CONGRESO DE LA REPÚBLICA
ÁREA DE TRAMITE Y DIGITALIZACIÓN DE DOCUMENTOS
23 OCT 2020
RECIBIDO
Firma..... Hora... 10:35

PROYECTO DE LEY QUE GARANTIZA LA EJECUCIÓN DE OPERACIONES DE CIBERSEGURIDAD Y SEGURIDAD DIGITAL A TRAVÉS DE UN CENTRO NACIONAL DE CIBERSEGURIDAD

Las y los Congresistas de la República, firmantes del Grupo Parlamentario **PODEMOS PERÚ,** en el pleno ejercicio del derecho de iniciativa legislativa reconocido en el artículo 107 de la Constitución Política del Perú y el numeral 2) del artículo 76 del Reglamento del Congreso de la República, proponen el siguiente proyecto de ley:

FÓRMULA LEGAL

EL CONGRESO DE LA REPÚBLICA;

Ha dado la presente Ley:

PROYECTO DE LEY QUE GARANTIZA LA EJECUCIÓN DE OPERACIONES DE CIBERSEGURIDAD Y SEGURIDAD DIGITAL A TRAVÉS DE UN CENTRO NACIONAL DE CIBERSEGURIDAD

Artículo 1.- Objeto

La presente ley tiene por objeto establecer medidas de carácter excepcional que garanticen la seguridad, en el ciberespacio frente a las amenazas o los ataques que afecten la Seguridad Nacional, para la ejecución de operaciones de Ciberseguridad y Seguridad Digital, a través del Centro Nacional de Ciberseguridad del Perú-CENACI.

Artículo 2.- Ámbito de aplicación

La presente Ley es aplicable a todas las entidades de la Administración Pública, comprendidas en el Artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS, a las organizaciones de la sociedad civil, sectores económicos y de servicios, ciudadanos y academia.

Artículo 3.- Objetivos

La presente ley persigue los siguientes objetivos:

1. Asegurar el máximo nivel de seguridad de la información que se genera en el ciberespacio y la infraestructura del estado.

2. Generar mecanismos de defensa y protección en el ciberespacio, de los intereses nacionales, los activos críticos nacionales y recursos claves de la nación, frente a las amenazas o los ataques que afecten la Seguridad Nacional.
3. Promover y garantizar la transparencia y seguridad digital de las entidades de la Administración Pública a los ciudadanos.
4. Promover la creación de un Centro Nacional de Ciberseguridad del Perú-CENACI, con el propósito de hacer frente a amenazas o ataques en el ciberespacio.

Artículo 4.- Definición

Para efectos de la presente Ley se consideran las siguientes definiciones:

4.1 Ciberseguridad. - Capacidad tecnológica que preserva la colección de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden utilizar para proteger la disponibilidad, integridad y confidencialidad de los activos en las infraestructuras pertenecientes al estado, organizaciones privadas y de los ciudadanos, ante amenazas y vulnerabilidades en el entorno digital.

4.2 Activos en la Infraestructura del Estado. - Es el conjunto de estructuras, instalaciones integradas a la operación de las tecnologías de la información y datos procesados en el entorno cibernético, incluida la infraestructura crítica como dispositivos informáticos conectados, infraestructura, aplicaciones, servicios, sistemas de acceso que son esenciales e imprescindibles para el normal desarrollo o funcionamiento de la vida en un país.

4.3 Seguridad Digital. - 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 y amenazas que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado, y otros quienes apoyan en la implementación de controles, acciones y medidas.

4.4 Gobierno Digital. - El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital; a fin de optimizar la

prestación y el acceso de los ciudadanos a los servicios públicos mediante el uso de las Tecnologías de la Información y la Comunicación (TIC).

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. - Declaración de interés nacional la creación del Centro Nacional de Ciberseguridad del Perú-CENACI.

Declárese de interés nacional y necesidad pública el fortalecimiento de la infraestructura del ciberespacio, a fin de salvaguardar la seguridad de las personas, los intereses nacionales, creándose un Centro Nacional de Ciberseguridad del Perú-CENACI.

Segunda. - Gestión y Coordinación Interinstitucional

Encargar a la Presidencia del Consejo de Ministros la conformación de una comisión multisectorial para reconocer y orientar la creación del Centro Nacional de Ciberseguridad del Perú-CENACI, a través de una Comisión Especial Multisectorial, que involucre la participación del Poder Legislativo, Judicial, el Consejo Nacional de Seguridad y Defensa (COSEDENA); y la participación del sector privado de telecomunicaciones y tecnología; entidades financieras y bancarías y la academia.

El Ministerio de Economía y Finanzas, deberá tener en cuenta el carácter público y esencial de la seguridad y defensa nacional, entre ellos la ciberseguridad, conforme lo señala la Política de Seguridad y Defensa Nacional, aprobada mediante Decreto Supremo N° 012-2017-DE.

Tercero. - Reglamento

La Presidencia del Consejo de Ministros, el Ministerio de Defensa y el Ministerio del Interior, mediante Decreto Supremo aprueban el Reglamento de la presente ley, en un plazo máximo de noventa (90) días contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

Primera. - Modificación del Decreto Legislativo Nº 1412, Ley de Gobierno Digital

Modifíquese los artículo 4, 8 y 30 del Decreto Legislativo Decreto Legislativo Nº 1412, Ley de Gobierno Digital; en los siguientes términos:

Artículo 4.- Finalidad
La presente Ley tiene por finalidad:

(...)

4.3. Optimizar la capacidad de respuesta de ciberseguridad para proteger la integridad, confidencialidad, activos en las infraestructuras pertenecientes al estado, privadas y de los ciudadanos.

Artículo 8.- Ente Rector en materia de Gobierno Digital
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital; ***en el ámbito de sus competencias como responsable exclusivo del gobierno digital***. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

Artículo 30.- De la Seguridad Digital
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 ***y amenazas*** que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

SEGUNDA. - Modificación del Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital

Modifíquese los artículos 7 y 8 del Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital, en los siguientes términos:

Artículo 7.- Ente rector del Sistema Nacional de Transformación Digital
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector del Sistema Nacional Transformación Digital, constituyéndose en la autoridad técnico-normativa a nivel nacional sobre la materia; ***en lo referido a gobierno digital.***

Artículo 8.- Funciones del ente rector
(...)
8.2 Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias; ***así también, las funciones del ente rector están referidas exclusivamente al gobierno digital.***

TERCERA. - Modificación del Decreto De Urgencia Nº 007-2020, Decreto de urgencia que aprueba el marco de Confianza Digital y dispone medidas para su Fortalecimiento

Modifíquese los artículos 3, 4, 5, 8, 9, 10, 11 y 13 del Decreto de Urgencia Nº 007-2020, Decreto de urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su Fortalecimiento, en los siguientes términos:

Artículo 3. Definiciones
(...)

h) Ciberseguridad. - Capacidad tecnológica que preserva ***la colección de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden utilizar para proteger la disponibilidad, integridad y confidencialidad de los activos en las infraestructuras pertenecientes al estado, organizaciones privadas y de los ciudadanos***, ante amenazas y vulnerabilidades en el entorno digital.

Artículo 4. Marco de Confianza Digital
(...)

c) Seguridad Digital. - La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de seguridad digital en el país, norma, dirige, supervisa y evalúa la materia de seguridad digital, ***en lo referido a gobierno digital.***

Artículo 5. Ente rector del Marco de Confianza Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos, ***en lo referido a gobierno digital.***

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

(...)

8.2.- El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad, ***solo en lo referido a gobierno digital.***

Artículo 9. Obligaciones del Proveedor de servicios digitales
(...)

a) Notificar al ***Centro Nacional de Ciberseguridad del Perú-CENACI*** todo incidente de seguridad digital.

9.2 Las organizaciones privadas toman como referencia las normas emitidas por la Secretaría de Gobierno Digital y del ***Centro Nacional de Ciberseguridad del Perú-CENACI*** en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.
9.3 Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital, y del ***Centro Nacional de Ciberseguridad del Perú-CENACI***.

Artículo 10. Articulación internacional
La Secretaría de Gobierno Digital ***y el Centro Nacional de Ciberseguridad del Perú-CENACI*** de la Presidencia del Consejo de Ministros coordina con el Ministerio de

Relaciones Exteriores las acciones vinculadas a la política exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias.

Artículo 11. Articulación en Materia de Comunicaciones
La Secretaría de Gobierno Digital ***y el Centro Nacional de Ciberseguridad del Perú-CENACI***.
de la Presidencia del Consejo de Ministros coordina con el Ministerio de Transportes y Comunicaciones las acciones vinculadas a la materia de comunicaciones en el marco de sus competencias.

Artículo 13. Centro Nacional de Datos
(...)
13.2 El Centro Nacional de Datos se encuentra a cargo de la Presidencia del Consejo de Ministros, a través ***del Centro Nacional de Ciberseguridad del Perú-CENACI*** y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.
...
13.4 La Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos, establece los protocolos y mecanismos en materia de gobierno de datos y emite los lineamientos y las directivas correspondientes; ***en lo referido a gobierno digital; mientras que el Centro Nacional de Ciberseguridad del Perú-CENACI; en el ámbito de sus competencias.***

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Única. - Adecuación de la presente ley. -

El Ministerio de Defensa priorizará y coordinará las medidas necesarias para salvaguardar la seguridad del ciberespacio, con el único objetivo de garantizar la integridad y confidencialidad de los activos en las infraestructuras pertenecientes al estado, organizaciones privadas y ciudadanos en general.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

Única. - Deróguese el artículo 7 del Decreto De Urgencia Nº 007-2020, que aprueba el marco de Confianza Digital y dispone medidas para su Fortalecimiento

Deróguese el artículo 7 del Decreto de Urgencia Nº 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su Fortalecimiento.

Lima, octubre de 2020

FIRMA DIGITAL
Firmado digitalmente por: URRESTI ELERA Daniel Belizario FIR 43883835 hard
Motivo: Soy el autor del documento
Fecha: 24/10/2020 01:13:53+0200

CONGRESO DE LA REPUBLICA

Lima, 02 de NOVIEMBRE del 2020

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición N° 6544 para su estudio y dictamen, a la (s) Comisión (es) de DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS

JAVIER ANGELES ILLMANN
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICION DE MOTIVOS

I. MARCO LEGAL

La Constitución Política del Perú establece que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado; asimismo, refiere que son deberes primordiales del Estado proteger a la población de las amenazas contra su seguridad, así como, garantizar la seguridad de esta última mediante el Sistema de Defensa Nacional. De otro lado, se protege que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar; ni que se atente contra el secreto y a la inviolabilidad de sus comunicaciones y documentos.

La Ley Nº 30999 Ley de Ciberdefensa, tiene como la finalidad la defensa y protección de la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional. La Ley de Ciberdefensa establece que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector de la seguridad digital en el país.

En ese sentido, el Decreto Legislativo Nº 1412, Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos digitales. Asimismo, define el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por las entidades de la Administración Pública en los tres niveles de gobierno.

No obstante, con Decreto de Urgencia N° 006-2020 se crea el Sistema Nacional de Transformación Digital, estableciendo el marco de gobernanza para la transformación digital en el país para integrar al sector público, privado y la academia en un "sistema", para promover la seguridad y confianza digital y por Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital para proteger las personas en el entorno digital, se integra a instituciones como el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), la Autoridad Nacional de Protección de Datos Personales, la Autoridad Nacional de Transparencia y Acceso a la Información Pública, la Presidencia del Consejo de Ministros en su calidad de ente rector de la Seguridad Digital; y crea el Centro Nacional de Seguridad Digital (CNSD).

Cabe señalar también que la Política de Seguridad y Defensa Nacional, aprobada con Decreto Supremo N° 012-2017-DE, identifica como sujetos de la Seguridad y Defensa

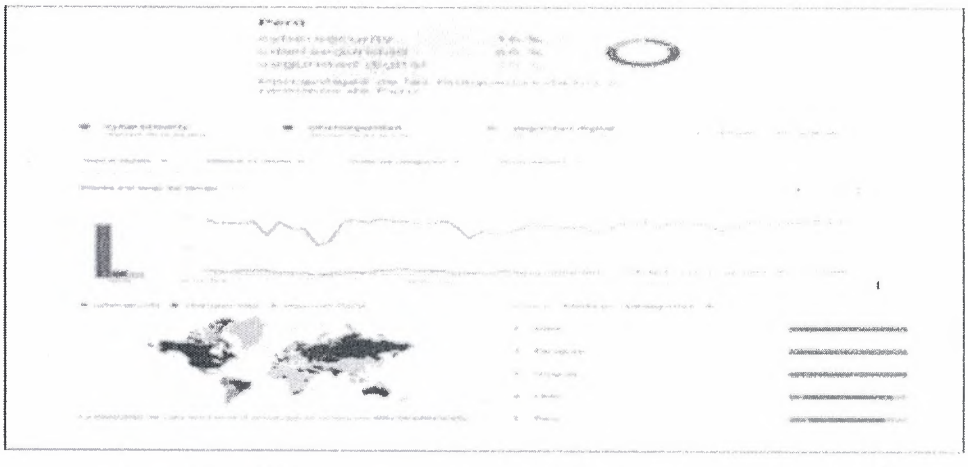
Nacional al Estado y a la persona humana. La problemática de la Seguridad Nacional incide en el desarrollo de otros problemas, generando efectos capaces de agravarla, incluso por la acción inadecuada o la inacción en su tratamiento. Las tecnologías de la información están cada vez más integradas a la operación de infraestructura física que puede ser dañada o interrumpida en su funcionamiento, poniendo en riesgo la economía y la sociedad.

La presente propuesta legislativa pretende hacer frente a la necesidad de contar con estrategias de ciberseguridad y planes de protección de infraestructura crítica que hagan frente a los riesgos y sus potenciales consecuencias, buscando proteger el ciberespacio y su infraestructura como un tema de Seguridad Nacional.

II. DEFICIONES DE CIBERSEGURIDAD Y SEGURIDAD DIGITAL

El termino ciberseguridad es ampliamente más conocido que el de seguridad digital, siendo así que, aunque pareciera que se estuviera hablando de lo mismo, cada término tiene un enfoque y una mirada distinta. La ciberseguridad por lo general está relacionado a todas las capacidades para hacer frente a los denominados ciberataques; sin bien, seguridad digital, versa sobre lo mismo, este último término se vincula más con todo lo relacionado a la interoperabilidad y de poner al servicio de los ciudadanos los "servicios" del Estado de manera digitalizada. La búsqueda por ejemplo de la palabra ciberseguridad en internet es más conocida que seguridad digital, incluso en nuestra región es uno de los más buscados, sea por querer saber de qué se trata la ciberseguridad, y otros por querer capacitarse en el tema. Así podemos mostrar según Google Trends en el motor de búsqueda de las palabras señaladas.

(Figura1)



Fuente:https://trends.google.com/trends/explore?q=cybersecurity,ciberseguridad,seguridad%20digitl

A modo de comparar ambos términos, la Unión Internacional de Telecomunicaciones (UIT) organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación–TIC, y que la mayoría de países toma como base esta definición; así como se indica en el artículo 30 del Decreto Legislativo N° 1412 Decreto Legislativo que aprueba la Ley de Gobierno Digital en el Perú, señalan lo siguiente:

CIBERSEGURIDAD	SEGURIDAD DIGITAL
Describe la colección de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden utilizar para proteger la disponibilidad, integridad y confidencialidad de los activos en los infraestructuras pertenecientes al gobierno, organizaciones privadas y ciudadanos. Estos activos incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y datos en el entorno cibernético.	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. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.
Fuente: Unión Internacional de Telecomunicaciones (UIT). La UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación – TIC.	Fuente: Artículo 30. Decreto Legislativo N° 1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital (13 de setiembre de 2018).

III. CONTEXTO SITUACIONAL QUE PROMUEVE LA CREACIÓN DEL CENTRO NACIONAL DE CIBERSEGURIDAD DEL PERÚ

Desde los últimos dos años en el Perú se viene promulgando algunos marcos normativos que tienen como propósito fundamental la protección de la seguridad digital del país. El Decreto Legislativo Nº 1412, Ley de Gobierno Digital (publicado el 13 de setiembre de 2018); señala que, la Secretaría de Gobierno Digital-SEGDI, es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y de gobierno electrónico; y es ese contexto, resulta necesario establecer el marco normativo que regule y habilite a las entidades del Estado *integrar de*

manera intensiva las tecnologías digitales para la prestación de servicios digitales en condiciones seguras, confiables, transparentes, interoperables en un entorno de gobierno digital[1]. Asimismo, se establece que la Secretaria de Gobierno Digital es el órgano rector de la Seguridad Digital en el Perú. El 26 de agosto de 2019, se promulga la Ley Nº 30999 Ley de Ciberdefensa, señala en la norma que su ámbito de aplicación se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional; y entiéndase por "ciberdefensa" *a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional*[2]. En cuanto al Decreto de Urgencia Nº 006-2020 y el Decreto de Urgencia Nº 007-2020 se dieron en el marco prepandemico COVID-19; sin embargo, fueron ratificados en la presente legislatura 2020-2021 del Congreso de la República.

Cabe mencionar que, en los últimos dos años en el Congreso de la República[3] se elaboraron tres proyectos de ley, referidos a la ciberseguridad y seguridad digital, que luego fueron materia de un dictamen por acumulación:

a) El proyecto de ley Nº 04237/2018-CR, *Ley que promueve la Seguridad Informática en el Perú y la conformación de un Consejo Nacional de Ciberseguridad*, presentado el 17 de abril de 2019, en donde señala que el objeto de la ley es *promover la seguridad informática en todo el territorio Nacional y la conformación de un Consejo Nacional de Ciberseguridad 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.*

b) Proyecto de ley Nº04344/2018-CR, *Ley que modifica el literal d) del artículo 10 del Decreto Legislativo 1186, que dota de herramientas tecnológicas a los efectivos policiales para que les permitan registrar sus actuaciones antes, durante y después de un operativo en el cumplimiento de sus deberes,* presentado el 16 de mayo de 2019, en donde se señala que el objeto es *modificar el literal a) del artículo 10 del Decreto Legislativo N° 1186, que dota de herramientas tecnológicas a los efectivos policiales para que les permitan registrar sus actuaciones antes, durante y después de un operativo en el cumplimiento de sus deberes.*

[1]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.
[2]https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/.
[3]http://www2.congreso.gob.pe/sicr/tradocestproc/Expvirt_2011.nsf/visbusqptramdoc1621/04352?opendocument.

c) Proyecto de ley Nº 04352/2018-CR, *Ley de Ciberseguridad*, presentado el 17 de mayo de 2019, cuyo objeto es *establecer el marco normativo en materia de Seguridad Digital del Estado Peruano,* documento que el Congreso de la República, remite el 20 de agosto de 2019 al Poder Ejecutivo. Mediante oficio Nº 244-2019-PR, del 11 de setiembre de 2019, el Poder Ejecutivo remite al Presidente del Congreso de la República, la observancia a la Autógrafa de Ley; y que, entre otros puntos refiere que *"... la Autógrafa resulta entonces contraria a los avances en gobernanza digital reconocidos por OCDE ocasionando un serio incumplimiento de las recomendaciones en materia digital al fraccionar la rectoría en seguridad digital, desconociendo lo establecido en la regulación vigente y poniendo en riesgo el cumplimiento de las recomendaciones para el ingreso del Perú a la OCDE...".*

Si bien, el Poder Ejecutivo, refiere que en materia de seguridad digital y "ciberseguridad" ya se encuentra normado, con la observancia de la Autógrafa de Ley, destacada líneas arriba, lo reafirman y sostienen que el Decreto Legislativo Nº 1412 Ley de Gobierno Digital, ya se establecen los principios vinculados con la "seguridad digital". El Ejecutivo también destaca que el Estudio de Gobernanza Pública de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) del año 2016, recomienda "establecer el gobierno digital en el centro de la reforma del sector público", y de esa manera, sostienen que es la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, la que concentra la rectoría en materia digital y, en particular, la seguridad digital, dando cumplimiento a los lineamientos de OCDE. Además, el fortalecimiento de la gobernanza digital en el Perú fue reconocido en el Estudio de Gobierno Digital en el Perú de la OCDE 2019[4]. Cabe destacar que según el último "Reporte de Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe del 2020", publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA)[5]; refieren que a pesar del progreso realizado en la región, en parte con el apoyo de la OEA, en donde en el año 2016 cuatro de cada cinco países ***carecían de estrategias de ciberseguridad o de un plan de protección de infraestructura crítica***; hoy en día, los gobiernos de la región son más conscientes de la necesidad de proteger el espacio digital del que depende el funcionamiento de nuestra sociedad; sin embargo, enfatizan que la ciberseguridad ***no ha ganado presencia en la agenda política de la región con la***

[4]https://leyes.congreso.gob.pe/Documentos/2016_2021/Observacion_a_la_Autografa/OBAU0423720190911.pdf.
[5]https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

urgencia que se esperaría; indican además que hasta principios de este año 2020, solo 12 países de la región, como Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) y Brasil (2020), *han aprobado una* ***estrategia nacional de ciberseguridad, y únicamente (solo) 10 países han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad.*** El informe señala que este mínimo avance en la región se debe también por la ausencia del talento humano calificado en asuntos de ciberseguridad; indican además que la *brecha de profesionales en ciberseguridad se estima en 600.000 personas en la región... frente a esta escasez, únicamente 20 de los países estudiados cuentan con alguna oferta académica en ciberseguridad*[6].

Es necesario destacar que a pesar de los avances que el Estado Peruano ha venido realizando últimamente respecto a la seguridad digital, la pandemia del COVID-19, ha desnudado las falencias que tenemos como Estado, y más aún para adecuarnos a las exigencias que el mundo cibernético demanda; en ese sentido, se requiere también un cambio de paradigma en la cooperación público-privada -como señala el Reporte de Ciberseguridad-2020-, por ser el entorno digital *de naturaleza intrínsecamente compleja* y de partes interesadas. *La digitalización ha transformado nuestra sociedad en un "sistema de sistemas", donde las funciones críticas se distribuyen entre los actores públicos y privados*; es así que en los últimos años la *cooperación público-privada en materia de ciberseguridad requiere pensar fuera de los formatos tradicionales y rígidos para superar las barreras y ser verdaderamente efectivos*. (Nayia Barmpaliou, Jefa de Políticas e Iniciativas Públicas, Centro para la Ciberseguridad, Foro Económico Mundial)[7].

La ciberseguridad de estos tiempos, como señala Farah Diva Urrutia Secretaria de Seguridad Multidimensional de la OEA, experimentará múltiples oportunidades, *en donde la puesta en práctica de políticas integrales de ciberseguridad permitirá a los países de nuestra región disfrutar de los beneficios de la Cuarta Revolución Industrial, protegiendo a sus ciudadanos y potenciando su actividad económica*[8]. Los cibercriminales y por tanto el ciberdelito no tienen fronteras, basta una computadora y tener acceso a una red de internet para causar enormes daños; por lo que, tanto las personas como las instituciones

[6] BID-OEA: Reporte de Ciberseguridad-2020, pág. 11.
[7] BID-OEA: Reporte de Ciberseguridad-2020, pág. 32.
[8] https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

están expuestas al delito cibernético; según Farah Diva, "se deben hacer esfuerzos de naturaleza multidimensional, *porque se requiere una variedad de factores para construir una cibersociedad resistente; y crear una cultura de ciberconciencia, y capacitar a profesionales calificados para construir una estrategia de ciberseguridad*".

Según el Informe de Cibercrimen ThreatMetrix , América Latina es *un foco para realizar fraude en la creación de cuentas* (alrededor del 20%), en relación al resto del mundo (12,2%), lo cual de cierta manera propicia un ambiente de mayor riesgo y vulnerabilidades en el espacio digital en América Latina y el Caribe, como lo señalan Miguel Porrúa del BID, y Belisario Contreras de la OEA[9]; además los ciberataques en esta parte de la región han ido en aumento afectando principalmente a las instituciones financieras.

Según Pawel Herczynski Director Gerente de PCSD y Respuesta a Crisis, Servicio Europeo de Acción Exterior, señala que la ciberseguridad es crítica para nuestra prosperidad y seguridad, en donde no sólo amenazan las economías del mundo, sino también el funcionamiento de las democracias, libertades y valores; por lo que es *necesario protegernos contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros.*

Para Sven Mikser, Ministro de Relaciones Exteriores, de la República de Estonia, refiere que, en la última década, han surgido diversas amenazas en el ciberespacio *que requieren la atención de los gobiernos de todo el mundo*. Las mismas que tienen que ver *con la creciente inestabilidad causada por el delito informático, las intrusiones en redes críticas y las operaciones motivadas políticamente*. Si bien, estos elementos han estado o están en proceso de implementación en las agendas políticas de los Estados de todo el mundo, difiere mucho entre los Estados; por lo que es necesario armonizar esfuerzos de los Estados para aumentar su ciberseguridad; y se requiere *incentivar a los Estados para que cooperen en un campo que convencionalmente se consideraría un área relacionada con sus asuntos internos*. Por otro lado, como señala Rodrigo Guillen en "Redes 5G Calentando la Nueva Guerra Fría"[10], mientras la economía digital sigue evolucionando a una velocidad vertiginosa, impulsada por la capacidad para recopilar, utilizar y analizar un volumen masivo de información que se realizan en diversas plataformas digitales, en donde el tráfico de datos mundial a través del Protocolo de Internet (IP), pasó de unos 100

[9] BID-OEA: Reporte de Ciberseguridad-2020: Miguel Porrúa Especialista Principal en Gobierno Digital, Coordinador del Grupo de Datos y Gobierno Digital del BID, y Belisario Contreras Gerente del Programa de Ciberseguridad de la OEA, pag. 16-18.

[10] Centro de Altos Estudios Nacionales. Cuadernos de Trabajo - Número Extraordinario 6: https://drive.google.com/file/d/1LRX8PnLxJ6mo_Od_kO4vR52cbub2SZ7K/view?fbclid=IwAR3yA20dVHgQNhpa_Xaoi7QAtdjr38ZnWBOwnDn9siOR_C7a_7XyIm2FDNo.

gigabytes (GB) al día en 1992 a más de 45,000 GB por segundo en 2017; se espera que para 2022 el tráfico IP mundial alcance unos 150.700 GB por segundo; hace que la inmensa infraestructura tecnológica de computadoras, redes LAN, WAN, dispositivos móviles, sistemas de transmisión inalámbrica y por cable, centros de datos, sistemas de satélites; y otros dispositivos; estén aún más vulnerables a los ciberataques. Asimismo, señala el autor que el predominio global de la economía digital ha reflejado una disputa comercial entre los Estados Unidos y China que ha obligado a las empresas y gobiernos de los países involucrados a rediseñar sus estrategias de seguridad Digital.

Por último, para Nayia Barmpaliou, Jefa de Políticas e Iniciativas Públicas del Centro para la Ciberseguridad del Foro Económico Mundial, señala que la ciberseguridad en la era de la hiperconectividad y de las pandemias, *marcará un punto de inflexión fundamental en la senda mundial y ha acentuado como nunca antes nuestra dependencia de la infraestructura digital*. Siendo así, se pensaba que la transformación digital iba a ocurrir en 3 años, pero, en los primeros meses de la pandemia se experimentó una aceleración en la puesta en operación la transformación digital; y por ende, reconfigurar nuestra vida profesional y personal; siendo evidente que *en el contexto de un ecosistema digital de vulnerabilidades;* donde *los cibercriminales aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas, trajo consigo un aumento de ataque cibernético.*

En el Reporte de Ciberseguridad-2020 referente al Perú, indica que: "*si bien Perú aún no cuenta con una Estrategia Nacional de Seguridad Cibernética, sí ha puesto en marcha una política nacional de ciberseguridad que, entre otras cosas, destaca la necesidad de crear una estrategia nacional de ciberseguridad y un comité nacional de ciberseguridad*". Por otro lado, el Convenio sobre Cibercrimen del Consejo de Europa (o "Convenio de Budapest"), *está referido a promover una política penal común contra el cibercrimen,* para ofrecer un marco común en las legislaciones de los países miembros.

Se requiere dar un giro y un enfoque de 360 grados para cambiar el paradigma y armonizar con el real nivel de capacidades de ciberseguridad que tenemos como país; no solo es suficiente realizar avances en las políticas de ciberseguridad y gobierno digital, en donde este último punto, pareciera se lo mismo, pero no lo es. Por último, cabe resaltar

que según el Reporte de Ciberseguridad-2020 del BID-OEA, señala que *únicamente 7 países de los 32 analizados en este reporte cuentan con un plan de protección de su infraestructura crítica, y 20 han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT. Esto limita la capacidad de identificar ataques y responder oportunamente a los mismos*.

Por lo que, nuestra propuesta de declarar de preferente interés nacional y necesidad pública la creación del Centro Nacional de Ciberseguridad del Perú-CENACI, será un hito valioso para replantear nuestras estrategias como país; por lo que se requiere una auténtica Estrategia Nacional de Ciberseguridad para funcionar como un principal instrumento centralizador que debe tener el Estado peruano para hacer frente a las diversas amenazas que afecten nuestro ciberespacio.

IV. CARACTERISTICAS DEL CENTRO NACIONAL DE CIBERSEGURIDAD DEL PERÚ

El Centro Nacional de Ciberseguridad del Perú-CENACI:

- Es una entidad adscrita y dependerá jerárquicamente de la Presidencia del Consejo de Ministros. Su titular es el Presidente Ejecutivo designado por la Presidencia del Consejo de Ministros.
- Es un órgano de línea, con autoridad técnico normativa a nivel nacional; y autonomía administrativa, funcional y económica; constituye pliego presupuestal propio.
- Es el órgano rector del Sistema Nacional de Ciberseguridad.

  La ejecución de su presupuesto no significa de modo alguno la ejecución de actividades que no son propias de sus funciones, y de sus características del porque y necesidad de su creación.
- Es responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Ciberseguridad.
- En el reglamento de ley de su creación se detallará en forma específica las responsabilidades y funciones, y se establecerá los límites para estos efectos.

V. GESTIÓN PARA EL CENTRO NACIONAL DE CIBERSEGURIDAD DEL PERÚ

A efectos de la gestión para el Centro Nacional de Ciberseguridad del Perú-CENACIP, se propone la conformación de una comisión multisectorial para reconocer y orientar la creación del Centro Nacional de Ciberseguridad del Perú-CENACI, a través de una Comisión Especial Multisectorial, que involucre la participación del Poder Legislativo, Judicial, el Consejo Nacional de Seguridad y Defensa (COSEDENA) y la participación del sector privado de telecomunicaciones y tecnología; entidades financieras y bancarías y la academia.

Cabe señalar que, a partir del análisis e investigación sobre entidades nacionales como extranjeras, así como lo señalado en el proyecto de ley No 04352/2018-CR, Ley de Ciberseguridad, podemos determinar que el Centro Nacional de Ciberseguridad-CENACIP puede ser el ente rector en políticas de ciberseguridad y seguridad digital, y como tal se constituirá en el órgano coordinador de los aspectos de ciberseguridad y seguridad digital de la Presidencia del Consejo de Ministros, a fin de contar con los procedimientos y capacidades para asegurar las operaciones y respuestas a incidentes de ciberseguridad y seguridad digital, que puedan afectar las sedes digitales, datos, activos críticos nacional y recursos claves, contra amenazas y riesgos en y a través del entorno y seguridad digital de la nación.

Es fundamental que el Estado pueda formular, diseñar, implementar y fiscalizar el cumplimiento de la Estrategia Nacional de Ciberseguridad y el plan multianual en Ciberseguridad; fortalecer el ecosistema de ciberseguridad para disminuir riesgos y vulnerabilidades inherentes a la tecnología; delimitar los marcos de referencia para fortalecer la ciberseguridad de entidades públicas, privadas, academia y sociedad en general; brindar soporte y capacitación técnica en el ámbito de la ciberseguridad a las entidades de la administración pública en todo el territorio nacional; ser la última instancia administrativa en materia de ciberseguridad; garantizar el cumplimiento cabal de la seguridad de la información y datos personales, tanto en la administración pública como en el sistema privado las políticas y lineamientos que se establezcan respecto a la ciberseguridad; supervisar a aquellas instituciones y entidades que no cumplan con la implementación y ejecución de las políticas de ciberseguridad correspondientes o que no informen de las incidencias, ataques o vulneraciones informáticas que sufran.

Cabe destacar que, para tales efectos se deberá modificar y rediseñar los alcances del Decreto Legislativo Nº 1412, Ley de Gobierno Digital, para lo cual la Secretaria de Gobierno Digital, orientará el marco de gobernanza del gobierno digital para la adecuada gestión de los servicios digitales e interoperabilidad que permita el uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

De otro lado, es necesario contar con una Estrategia Nacional de Ciberseguridad que:

- Establezca los objetivos estratégicos y lineamientos orientadores para la formulación de los Planes de Ciberseguridad de las diferentes entidades que conforman el Comité Nacional de Ciberseguridad.
- Determine las capacidades que deben disponerse para asegurar un óptimo funcionamiento y operación de la Ciberseguridad, Ciberdefensa y Ciberinteligencia; en concordancia con los lineamientos y estrategias de la Secretaría de Gobierno Digital en materia de informática y de Gobierno Electrónico; con el fin de garantizar la Ciberseguridad y Seguridad Digital como parte de la Seguridad Nacional y como soporte para el logro de los Objetivos Nacionales.
- Oriente los procedimientos operativos y protocolos para la acción de las entidades que conforman el Comité Nacional de Ciberseguridad, con el único propósito de garantizar una eficaz gestión de la Ciberseguridad en el país.
- Busque la participación activa de todos las entidades y organizaciones, tanto del sector público, privado y de la academia; orientando sus esfuerzos y actuación en provecho de garantizar el ciberespacio a nivel nacional, así como emplear sinérgicamente las diversas capacidades en Ciberseguridad para una óptima gestión de los riesgos en concordancia con la Secretaria de Gobierno Digital.
- Considere como parte de sus estrategias de acción la cooperación internacional y asistencia técnica mutua en aspectos relacionados con la Ciberseguridad.
- La necesidad de recursos financieros como el soporte de diferentes fuentes de financiamiento y presupuestos disponibles, en relación a las pérdidas económicas que podrían sufrir las sedes digitales, datos, activos críticos nacional y recursos claves; a consecuencia de la afectación por incidentes y ataques a la seguridad digital o acciones de amenazas a la seguridad nacional en o a través de otros entornos digitales, las mismas que afecten la Ciberseguridad de la nación.

Secretaria de Gobierno Digital:

La Secretaría de Gobierno Digital, como está establecido en el Decreto Legislativo Nº 1412, es el órgano de línea, con autoridad técnico normativo a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y de Gobierno Electrónico. La Secretaría de Gobierno Digital es una entidad orgánica adscrita a la Presidencia del Consejo de Ministros, y órgano rector de la Seguridad Digital; del Sistema Nacional de

Transformación Digital y administra las Plataformas Digitales del Estado Peruano; lidera los procesos de innovación tecnológica y de transformación digital del Estado; y, siguiendo las recomendaciones de la OCDE en materia de gestión de riesgos de seguridad digital, el Perú ya tiene un arreglo institucional que permite regular, dirigir, orientar y supervisar la Seguridad Digital en el país, el cual es gestionado por la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital, tal como se establece en el Decreto Supremo Nº 022-2017-PCM, Decreto Legislativo Nº 1412 y Ley Nº 30999.

De otro lado, el Perú cuenta con un CSIRT nacional, denominado PeCERT, en donde a través de un informe y análisis técnico indican los distintos ataques a la seguridad de la información de entidades públicas y empresas privadas en el ciberespacio. El documento es preparado por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM), el Comando Conjunto de las Fuerzas Armadas, el Ejercito del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, entre otras instituciones(Fuente: https://cdn.www.gob.pe/uploads/document/file/1373500/Alerta%20integrada).

VI. MODELO DE MADUREZ DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LAS NACIONES" (CMM)

Antes de pasar al Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones-CMM, es importante señalar que, en el Perú, el acceso a internet lo tiene alrededor de 15 millones de ciudadanos, y un porcentaje del 49% de cobertura de internet en el país (Figura 5).

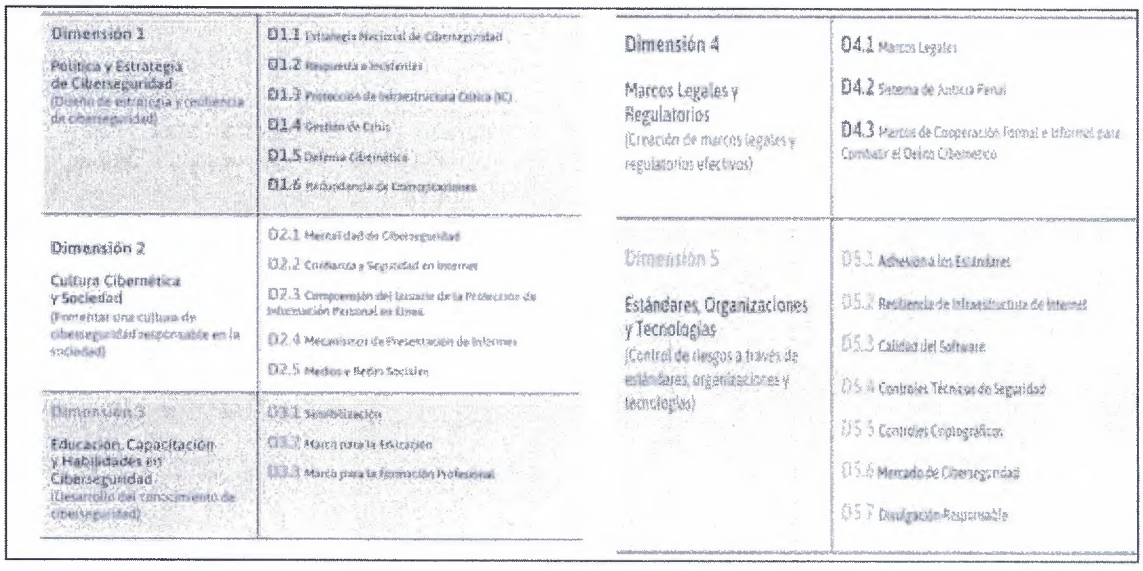
Figura 5

Fuente: Reporte de Ciberseguridad-2020 del BID-OEA (pág.142)

El Reporte de Ciberseguridad-2020 del BID-OEA, señala que para medir un país respecto a sus capacidades de ciberseguridad toma en cuenta el "Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones" (CMM, por sus siglas en inglés) modelo desarrollado por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC) de la Universidad de Oxford, en donde se fija un medio de evaluación que sigue cinco etapas (Figura 6), con el propósito de medir de manera confiable la capacidad de seguridad cibernética, siendo así que se tiene: inicial (política y estrategia de ciberseguridad); formativa (cultura cibernética y sociedad); consolidada (educación, capacitación y habilidades en ciberseguridad); estratégica (marcos legales y regulatorios); y dinámica (estándares, organizaciones y tecnologías).

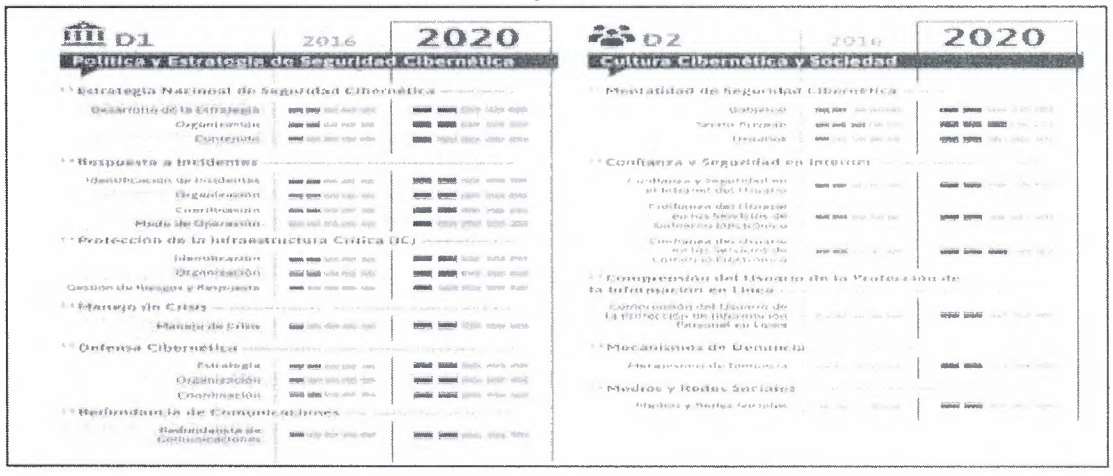
Figura 6

Fuente: Reporte de Ciberseguridad-2020 del BID-OEA (pág.43-44)



Estos son los indicadores que señala el "Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones" (CMM), para el Perú con el propósito de medir la capacidad de seguridad cibernética, entre ellas podemos notar que respecto al año 2016 frente al 2020, ha habido ligeros avances, tal como se observan en la figura 7 y en la 8 respecto a los demás países de como gestionan su CSIRTs.

Figura 7



Fuente: Reporte de Ciberseguridad-2020 del BID-OEA (pág.181-183)

VII. ANALISIS COSTO BENEFICIO

La presente propuesta legislativa no irrogará gasto al erario nacional, tiene como finalidad poner de manifiesto ante el Poder Ejecutivo la importancia de declarar de interés nacional y necesidad pública la creación del Centro Nacional de Ciberseguridad del Perú, cuyo beneficio está relacionado a la protección de la nación respecto a la ciberseguridad, y de esa manera manejarse a la luz de los tiempos que demanda con urgencia contar con una agencia especializada en ciberseguridad. De aprobarse la propuesta se contribuirá a la Seguridad y Defensa Nacional; lo que permitirá que el País esté a la vanguardia y permitirá la protección de los intereses ciudadanos, de las entidades públicas y privada y la sociedad en su conjunto, lo que beneficiará a la población y al país.

VIII. EFECTOS DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa se ampara en el respeto irrestricto de la Constitución Política del Perú, en lo referido a la defensa de las personas, el derecho a la justicia y el respeto de su dignidad como fin supremo de la sociedad y del Estado; y de la normatividad existente en nuestro ordenamiento jurídico.

IX. VINCULACIÓN CON EL ACUERDO NACIONAL.

El proyecto de ley se enmarca con la séptima política de Estado expresada en el Acuerdo Nacional, denominada: Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana; que promueve normar y fomentar las acciones destinadas a fortalecer el orden público y el respeto al libre ejercicio de los derechos y al cumplimiento de los deberes individuales; así como en la novena política de Estado denominada Política de Seguridad Nacional; y en la vigésima política de Estado denominada Desarrollo de la ciencia y la tecnología.