenta con un expediente digital.

Como podemos apreciar, estos ataques se encuentran dirigidos tanto a la sociedad civil, sector privado y público, por lo que no se debe escatimar en esfuerzos para establecer con los representantes de los actores involucrados para que puedan sumar a través de su experiencia y así fortalecer las políticas y estrategias en materias de seguridad digital o ciberseguridad.

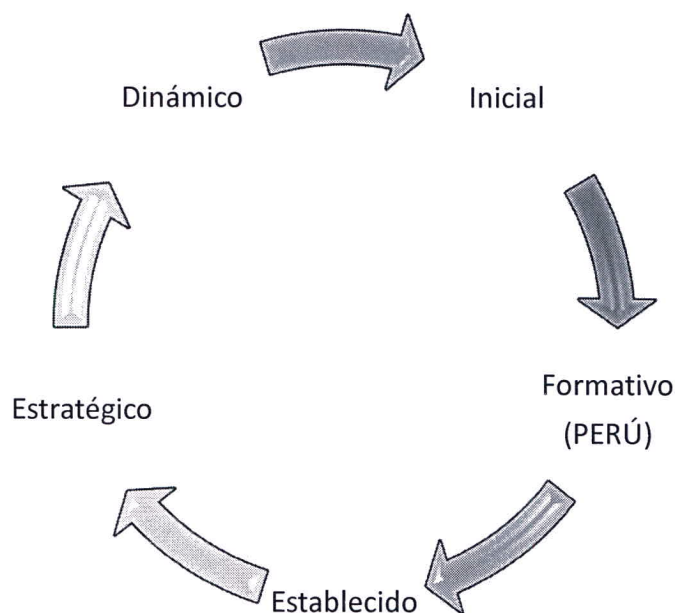
En ese sentido, el Centro Nacional de Seguridad Digital de Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, a través del Documento denominado Estrategia Nacional de Seguridad y Confianza Digital 2021-2026¹⁰ cita el reporte de Ciberseguridad 2020 de la Organización de los Estados Americanos(OEA) y el Banco Interamericano de Desarrollo(BID), que indica entre una de sus conclusiones que entre los países de Latinoamérica el Perú aún se encuentra en el nivel formativo respecto al nivel de madurez de la estrategia nacional de la ciberseguridad.

⁹Optical Networks (27 de diciembre de 2021) Tipos de ataques informáticos y previsiones para el 2022 <https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/>

¹⁰Centro Nacional de Seguridad Digital (s.f). Estrategia Nacional de Seguridad y Confianza Digital. Documento de Trabajo de la Estrategia Nacional de Seguridad y Confianza Digital 2021-2026. <https://cdn.www.gob.pe/uploads/document/file/1985045/Estrategia%20Nacional%20de%20Seguridad%20y%20Confianza%20Digital%20v1.5.pdf.pdf>

Figura 1

Niveles de madurez de la estrategia nacional de ciberseguridad en 10 países de Latinoamérica



Nota: Adaptado de Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020 de la Organización de los Estados Americanos(OEA) y el Banco Interamericano de Desarrollo(BID).¹¹

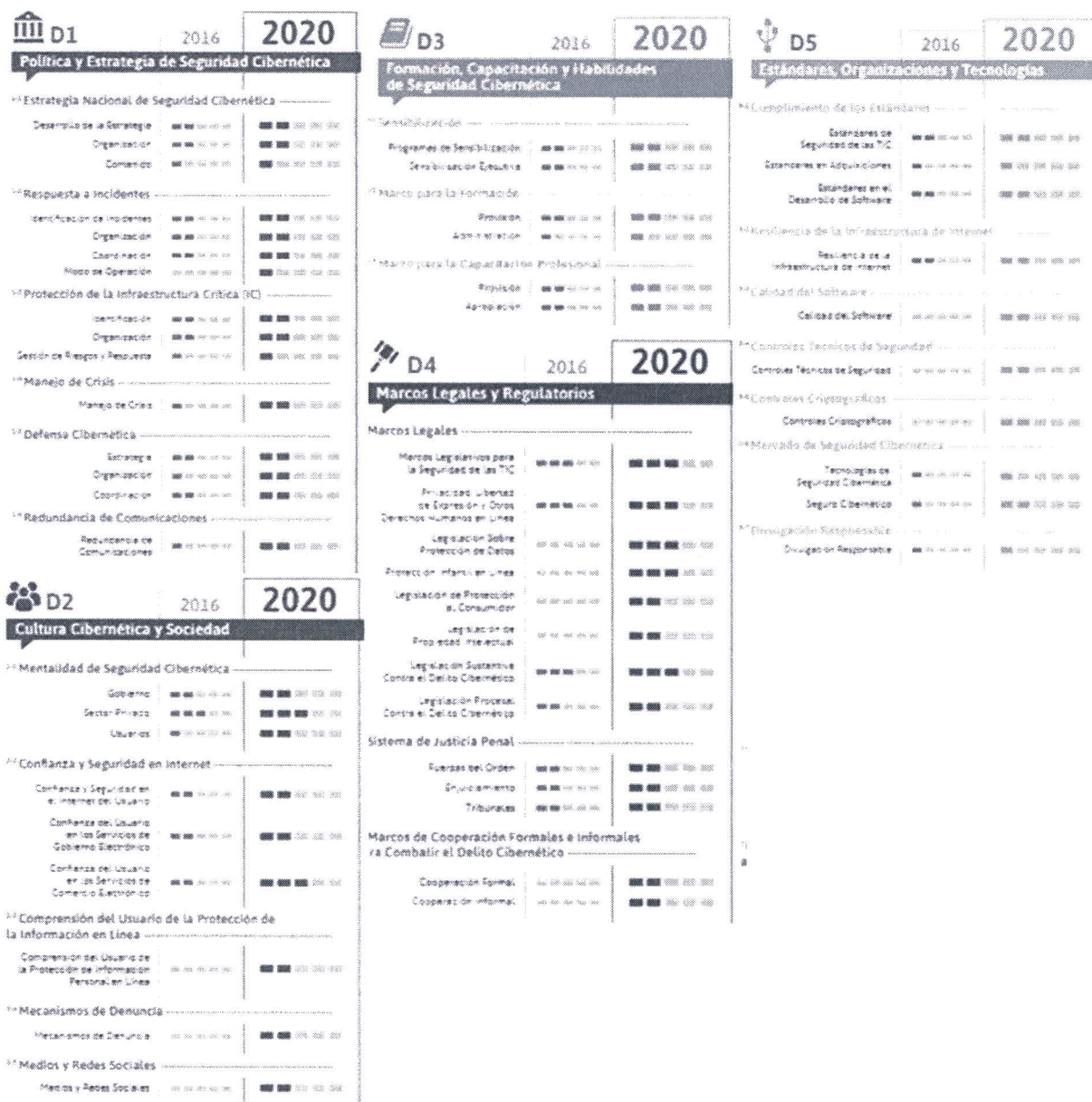
Estos indicadores se encuentran definidos dentro del mismo informe:

NIVEL		DESCRIPCIÓN
1	INICIAL	No se encuentra previsto nada en ciberseguridad o el mismo es un nivel básico.
2	FORMATIVO	No existe mucha evidencia en esa materia, existen características nuevas, casuales, desorganizadas, mal definidas
3	ESTABLECIDO	Elementos establecidos y funcionando, sin asignación de recursos
4	ESTRATÉGICO	Se han definido los indicadores claves, trabajando de acuerdo a los resultados proyectados
5	DINÁMICO	Instrumentos claros para acoplar la estrategia a las circunstancias imperantes. Respuesta inmediata

¹¹ Organización de Estados Americanos y Banco Interamericano de Desarrollo. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020. <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>

Figura 2

Análisis sobre el panorama en materia de ciberseguridad desde el año 2016 al 2020 en Perú



Nota: Adaptado de Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020 de la Organización de los Estados Americanos(OEA) y el Banco Interamericano de Desarrollo(BID).¹²

¹² Organización de Estados Americanos y Banco Interamericano de Desarrollo. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020.

De los indicadores antes referidos, se ven incrementos no tan significativos, lo que nos obliga a reflexionar que en el marco de seguridad digital aún existen deficiencias en sectores relevantes que no deben ser permitidos ya que nuestro país tiene un desarrollo digital muy álgido, esto motiva a que prioricemos adherirnos a políticas sólidas en materia de modernización de la gestión del Estado.

Un punto también que es importante señalar a señalar es que la Organización para la Cooperación y el Desarrollo Económico (OCDE) en su Estudio de Gobierno Digital en el Perú de la OCDE del año 2019 (Digital Government in Perú: Working Closely with Citizens) recomienda considerar el establecimiento de un Centro Nacional para gestionar los riesgos e incidentes de seguridad digital, conforme las mejores prácticas y las recomendaciones de la OCDE; además de señalar la necesidad de cooperación con el sector privado y otros actores relevantes en este entorno.¹³

Por último, mencionar como se encuentra normado la seguridad digital o ciberseguridad en el derecho comparado:

- **Alemania**

Cuenta con una Estrategia Nacional de Ciberseguridad, así como instituciones que se encargan de cumplir y establecer las principales políticas en la materia, estos organismos son el Consejo Nacional de Ciberseguridad, la Central Nacional para la Defensa Cibernética, así como la Oficina para la Seguridad de las tecnologías. Se destaca la participación del sector privado quienes también cuentan con instancias para afrontar este fenómeno.¹⁴

- **Brasil**

Se encuentra regulado la Estrategia Nacional de Seguridad Cibernética a través del Decreto N° 10.222/2020. En síntesis, el Decreto N° 10.222/20 presenta la Estrategia Nacional de Ciberseguridad y tiene como metodología el tratamiento de la ciberseguridad a través de un contexto de gobernanza con el fin de armonizar intereses y esfuerzos por parte de la administración pública, empresas privadas, investigadores de esa área del conocimiento y de la sociedad civil. La estrategia también está compuesta por acciones y objetivos que, en conjunto, proponen el perfeccionamiento de la estructura de ciberseguridad con el fin de promover la resiliencia del país frente a las amenazas en el entorno digital, como también su confiabilidad en el escenario internacional.¹⁵

<https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>

¹³ Dictamen recaído en el Proyecto de Ley N° 6544/2020. Periodo Anual de Sesiones 2020-2021. (15 de enero de 2021). Pg. 11.

¹⁴ Barrios, V. (2018). "Derecho Comparado de Ciberseguridad". Biblioteca del Congreso Nacional de Chile. Pág. 2. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26759/1/DERECHO_COMPARADO_CIBERSEGURIDAD.pdf

¹⁵ Neves, R, Charlita de Freitas, F., Cervieri, E., Euler, L., Almeida, M, (02 de agosto de 2021). *Regulación de la ciberseguridad en el sector de telecomunicaciones de Brasil: un balance de incentivos en un contexto de neutralidad tecnológica.* https://revistalatam.digital/article/210216/?utm_source=CLD&utm_medium=RLESD&utm_campaign=RLESD

- **Canadá**

Desde el año 2010, ya contaba con Estrategias en Ciberseguridad, destacamos de igual manera que institucionalmente Canadá tiene al Ministerio de Seguridad Pública, un Centro de Respuesta ante ciberincidentes.¹⁶

- **Estados Unidos**

Desde los ataques del 11 de setiembre de 2001, se impulsaron estrategias de una defensa territorial más activa y coordinada que culmina en noviembre de 2002 con la creación del Departamento de Seguridad del Territorio Nacional, (DHS), desarrollando una amplia legislación relacionada con la Ciberseguridad y la protección de infraestructuras críticas, la cual hasta el 2015.¹⁷

En términos de institucionalidad, la estrategia estadounidense establece la creación de la Oficina del Asesor Principal en materia de Ciberdefensa, del Secretario de Defensa, que interactuará con el Pentágono a través de un Consejo de Administración e Inversión Cibernética (CIMB), cuyo objetivo principal será coordinar y sincronizar todos los programas y actividades en materia de Ciberseguridad que se desarrollen desde el DOD, sin interferir en la cadena de mando.¹⁸

Como podemos observar es evidente que, a diferencia de otros países, aún existen puntos que reforzar en materia de seguridad digital o ciberseguridad, si bien dentro de la región y en general existen esfuerzos para fortalecer la gestión en ciberseguridad, pero los mismo aún no son del todo suficientes, en tal sentido, proponemos reforzar el marco normativo y fortalecerlo con los actores involucrados.

II. FUNDAMENTOS DE LA PROPUESTA

La solución al problema señalado en los acápites anteriores se compone por fortalecer el marco legal de ciberseguridad o seguridad digital y promoverlo a través de la creación de un Consejo Nacional de Ciberseguridad o Seguridad Digital, así como también fortalecer el Centro Nacional de Seguridad Digital, por lo que es necesario dar viabilidad al presente proyecto de ley.

¿Qué se logrará principalmente?

- *Es urgente ofrecer a la sociedad civil niveles de seguridad óptimos que les permita desarrollar sus actividades sobre todo aquellas referidas a la materia económica que se realizan en el ciberespacio, así como todas aquellas que involucren el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada, los datos personales y la propiedad.*

¹⁶ Barrios, V. (2018). "Derecho Comparado de Ciberseguridad". Biblioteca del Congreso Nacional de Chile. Pág. 5. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26759/1/DERECHO_COMPARADO_CIBERSEGURIDAD.pdf

¹⁷ Barrios, V. (2018). "Derecho Comparado de Ciberseguridad". Biblioteca del Congreso Nacional de Chile. Pág. 6. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26759/1/DERECHO_COMPARADO_CIBERSEGURIDAD.pdf

¹⁸ Barrios, V. (2018). "Derecho Comparado de Ciberseguridad". Biblioteca del Congreso Nacional de Chile. Pág. 7. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26759/1/DERECHO_COMPARADO_CIBERSEGURIDAD.pdf

- *Es urgente fortalecer los entes ya instituidos en aras resguardar la información que se encuentra dentro de las redes y sistemas informáticos del sector público y privado, específicamente las que son necesarias para el óptimo manejo del país.*
- *Es urgente coordinar la participación de actores tanto del sector público como privado para hacer sinergia con el objetivo de garantizar la creación de políticas sólidas que permitan hacer frente a todos los riesgos del ciberespacio.*

III. ANTECEDENTES LEGISLATIVOS

Es menester señalar que durante el período parlamentario 2016-2021, se introdujeron distintas propuestas legislativas con el objetivo de establecer el marco normativo en ciberseguridad. A continuación, enumeraremos aquellos que comparten espíritu normativo con la presente iniciativa legislativa:

Primera legislatura Ordinaria 2018

- Proyecto de ley N° 4237/2018-CR presentado por el grupo parlamentario Fuerza Popular, a iniciativa del congresista Carlos Domínguez Herrera.
- Proyecto de ley N° 4352/2018-CR, presentado por el grupo parlamentario Fuerza Popular, a iniciativa del congresista Jorge del Castillo Gálvez.

Ambos proyectos conjuntamente fueron objeto de Dictamen por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas, asimismo fue exonerado en segunda votación por Acuerdo de Junta de Portavoces, y fue aprobado por la Comisión Permanente, sin embargo, la autógrafa fue observada por el Poder Ejecutivo y no pudo ser promulgada.

Segunda Legislatura Ordinaria 2020

- Proyecto de Ley N° 6544/2020-CR, presentado por el grupo parlamentario Podemos Perú a iniciativa del congresista Daniel Urresti Elera.

Aclaremos que el referido proyecto fue también objeto de Dictamen por la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas, la misma cuya autógrafa fue observada por el Poder ejecutivo. En ese sentido, a la fecha no se ha promulgado ninguna ley en el sentido que proponemos.

IV. MARCO JURÍDICO

1. Ley N° 27309, Ley que Incorpora los Delitos Informáticos al Código Penal.
2. Ley N° 29733 de Protección de Datos Personales.
3. Ley N° 30096 de Delitos Informáticos.
4. Convenio Sobre la Ciberdelincuencia de Budapest.
5. Decreto Legislativo N° 1412, Ley de Gobierno Digital.
6. Decreto de Urgencia N° 006-2020, Sistema Nacional de Transformación Digital.

7. Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
8. Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
9. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital.

V. EFECTOS DE LA VIGENCIA DE LA NORMA QUE SE PROPONE EN LA LEGISLACIÓN NACIONAL.

Con la entrada en vigencia de la presente Ley, se promueve la creación del Consejo Nacional de Ciberseguridad o Seguridad Digital en el Perú, además se fortalecerá el Centro Nacional de Seguridad Digital. Se ha determinado de igual manera la modificatoria del artículo 7° del Decreto de Urgencia 007-2020, conforme se detalla a continuación:

Decreto de Urgencia N° 007-2020, redacción actual	Modificación propuesta
Artículo 7. Centro Nacional de Seguridad Digital 7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos. 7.2 El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos,	"Artículo 7.- Centro Nacional de Seguridad Digital 7. 1. Créase el Centro Nacional de Seguridad Digital como plataforma digital que deberá contar con infraestructura y se encargará de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer y asegurar la confianza en el entorno digital. Asimismo, es responsable de identificar, prevenir, reducir, tratar de manera inmediata, proteger, detectar, responder, recuperar, y recopilar, información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos. 7. 2. El Centro Nacional de Seguridad Digital se encuentra adscrito a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y se constituye en el Centro Nacional de Operaciones en Seguridad Digital lo que incluye la creación de herramientas legales y

centros o equipos nacionales e internacionales de similar naturaleza.

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

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

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

técnicas para garantizar la confianza en el entorno digital, la gestión de la plataforma Digital, el equipo de expertos en el campo de la seguridad digital, siendo único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

7. 3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano y el Marco de Confianza Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y el artículo 4 del presente Decreto de Urgencia.

7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a

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

7. 5 La Secretaría de Gobierno Digital, establece los protocolos de escalamiento, coordinación, intercambio y activación **inmediata** ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes."

VI. ACTORES INVOLUCRADOS

ACTOR	DEFINICIÓN
ESTADO PERUANO	- Principal involucrado, establece el marco normativo adecuado y óptimo para la promoción de la seguridad digital.
ADMINISTRADOS	- Participantes intrínsecos, quienes vienen desarrollando sus actividades dentro del mundo digital.
DEMÁS ESTADOS	- Con el que se articula e intercambia distintas estrategias para fortalecer el marco de la seguridad digital en el marco internacional.

VII. ANÁLISIS COSTO BENEFICIO

La presente iniciativa legislativa procura hacer más idóneo, necesario y ponderado el marco normativo respecto a la seguridad digital o ciberseguridad, fortaleciendo una institución ya creada, así como promover la creación de un ente que articule esfuerzos entre los sectores públicos y privados.

ACTOR	BENEFICIOS	
	POSITIVO	NEGATIVO
ESTADO PERUANO	Con la conformación de un Consejo Nacional de Seguridad Digital o Ciberseguridad en el que participen actores tanto del sector público y privado, afianzará nuestras estrategias en Seguridad Digital como país. Reforzará el Centro Nacional de Seguridad Digital, en aras de que no solo funcione como una plataforma digital.	Ninguno
ADMINISTRADOS	Podrán tener confianza y seguridad al realizar sus actividades en el mundo digital, asegurándose también de que sus derechos fundamentales serán protegidos.	Ninguno
DEMÁS ESTADOS	A través de la cooperación internacional se articulan esfuerzos para la implementación de mejores estrategias en seguridad digital o ciberseguridad y la lucha contra el ciberdelito.	Ninguno

VIII. EL PLAN RESCATE Y EL DECÁLOGO DE FUERZA POPULAR

El presente proyecto de ley se encuentra enmarcado dentro de los propósitos del Plan Rescate 2021 de Fuerza Popular, específicamente en el Pilar Estratégico 2: La Salud, Innovación e Investigación Científica, Eje 9: Gestión Pública Moderna y Descentralización.

IX. LA AGENDA LEGISLATIVA Y EL ACUERDO NACIONAL

Vinculación con el Acuerdo Nacional

La presente iniciativa se encuentra dentro del Primer Objetivo del Acuerdo Nacional, que dice: "Democracia y Estado de Derecho", específicamente en la Política de Estado 9, denominado "Política de Seguridad Nacional", que señala:

"9. Política de Seguridad Nacional

Nos comprometemos a mantener una política de seguridad nacional que garantice la independencia, soberanía, integridad territorial y la salvaguarda de los intereses nacionales. Consideramos que ésta es una tarea que involucra a la sociedad en su conjunto, a los organismos de conducción del Estado, en especial a las Fuerzas Armadas, en el marco de la Constitución y las leyes. En tal sentido, nos comprometemos a prevenir y afrontar cualquier amenaza externa o interna que ponga en peligro la paz social, la seguridad integral y el bienestar general. Con este objetivo el Estado: (a) fomentará la participación activa de toda la sociedad en su conjunto, en el logro de objetivos de la política de seguridad nacional; (...) (c) impulsará la enseñanza de los conceptos básicos de la seguridad nacional en todos los niveles del sistema educativo nacional; (...) y (e) mantendrá una estrecha coordinación entre el sistema de defensa nacional y la política exterior para la definición y defensa de los intereses permanentes del Estado.