Proyecto de Ley N° 4237/2018-CR

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
17 ABR 2019
CARLOS ALBERTO DOMÍNGUEZ HERRERA
RECIBIDO
Firma Hora 9:53

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año de la Lucha Contra la Corrupción y la Impunidad"

LEY QUE PROMUEVE LA SEGURIDAD INFORMÁTICA EN EL PERÚ Y LA CONFORMACIÓN DE UN CONSEJO NACIONAL DE CIBERSEGURIDAD

El **Grupo Parlamentario Fuerza Popular**, a iniciativa del Congresista de la República, **Carlos Alberto Domínguez Herrera** 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:

CONGRESO DE LA REPÚBLICA * CARLOS DOMINGUEZ HERRERA *

FÓRMULA LEGAL

LEY QUE PROMUEVE LA SEGURIDAD INFORMÁTICA EN EL PERÚ Y LA CONFORMACIÓN DE UN CONSEJO NACIONAL DE CIBERSEGURIDAD

Artículo 1°.- Objeto de la Ley
La presente Ley, tiene por objeto 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.

Artículo 2°.- Principios Rectores de la Ley
La presente ley se rige por los siguientes principios:

1. **Colaboración multidisciplinaria multisectorial e inter institucional:**
   Enfoque basado en la colaboración multidisciplinaria de los diferentes niveles de gobierno y poderes del Estado en materia de ciberseguridad, que permita el desarrollo integral, transversal de la estrategia y facilite la participación de todos los involucrados.

2. **Respeto a los derechos humanos:**
   Contemplar en las diferentes acciones en materia de ciberseguridad la promoción, respeto y cumplimiento de los derechos humanos; entre otros, la libertad de expresión, el acceso a la información, el respeto a la vida privada, la protección de datos personales, la salud, educación y trabajo.

3. **Enfoque basado en gestión de riesgos:**
   Contar con la capacidad de manejar escenarios de incertidumbre por medio de enfoques preventivos y correctivos, con la intención de minimizar el impacto de las cambiantes amenazas y riesgos del ciberespacio.

328779-ATD

Artículo 3°.- De las Políticas de Seguridad Informática
La Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital, establece el fortalecimiento de las políticas de seguridad informática en todos los organismos de la administración pública.

Artículo 4°.- Condiciones mínimas para la implementación de la Ciberseguridad
Las condiciones mínimas para la implementación de la ciberseguridad son las siguientes:

4.1. Asegurar la ciberresiliencia bajo un enfoque de gestión de riesgo con mecanismos y protocolos claros para la recuperación de los sistemas.

4.2. Sistematizar las normas en materia de ciberseguridad con rango de ley, provenientes de todos los niveles del Estado, a fin de garantizar la protección de datos personales, estimulando el que se pueda compartir información y que dote a la Policía Nacional de herramientas adecuadas para su cumplimiento.

CONGRESO DE LA REPÚBLICA
CARLOS DOMÍNGUEZ HERRERA

4.3. Clasificar información, métricas de ciberseguridad, capacitación en continuidad de ciberresiliencia y realización de pruebas de vulnerabilidades.

4.4. Establecer criterios, normas y metodologías para la generación, uso y adopción de hardware y software con la finalidad de fortalecer el ecosistema de ciberseguridad y disminuir riesgos y vulnerabilidades inherentes a la tecnología.

4.5. Desarrollar un marco jurídico nacional vinculado a la ciberseguridad y de autorregulación; por parte de los concesionarios y distribuidores de servicios de Tecnologías de la Información y Comunicación - TIC, incluida la modificación a efecto de brindar certeza jurídica al actuar de los intermediarios de Internet, y la sociedad en general, con ajuste al derecho nacional, los acuerdos, convenios y tratados internacionales de la materia.

Artículo 5°.- Principales Objetivos de la Ciberseguridad en el Perú
Los principales objetivos de la ciberseguridad en el Perú son:

5.1. Resguardar la seguridad de las personas en el ciberespacio.
5.2. Proteger la seguridad informática del país.
5.3. Promover la colaboración y coordinación entre instituciones.
5.4. Gestionar los riesgos del ciberespacio.
5.5. Identificación y jerarquización de las infraestructuras críticas de la información.
5.6. Protección de las infraestructuras críticas de la información.
5.7. Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

5.8. Establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales de la materia.
5.9. Promover el desarrollo de la industria de ciberseguridad y el desarrollo digital del país, dando énfasis en la generación de oferta por parte de la industria local y demanda por parte del sector público en base a los intereses estratégicos del Estado.

Artículo 6°.- Del Comité de Respuesta ante Ciberdelincuencia
Promuévase la creación de un Comité de Respuesta ante Ciberdelincuencia (CORECY), como una dependencia del Consejo Nacional de Ciberseguridad, el cual, dentro de las funciones que se le asignen, se encargará de ser la primera fuente de respuesta y ayuda ante las dificultades de seguridad informática y los ciberataques que se realicen a cualquier entidad de la administración pública y privada, y de la recepción de denuncias de los afectados por contenido ilegal que se difunda a través de Internet incluyendo los llamados "troleos" informáticos que tengan como fin perturbar las buenas costumbres, el orden público y la correcta prestación de los servicios de la administración pública.

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

Artículo 7°.- Obligatoriedad de la información de incidencias y acciones correspondientes.
En el marco de la competencias de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, las entidades de la administración pública y privada, estará obligada a reportar ante el Consejo Nacional de Ciberseguridad correspondiente, los incidentes, ataques y/o vulneraciones cibernéticas que hayan sufrido y sobre las acciones correspondientes tomadas para la solución de los mismos, dentro de los plazos que este comité establezca.

Las instituciones del sector público o privado están obligadas a proteger las infraestructuras críticas de la información, en especial los datos y data sensible de los administrados y/o clientes que tengan almacenados, asegurando el correcto tratamiento de los mismos.

Artículo 8°.- Promoción de la creación del Consejo Nacional de Ciberseguridad
Promuévase la creación del Consejo Nacional de Ciberseguridad (CONACY), cuya conformación deberá contar con las siguientes entidades:

8.1. Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital (SEGDI) quien la preside.
8.2. Poder Judicial
8.3. Dirección Nacional de Inteligencia (DINI)
8.4. Ministerio de Defensa (MINDEF)
8.5. Ministerio del Interior (MININTER)
8.6. Ministerio de Transportes y Comunicaciones (MTC)
8.7. Policía Nacional del Perú (PNP)
8.8. Asociación de Gobiernos Regionales

8.9. Sociedad Nacional de Industrias (SNI)
8.10. Asociación de Bancos del Perú (ASBANC)
8.11. Asociación para el Fomento de la Infraestructura Nacional (AFIN)
8.12. Red Científica Peruana (RCP).
8.13. Cámara de Comercio de Lima (CCL) (OBS)
8.14. Cámara Nacional de Comercio, Producción, Turismo y Servicios – PERUCÁMARAS
8.15. Colegio de Abogados de Lima (CAL)
8.16. Colegio de Ingenieros del Perú (CIP)
8.17. NAP (Network Access Point) Perú
8.18. Confederación Nacional de Institucionales Empresariales Privadas (CONFIEP)

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

Artículo 9°.- De las funciones del Consejo Nacional de Ciberseguridad
El Consejo Nacional de Ciberseguridad ejercerá las siguientes funciones:

9.1. Formular, diseñar, implementar y fiscalizar el cumplimiento de la Estrategia Nacional de Ciberseguridad y el plan multianual en Ciberseguridad.
9.2. Formar parte de los foros y/o tener representantes en los encuentros, acuerdos y todos los eventos oficiales internacionales de la materia, como el Foro de Gobernanza de Internet de Latinoamérica y el Caribe (LACIGF).
9.3. 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.
9.4. 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.
9.5. Velar y fiscalizar el cumplimiento a cabalidad 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.
9.6. Fiscalizar y sancionar 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.

9.7. Dirigir de manera prudente el cambio o adecuación de normas nacionales en concordancia con los tratados, convenios y acuerdos internacionales de la materia en los que formemos parte.

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.

Carlos Tubino Aries Schreiber
Portavoz (T)
Grupo Parlamentario Fuerza Popular

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

CARLOS DOMINGUEZ HERRERA
Congresista de la República

CONGRESO DE LA REPÚBLICA

Lima, 25 de ABRIL del 2019

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición N° 4237 para su estudio y dictamen, a la (s) Comisión (es) de DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS; CIENCIA, INNOVACIÓN TECNOLOGÍA. –

GIANMARCO PAZ MENDOZA
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICIÓN DE MOTIVOS

I. DESCRIPCIÓN DEL PROBLEMA. –

En el mundo se ha creado un problema sin precedentes por que la ciberseguridad no se ha desarrollado a la par de la expansión digital, es por ello que los sistema de información digital se han vuelto altamente propensos a sufrir ataques de todo tipo de tecnologías, herramientas y programas que buscan acceder a los datos de información más sensibles que puedan aprovechar en su beneficio.

Ante el uso cada vez más generalizado de las Tecnologías de la información y comunicación-TIC en las actividades cotidianas de individuos, organizaciones privadas y públicas, aunado a su importancia como un factor de desarrollo político, social y económico; el valor económico de la información, así como el riesgo inherente del uso de dichas tecnologías, es muy *necesario contar con* estrategias nacionales de ciberseguridad que articulen *las acciones dirigidas a individuos, organizaciones privadas e instituciones públicas.*[1]

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

Es más, si bien es cierto que, tanto la administración pública como la empresa privada, vienen transformándose digitalmente y buscan implementar las nuevas tecnologías de información a sus procesos y volverlos informáticos para la modernización de la gestión; lo hacen sin tener en cuenta la necesidad de la seguridad informática, por lo que dejan expuestas sus vulnerabilidades.

Perú es el quinto país más atacado a nivel de la región[2], pero a pesar de ello y de que a nivel mundial el ciberdelito ha aumentado 10'000%; las inversiones de ciberseguridad en el Perú crecieron a penas 10% en el 2017[3] y aún las empresas privadas (quienes son llamadas a tener más interés en el tema) invierten en promedio menos del 20% de su presupuesto de tecnología, en seguridad. Es por ello que los hackers tienen en la mira al Perú[4], ya que la ciberseguridad que opera aquí es bastante anticuada o tradicional y no sería capaz de soportar ciberataques de desarrolladores modernos.

Los expertos en el tema, consideran que no solo el anticuado parque de ciberseguridad es un limitante del sector, sino también **la inexistente legislación sobre la materia**[5], aunque consideran también que el Perú es un

---

[1] Estrategia Nacional de Ciberseguridad – México 2017, pág. 5
[2] Las inversiones en ciberseguridad no son prioridad en el Perú, revisado el 19/02/2019: https://elcomercio.pe/economia/ejecutivos/inversiones-seguridad-informatica-son-prioridad-peru-noticia-541276
[3] Ídem
[4] Mercado de ciberseguridad en Perú crecerá hasta US$ 220 millones en 2021, revisado el 19/02/2019: https://gestion.pe/economia/mercado-ciberseguridad-peru-crecera-us-220-millones-2021-nndc-252046
[5] Ídem

mercado más grande y más atractivo en ciberseguridad que otros países de la región como Chile o Argentina[6], pero sin embargo solo invertimos un 0.07% del PBI nacional en ciberseguridad[7] y esto a pesar de que el año pasado se registró un incremento de 600% en los ciberataques realizados a empresas a nivel nacional[8].

En Microsoft, se desarrolla anualmente, desde el 2004, un Índice de Civismo Digital que analiza la magnitud de las conductas e interacciones negativas en línea y sus consecuencias, cuyos resultados en el 2018 arrojaron los siguientes datos alarmantes:

"Perú resultó el segundo país con el puntaje más alto en relación a la categoría de ataques intrusivos, es decir los que más padecen de contacto no deseado, engaños, estafas y fraudes en línea, etc. y solo es superado por Sudáfrica. Por otro lado, ***el país obtuvo la mayor puntuación en relación con riesgos sexuales*** *entre los 23 países encuestados. Aquí destacan los relacionados a la recepción y envío de 'sexteo' no deseado (imágenes y contenido sexual)."*[9]

CONGRESO DE LA REPÚBLICA
CARLOS DOMÍNGUEZ HERRERA

Lo que nos enseña que necesitamos no solo tecnologías más seguras, sino usuarios más educados en el tema, ya que de nada serviría tener una tecnología de seguridad de punta, si es que los usuarios no saben cómo usarla.

El día 17 de agosto del 2018, los agentes del sistema financiero tuvieron el ciberataque más mediático de los últimos tiempos, aquí en el Perú fue una noticias bastante comentada, ya que el servicios atacado –cajeros automáticos– es uno de los más usados en nuestra patria. El ataque, por la filtración del mismo y por el gran poder de las redes sociales, pudo ser repelido sin mayores consecuencias; sin embargo diariamente vemos casos de pishing, o de páginas clonadas de las entidades bancarias en los cuales normalmente los usuarios sucumben de manera fácil ante los engaños de los inescrupulosos ciberdelincuentes. Esto en materia privada, pero ni siquiera en el ámbito público se cuenta con una Estrategia Nacional de Ciberseguridad a pesar de habernos recientemente adherido al Convenio de Budapest, que es el tratado internacional rector en materia de cooperación sobre delitos informáticos.

En el 2016 el BID hizo un informe sobre la ciberseguridad en Latinoamérica, basado en el modelo de madurez desarrollado por Centro Global de Capacidad sobre Seguridad Cibernética (Oxford) que utiliza 49 indicadores. Este estudio

---

[6] Ídem
[7] El Perú invierte 0.07% de su PBI en ciberseguridad, revisado el 19/02/2019: https://peru21.pe/economia/peru-invierte-0-07-pbi-ciberseguridad-447872
[8] ídem
[9] Andrés Rengifo, director para América Latina de la Unidad de Delitos Informáticos y Asuntos de Propiedad Intelectual de Microsoft, en una entrevista con el diario Perú21, revisado el 19/02/2019: https://peru21.pe/tecnologia/ciberseguridad-seguros-peruanos-internet-entrevista-396789

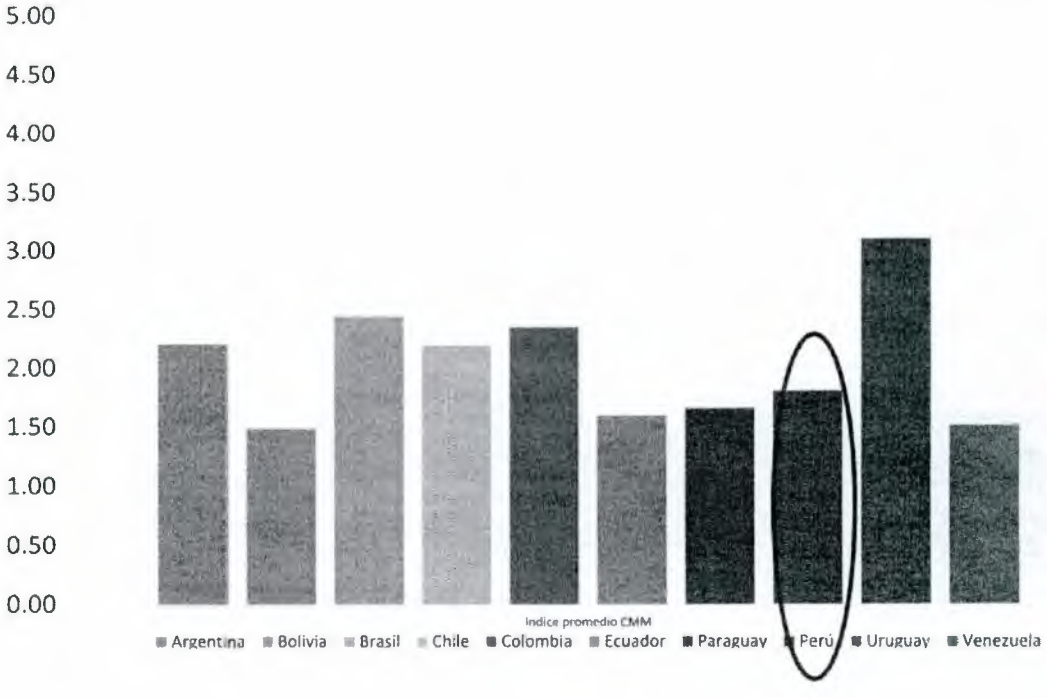
concluye que muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores.

En el mismo informe se hizo un cuadro indicador con cinco niveles de madurez en ciberseguridad:

NIVEL		DESCRIPCIÓN
1	INICIAL	No existe nada en materia de ciberseguridad o es sumamente básico
2	FORMATIVO	Características nuevas, casuales, desorganizadas, mal definidas
3	ESTABLECIDO	Elementos establecidos y funcionando, falta asignación de recursos
4	ESTRATÉGICO	Se han elegido elementos que son clave, trabajando en función a resultados esperados
5	DINÁMICO	Mecanismos claros para adaptar la estrategia a las circunstancias imperantes. Toma de decisiones rápida

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

Y cuál fue nuestra calificación:



Nuestro promedio en la región fue de 1.8, es decir nos encontramos en una ciberseguridad incipiente y casi embrionaria, no llegando siquiera a ser considerados en el nivel formativo, sin embargo, es importante mencionar también que los países de Sudamérica no tienen promedio muy superior al del Perú, encontrándose en una situación similar.

A nivel mundial, el International Telecommunications Union (ITU) en el año 2017 publicó el Índice de Ciberseguridad Global, en el cual nos sitúa en el puesto 79 de 193 países y denota la gestión y calidad de la ciberseguridad en un mínimo de 0 y un máximo de 1, teniendo el Perú una calificación de 0.374 que representa básicamente los esfuerzos privados por la ciberseguridad:

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

AMERICAS Region	Score	Global Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81

Global Cybersecurity Index (GCI) 2017

Lo que evidencia que nuestra relación, preocupación, gestión y calidad de ciberseguridad es aún un punto clave de desarrollo, pendiente de elaboración y de acción dentro de nuestra patria.

Además de que si deseamos lograr la verdadera modernización de la Gestión del Estado, se debe implementar de manera inmediata una política adecuada de ciberseguridad.

Algunos Ejemplos de los Peores Ciberataques

ENERO 2017

Las **cámaras de seguridad de Washington** son infectadas por 2 ransomware y dejan sin vigilancia a la ciudad durante **48 horas**

FEBRERO 2017

El grupo de hackers "Anonymus" **cierra 10.613 páginas de la Darknet** que representaban un **20%, de la pornografía infantil.**

MAYO 2017

El ransomware WannaCry **aprovecha vulnerabilidades de Windows** con una herramienta desarrollada por la Agencia Nacional de Seguridad (NSA) de Estados Unidos llamada "**EthernalBlue**"

SEPTIEMBRE 2017

Equifax, sufre el **hackeo de toda su base de datos**, filtrando la información de **143 millones de usuarios** en Canadá, Estados Unidos y Reino Unido.

MAYO 2018

Un virus entra a la red del Banco de Chile, **anulando sus discos de arranque** y obliga a la suspensión de más de **9 mil estaciones de trabajo** a nivel nacional, reconociendo el robo de **10 millones de dólares.**

OCTUBRE 2018

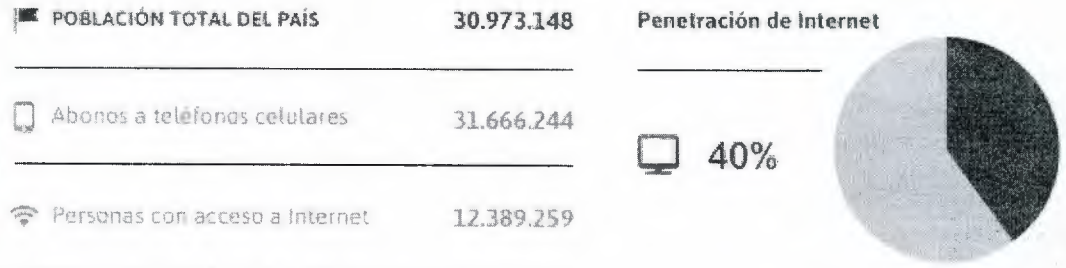
Facebook reconoció un problema de seguridad que afectaba a casi **30 millones de cuentas.**

Fuente: Ciberseguridad en Chile: Mirada Público-Privada, pág. 2

CONGRESO DE LA REPÚBLICA * CARLOS DOMINGUEZ HERRERA *

Números de Ciberdelincuencia en América Latina

"El Banco Interamericano de Desarrollo (BID) en conjunto con la Organización de los Estados Americanos (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford, publicó el documento Ciberseguridad: Estamos preparados en América Latina y el Caribe"[10], que ubica al Perú en un escaso nivel de implementación en los componentes de Política y Estrategia, y Tecnologías, además de arrojar algunos datos e información importante de conocer en el marco de lo que se quiere conocer con respecto a nuestro nivel de ciberseguridad en el país:



Informe Ciberseguridad 2016 – Banco Interamericano de Desarrollo

Con el 40% de la población con acceso a internet, nos convertimos en un eje regional de actividad y comercio digital[11] y por lo tanto en un "mercado" muy atractivo para la ciberdelincuencia. Se menciona también:

"Mientras que la conciencia de las partes interesadas ha aumentado con gestiones recientes, la ausencia de una estrategia y una cadena de mando clara continúan impidiendo el fortalecimiento de la seguridad cibernética del país (...)

(...) Entre los constantes desafíos que se enfrentan, cabe citar su limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado (...) Sobre la Gestión de crisis (...) el alcance de denuncia responsable sigue siendo bajo, ya que las tecnologías de seguridad y la Infraestructura Crítica Nacional (ICN) son gestionadas de manera informal (...)

Mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en el Perú, la conciencia social de la seguridad cibernética es generalmente baja."[12]

[10] Banco Interamericano de Desarrollo y Organización de los Estados Americanos, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (14 de marzo de 2016), pág. 108 revisado el 20/02/2019:
https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

[11] Perú será el mercado con más compras online en Sudamérica para el 2019:
https://andina.pe/agencia/noticia-peru-sera-mercado-mas-compras-online-sudamerica-para-2019-733549.aspx

[12] Banco Interamericano de Desarrollo y Organización de los Estados Americanos, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Ídem.

Creándonos un claro panorama de lo que debemos implementar en materia de ciberseguridad, según sus indicadores, estos son nuestros resultados:

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

Desarrollo de la estrategia [redacted]

FORMATIVO

[redacted]

Se ha articulado un esquema de una estrategia nacional de seguridad cibernética construido sobre la base de la consulta del gobierno; se han establecido procesos de consulta para los grupos de interés clave, posiblemente con asistencia internacional.

Organización [redacted]

FORMATIVO

[redacted]

Se ha diseñado y difundido un programa de seguridad cibernética coordinado; los presupuestos todavía pueden estar distribuidos; aún es limitada la cooperación interdepartamental.

Contenido [redacted]

INICIAL

[redacted]

Puede no existir ninguna o puede haber varias estrategias nacionales con una referencia a la seguridad cibernética; si es que existen, el contenido es genérico, no necesariamente alineado con los objetivos nacionales y no proporciona directrices recurribles.

Defensa cibernética

Estrategia [redacted]

FORMATIVO

[redacted]

Han sido identificadas amenazas específicas a la seguridad nacional en el ciberespacio, tales como actores de amenazas externas, amenazas internas, vulnerabilidades del sistema de suministro y amenazas a la capacidad operativa militar, pero aún no existe una estrategia de respuesta coherente.

Organización [redacted]

INICIAL

[redacted]

No hay gestión de la defensa cibernética; si es que existe, puede ser distribuida entre las fuerzas armadas y/o algunas otras organizaciones gubernamentales; no hay una estructura de mando clara para la seguridad cibernética en las fuerzas armadas.

Coordinación [redacted]

FORMATIVO

[redacted]

Se acuerdan los requisitos de capacidad de defensa cibernética entre el sector público y privado con el fin de minimizar la amenaza a la seguridad nacional.

Marcos legales

Marcos jurídicos de seguridad cibernética

Para la seguridad de las TIC [redacted]

ESTABLECIDO

[redacted]

Se han implementado los marcos legislativos y reglamentarios de seguridad integral de las TIC que abordan la seguridad cibernética; se ha adoptado la legislación que protege los derechos de los individuos y las organizaciones en el entorno digital.

Privacidad, protección de datos y otros derechos humanos [redacted]

ESTABLECIDO

[redacted]

Se han aplicado procedimientos reglamentarios y legislación de protección de datos integral; la legislación nacional prevé el derecho del individuo a la privacidad especificando el aviso, el propósito, el consentimiento, la seguridad, la divulgación, el acceso y la responsabilidad de la información personal.

Derecho sustantivo de delincuencia cibernética [redacted]

ESTABLECIDO

[redacted]

La legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordados en el código penal.

Derecho procesal de delincuencia cibernética [redacted]

FORMATIVO

[redacted]

Se está discutiendo y desarrollando el derecho procesal penal en relación con la prueba electrónica; el derecho procesal penal se aplica ad hoc a la delincuencia cibernética, pero no ha comenzado el desarrollo de los delitos cibernéticos específicos.

Investigación jurídica

Cumplimiento de la ley [redacted]

FORMATIVO

[redacted]

Existe alguna capacidad de investigación para indagar delitos que involucren pruebas electrónicas, así como para obtener dichas pruebas, de conformidad con el derecho interno; sin embargo, esta capacidad es mínima.

La fiscalía [redacted]

FORMATIVO

[redacted]

Un número limitado de fiscales tienen la capacidad de construir un caso basado en información electrónica, pero esta capacidad es en gran medida ad hoc, no institucionalizada, y se carece de mecanismos formales de colaboración con la policía.

Tribunales [redacted]

FORMATIVO

[redacted]

Un número limitado de jueces tiene capacidad para presidir un caso de delito cibernético, pero esta capacidad es en gran medida ad hoc y no sistemática; no existen recursos judiciales o de formación en delincuencia cibernética.

Divulgación responsable de la información

Divulgación responsable de la información [redacted]

INICIAL

[redacted]

No se reconoce la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.

Cultura y sociedad

Mentalidad de seguridad cibernética

En el gobierno

FORMATIVO

Agencias líderes han comenzado a darle prioridad a la seguridad cibernética, mediante la identificación de los riesgos y amenazas.

En el sector privado

ESTABLECIDO

Se ha arraigado una mentalidad de seguridad cibernética entre las empresas y la industria.

En la sociedad

INICIAL

La sociedad desconoce las amenazas cibernéticas y no puede tomar medidas concretas de seguridad cibernética o la sociedad es consciente de las amenazas cibernéticas, pero no toma medidas proactivas para mejorar su seguridad cibernética.

Conciencia de seguridad cibernética

Sensibilización

FORMATIVO

Se establecen campañas de sensibilización con objetivos definidos, pero son ad hoc, no cubren necesariamente todos los grupos y no están estrechamente vinculadas a la estrategia de seguridad cibernética; están disponibles seminarios y recursos en línea para la población objetivo, pero no hay esfuerzos de coordinación o de medición.

Confianza en el uso de Internet

En los servicios en línea

FORMATIVO

La confianza en los servicios en línea se identifica como una preocupación; los operadores de infraestructuras toman en consideración medidas para fomentar la confianza en los servicios en línea; sin embargo, no se han establecido medidas.

En el gobierno electrónico

FORMATIVO

La gama de servicios electrónicos del gobierno continúa en expansión, con un reconocimiento de la necesidad de aplicar medidas de seguridad para promover la confianza en los servicios electrónicos; múltiples partes interesadas analizan las prácticas indeseables en línea.

En el comercio electrónico

FORMATIVO

Los servicios de comercio electrónico son mínimos y no totalmente organizados; las partes interesadas y los usuarios reconocen la necesidad de seguridad en los servicios electrónicos y ha comenzado el análisis de inversión entre los proveedores de servicios.

Privacidad en línea

Normas de privacidad

FORMATIVO

Se consideran las leyes y políticas que promueven el acceso a datos personales recogidos y almacenados por todo el gobierno y otras instituciones públicas.

Privacidad del empleado

ESTABLECIDO

Los empleadores mantienen políticas de privacidad que ofrecen un nivel mínimo de privacidad para los empleados.

Educación

Disponibilidad nacional de la educación y formación cibernéticas

Educación

FORMATIVO

Existe mercado para la educación y la formación en seguridad de la información con evidencia de asimilación; las iniciativas de los profesionales están dirigidas a incrementar el atractivo de las carreras en seguridad cibernética y su pertinencia para roles de liderazgo más amplios.

Formación

FORMATIVO

Existe capacitación en seguridad de la información, pero es ad hoc y sin coordinación; en cuanto a formación, hay disponibles seminarios y recursos en línea para grupos demográficos específicos, pero no existen medidas de efectividad.

Desarrollo nacional de la educación de seguridad cibernética

Desarrollo nacional de la educación de seguridad cibernética

INICIAL

No existen instructores profesionales en seguridad cibernética, o son pocos; no se cuenta con un programa para capacitar a instructores en seguridad cibernética; o no existe o apenas está siendo discutida la justificación del presupuesto para la educación y la investigación.

Formación e iniciativas educativas públicas y privadas

Capacitación de empleados en seguridad cibernética

FORMATIVO

No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas existentes para la planeación de la seguridad cibernética de la organización, sin la integración automatizada de datos.

Gobernanza corporativa, conocimiento y normas

Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

FORMATIVO

Las juntas directivas tienen algún conocimiento de cuestiones de seguridad cibernética, pero no de la forma en que estas podrían afectar a la organización, o cuáles serían las amenazas directas que pudieran enfrentar.

Tecnologías

Adhesión a las normas

FORMATIVO

Se han identificado estándares de seguridad de la información para su uso y ha habido algunos signos iniciales de promoción y adopción del gobierno, sector público y organizaciones de la Infraestructura Crítica Nacional (ICN); hay una aplicación mínima de las normas nacionales e internacionales.

INICIAL

No hay evidencia de uso de las normas relacionadas con la seguridad cibernética en la orientación de los procesos de adquisición, o existe algún reconocimiento de la orientación disponible, pero no existe ningún esfuerzo para utilizarlo.

FORMATIVO

Se están discutiendo metodologías para los procesos de desarrollo de software que se centran en la integridad y la capacidad de recuperación, y el gobierno y las comunidades profesionales las están promoviendo; existe evidencia de que dentro de la ICN y del sector público hay organizaciones que suministran y buscan adoptar normas de desarrollo de código y del logro de algunas acreditaciones con la promoción gubernamental de prácticas seguras.

Organizaciones de coordinación de seguridad cibernética

INICIAL

No existe un centro de mando y control de la seguridad cibenética, o se está considerando crearlo a nivel nacional.

FORMATIVO

Existe un equipo o personal de respuesta a incidentes en el país, con roles y responsabilidades identificadas; la actividad se concentra en la detección y respuesta a incidentes cibernéticos específicos de la organización.

Respuesta a incidentes

ESTABLECIDO

Se establece un registro central de incidentes cibernéticos a nivel nacional.

FORMATIVO

Han sido identificadas y contactadas las organizaciones del sector privado que son clave para la seguridad cibernética nacional, sin que haya mecanismos de coordinación o de intercambio de información con el sector público formal; un cuerpo central ha sido designado para recopilar información sobre amenazas de emergencia, sin un mandato específico para una agencia de respuesta cibernética nacional.

FORMATIVO

Se han identificado y publicitado directores de incidentes en cada agencia y ministerio a nivel nacional; los canales de comunicación entre estos directores siguen siendo ad hoc e incoherentes.

Resiliencia de la infraestructura nacional

FORMATIVO

Se realiza el despliegue no estratégico de la tecnología y los procesos en los sectores público y privado; están disponibles en línea servicios públicos, información y contenidos digitales, pero son limitadas la implementación y el proceso.

INICIAL

El gobierno no tiene control de la infraestructura tecnológica o este control es mínimo; las redes y sistemas son tercerizados, con potencial de adopción por parte de mercados de terceros poco fiables; puede haber una dependencia de otros países en tecnología de la seguridad cibernética.

Protección de la Infraestructura Crítica Nacional (ICN)

FORMATIVO

Se ha creado una lista general de activos de la ICN, sin identificar prioridades basadas en el riesgo.

FORMATIVO

Se establece un mecanismo para la divulgación periódica de vulnerabilidades entre el sector público y privado, pero no se ha especificado el alcance de los requisitos de presentación de informes.

INICIAL

La planeación de la respuesta a un ataque a los activos críticos puede haber sido discutida ampliamente, pero no existe un plan formal.

INICIAL

Los procedimientos informales de diálogo entre el sector público y privado son inexistentes; o, pueden haber sido desarrollados, pero carecen de parámetros de intercambio de información y generalmente o son individuales o no estructurados.

INICIAL

La conciencia acerca de amenazas por parte de los operadores de la ICN es mínima, o no existe en absoluto; las habilidades y comprensión básicas de gestión de riesgos pueden ser incorporadas en las prácticas empresariales, pero la seguridad cibernética está supeditada a las TI y el riesgo de protección de datos y no se reconoce más ampliamente.

Gestión de crisis

FORMATIVO

Se ha llevado a cabo una evaluación preliminar de las necesidades de las medidas que requieren comprobación, con la consideración de un escenario de ejercicio simple, con un tamaño, ámbito geográfico, recursos y coordinación limitados; están incluidos actores clave en el proceso de planeación.

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

No se ha realizado ninguna evaluación de los protocolos y procedimientos de gestión de crisis; los resultados de los ejercicios no informan a la gestión global de crisis.

Redundancia digital

Pueden considerarse o no medidas de redundancia digital.

Los activos de respuesta de emergencia se mapean y se identifican, posiblemente incluyendo detalles sobre su ubicación y sus operadores designados.

Mercado de la ciberseguridad

Poca o ninguna tecnología se produce en el país; pueden estar restringidas las ofertas internacionales o son vendidas con un sobreprecio.

La necesidad de un mercado para los seguros de delincuencia cibernética no ha sido identificada a través de la evaluación de riesgos financieros para el sector público y privado.

Como podemos observar es evidente que tenemos carencias importantes en cada uno de los sectores vitales de la ciberseguridad, manteniendo un promedio por debajo del "formativo", es decir una ciberseguridad primigenia y demasiado básica, cosa que no puede darse en un país con el nivel de desarrollo digital que tiene el Perú, que busca el Gobierno Digital y que busca tanto la modernización de la gestión del Estado como la integración de las políticas más avanzadas en el marco de la institucionalización del Estado que se necesita para formar parte de los grandes organismos, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), es por eso que debemos entender que nos encontramos en una posición no favorable y muy por debajo de los estándares mínimos que deberíamos tener ya en el marco de la ciberseguridad.

En Latinoamérica, la Agenda Digital para América Latina y el Caribe (eLAC) cuenta con cinco pilares de implementación[13]. En el pilar de *"gobernanza para la Sociedad de la Información"* destaca el objetivo 19:

"Promoción de la seguridad, privacidad, protección de datos y confianza en el uso de Internet"

Y el "Objetivo 20:

"Prevención y combate del ciberdelito mediante estrategias y políticas de ciberseguridad. Coordinarse a nivel local y regional entre equipos de respuesta ante acontecimientos".

En el marco de la Alianza del Pacífico, en diciembre de 2016 se aprobó la Agenda Digital con el precepto de: "Potenciar la cooperación en materia de seguridad digital y fomento

[13] Comisión Económica para América Latina y el Caribe, Agenda Digital para América Latina y el Caribe (eLAC2018), (7 de agosto de 2015), revisado el 20/02/2019: http://repositorio.cepal.org/handle/11362/38886

de la confianza en el uso de las TIC"[14]. Dicha agenda posee una hoja de ruta con cuatro ejes:

1. Economía digital
2. Conectividad digital
3. Gobierno digital y
4. Ecosistema digital,

Que buscan mejorar la competitividad de los países que la conforman por medio de las TIC y la promoción de la economía digital.

> *"En cuanto al Foro Económico Mundial (WEF, por sus siglas en inglés), este define a la resiliencia y seguridad cibernética como condiciones clave para el desarrollo tecnológico y económico. En 2016, el Consejo de la Agenda Global en Ciberseguridad publicó su libro blanco orientado a señalar los obstáculos existentes en el sector público y privado, que dificultan la colaboración y la adopción de mejores prácticas en materia de ciberseguridad[15]. Además, identificó en su Informe de Riesgos Globales 2017 al robo masivo de datos y ciberataques en el escenario de riesgo para dicho año, señalando también el reto que representan las tecnologías emergentes en lo relativo a su gobernanza."[16]*
>
> *"La Reunión Regional Preparatoria de América Latina y el Caribe para el Foro para la Gobernanza de Internet (LACIGF) es el espacio para que los diferentes actores toquen cuestiones de políticas relacionadas con Internet desde un enfoque regional y se celebra anualmente desde 2008"*[17].

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

También es importante conocer del Informe de 2014 Tendencias de Seguridad Cibernética en América Latina y el Caribe, patrocinado por la Organización de Estados Americanos (OEA) da luces de la situación del Perú y arroja resultados bastante similares a los ya mostrados en este proyecto de ley

TLD (dominio de nivel superior)	Ubicación del TLD	Nro. de ataques tipo *phishing* únicos —2da. mitad de 2013	Nombres de dominio únicos usados para *phishing* —2da. mitad de 2013	Dominios registrados, noviembre de 2013	Puntuación: dominios de *phishing* cada 10.000 dominios —2da. mitad de 2013	Puntuación: ataques cada 10.000 dominios —2da. mitad de 2013	Tiempo de actividad promedio en hh:mm —2da. mitad de 2013	Tiempo de actividad medio en hh:mm —2da. mitad de 2013	Nro. total de dominios maliciosos registrados —2da. mitad de 2013	Puntuación de los registros maliciosos/ 10.000 dominios registrados
pe	Peru	112	100	75.116	13.3	14.9	44:52	8:17		

[14] Alianza del Pacífico, Declaración de Cali, (30 de junio de 2017), Anexo I, párrafo 8, disponible en: https://alianzapacifico.net/?wpdmdl=9850
[15] World Economic Forum, Global Agenda Council on Cybersecurity, White Paper, abril 2016, disponible en: http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf
[16] World Economic Forum, The Global Risks Report 2017, enero 2017, disponible en: http://www3.weforum.org/docs/GRR17_Report_web.pdf
[17] Reunión Preparatoria para el Foro de Gobernanza de Internet (LACIGF), disponible en: https://lacigf.org/

Como vemos, dentro de la región existen ya múltiples esfuerzos para desarrollar la gestión en ciberseguridad, pero nosotros no pertenecemos a ninguno de estos grupos, ni hemos suscrito los suficientes convenios sobre la materia, lo que deja en claro nuestra carencia en el tema.

II. PROPUESTA DE SOLUCIÓN

Establecer un marco legal de ciberseguridad y promoverlo en todos los niveles, creando además un Consejo Nacional de Ciberseguridad, dar viabilidad al presente proyecto de ley constituye la solución a priori de este problema.

¿Qué se logrará principalmente?

- *Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con 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.*

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

- *Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos.*

- *Es necesario mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacional e internacional, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio.*

- *Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente.*

- *Hasta que se adopte una política específica en cuanto a las infraestructuras críticas de la información (ICI), la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa.*

- *Una vez determinadas las ICI's, su protección debe ser política principal en materia de ciberseguridad.*[18]

[18] Política Nacional De Ciberseguridad, Gobierno de Chile, pág. 12

Es necesario mencionar que el presente proyecto de ley se ha elaborado teniendo como base las experiencias de Estados hermanos en sus propias políticas del ciberseguridad, como México[19] y Chile[20], tomando los principios generales y algunas fórmulas legales para estar alineados en la legislación de la materia.

III. ACTORES INVOLUCRADOS

ACTOR	DEFINICIÓN
ESTADO PERUANO	- Principal involucrado, quien debe establecer el marco normativo suficiente y empezar a promover la Ciberseguridad
ADMINISTRADOS	- Participantes intrínsecos y como sujetos pasivos en esta relación
DEMÁS ESTADOS	- Con quienes el Perú se debería relacionar para la cooperación internacional

CONGRESO DE LA REPÚBLICA
CARLOS DOMINGUEZ HERRERA

IV. MARCO JURÍDICO

1. Ley 27309, Ley que Incorpora los Delitos Informáticos al Código Penal.
2. Ley 29733 de Protección de Datos Personales.
3. Ley 30096 de Delitos Informáticos.
4. Convenio Sobre la Ciberdelincuencia de Budapest

V. EFECTOS DE LA NORMA EN LA LEGISLACIÓN NACIONAL.

Con la entrada en vigencia de la presente Ley, se promueve la creación del Consejo Nacional de Ciberseguridad y se dará un impulso y promoción de grandes proporciones a la Seguridad Informática en el Perú.

VI. ANÁLISIS COSTO BENEFICIO

La presente iniciativa legislativa ordena nuestro ordenamiento administrativo, haciéndolo más idóneo, necesario y ponderado respecto a la ciberseguridad o seguridad informática, además de ordenar la situación que puedan presentarse dentro de las acciones y/o contingencias que tengan que ver con la materia y de esa manera coberturar en su mayoría las situaciones a presentarse.

---

[19] Estrategia Nacional de Ciberseguridad – México 2017, revisado el 09 de abril del 2019: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[20] Política Nacional De Ciberseguridad, Gobierno de Chile, revisado el 09 de abril del 2019: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

BENEFICIOS / ACTOR	POSITIVO	NEGATIVO
ESTADO PERUANO	Contará con una Estrategia Nacional de Ciberseguridad y un Plan Multianual de Ciberseguridad que abrirá nuestra visión de un gobierno digital moderno y seguro.	Ninguno
ADMINISTRADOS	Verán resguardados sus derechos fundamentales y estar seguros durante su estadía en internet, generando confianza en los usuarios cibernéticos.	Ninguno
DEMÁS ESTADOS	Podrán contar con la cooperación internacional para la colaboración en la implementación de la ciberseguridad y la lucha contra el ciberdelito.	Ninguno

VII. LA INICIATIVA LEGISLATIVA Y 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; (b) garantizará la plena operatividad de las Fuerzas Armadas orientadas a la disuasión, defensa y prevención de conflictos, así como al mantenimiento de la paz; (c) impulsará la enseñanza de los conceptos básicos de la seguridad nacional en todos los niveles del sistema educativo nacional; (d) fomentará la participación activa en la protección de la Antártida, el medio ambiente, el desarrollo de la Amazonía y la integración 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.