ESTRATEGIA DE TRANSFORMACIÓN DIGITAL

DIGITAL TRANSFORMATION STRATEGY

CHILE DIGITAL 2035

CIBERSEGURIDAD/CYBERSECURITY

Senadora/Senator
XIMENA ORDENES N.

Senador/Senator
KENNETH PUGH O.

PRÓLOGO

La Senadora Ximena Ordenes y el Senador Kenneth Pugh, miembros de la Comisión "Desafíos del Futuro, Ciencia, Tecnología e Innovación", tienen el agrado de presentar la Estrategia de Ciberseguridad que forma parte de "CHILE DIGITAL 2035" presentada el pasado 19 de mayo, con el apoyo de la CEPAL, la academia y la sociedad civil organizada.

La estrategia señala los principales aspectos a considerar para su desarrollo en los próximos 12 años, comprometiendo los esfuerzos de tres gobiernos consecutivos a nivel nacional, regional y comunal. Se espera que sea una herramienta de planificación que oriente las estrategias de desarrollo y la asignación de los recursos humanos, materiales y financieros necesarios, donde la asociación público-privada es vital para el progreso, basándose en que el denominador común en ciberseguridad es la "Colaboración y Cooperación con Compromiso".

La ciberseguridad es algo mucho más amplio que una adecuada gestión de riesgos. Es una nueva cultura que requiere el conocimiento de la ciber-higiene desde una edad temprana, la detección de ciber-talento, interoperabilidad, nuevas y mejores identidades digitales entregadas por el Estado, la protección de los datos personales, y temas industriales como la protección de las infraestructuras críticas de información. Incluso hacer frente a las campañas de desinformación en línea que ponen en riesgo el Estado de Derecho, la Democracia y los Derechos Humanos. Cualquier cosa que salga mal en el mundo digital puede producir daños físicos, como muertes, perjuicios económicos, daños a la reputación e incluso daños políticos.

A largo plazo, los principales objetivos de esta estrategia se basan en el Modelo de Madurez de Ciberseguridad para las Naciones (CMM) del Centro de Ciberseguridad Global de la Universidad de Oxford, que establece cinco dimensiones diferentes.

La OEA ha utilizado este modelo como herramienta de medición para las naciones de América Latina y el Caribe, con el apoyo del BID, en 2016 y 2020. Presenta una excelente línea de base y evolución que permite medir el impacto de las políticas públicas, una de las aspiraciones de este esfuerzo, el primero con un sólido compromiso político a largo plazo.

FOREWORD

Senators Ximena Ordenes and Kenneth Pugh, members of the Committee "Challenges of the Future, Science, Technology, and Innovation" of the Chilean Senate are pleased to present the Cybersecurity Strategy part of "CHILE DIGITAL 2035" issued last May 19, with the support of ECLAC, academia and organized civil society.

The strategy outlines the main aspects to be considered for development in the next 12 years, committing the efforts of three consecutive governments at the national, regional, and communal levels. It is expected to be a planning tool guiding development strategies and allocation of the necessary human, material, and financial resources, where the public-private partnership is vital for progress, based on the common denominator in cybersecurity is "Collaboration and Cooperation with Commitment."

Cybersecurity is something much broader than adequate risk management. It is a new culture that requires knowledge of cyber hygiene from an early age, detection of cyber talent, interoperability, new and better digital identities delivered by the state, protection of personal data, and industrial issues such as the protection of critical information infrastructure. Even tackling online disinformation campaigns that put the rule of law, democracy, and human rights at risk. Anything that goes wrong in the digital world can produce physical damage, including death, economic injury, reputational damage, and even political damage.

In the long term, the main objectives of this strategy are based on the Cybersecurity Maturity Model for Nations (CMM) of Oxford University's Centre for Global Cybersecurity, which sets out five different dimensions.

The OAS has used this model as a measurement tool for Latin American and Caribbean nations, supported by the IDB, in 2016 and 2020. It presents an excellent baseline and evolution that allows measuring the impact of public policies, one of the aspirations of this effort, the first with a solid long-term political commitment.

ÍNDICE / INDEX

No se puede avanzar en transformación digital sin una adecuada estrategia de ciberseguridad. Chile debe, conforme con su propia realidad, establecer políticas y medios que permitan la protección de sus activos informáticos y de comunicaciones, así como su resiliencia frente a eventuales vulnerabilidades o fallas.

La ciberseguridad es un concepto amplio que abarca desde la protección de los datos personales hasta la protección de la infraestructura crítica de la información. Asimismo, comprende a todas las actividades asociadas a la protección de sistemas, redes, programas, dispositivos y datos de accesos no autorizados o para uso criminal y, a la vez, la práctica de asegurar la confidencialidad, integridad y disponibilidad de la información[1]. Durante la última década existe una creciente preocupación sobre la importancia de la ciberseguridad y su impacto en la humanidad.

Considerando la amplitud del concepto de ciberseguridad, se requiere de un enfoque holístico, que establezca múltiples barreras de protección entre diversos sistemas, redes, programas y datos (Fundación País Digital, 2021).[2] Es necesario, crear una cultura efectiva de higiene, prevención y defensa ante posibles riesgos digitales.

Para evaluar la situación actual de Chile en materia de ciberseguridad, se pueden tomar en cuenta diversos índices internacionales. De acuerdo con el Índice de Ciberseguridad desarrollado por la Unión Internacional de Telecomunicaciones (ITU, 2020). Chile cuenta con un nivel de ciberseguridad sensiblemente por detrás de los países OCDE y de las economías más avanzadas. Chile se encuentra en el puesto 74 a nivel mundial, situándose incluso por detrás de varios países latinoamericanos como Brasil, México, Uruguay y República Dominicana. Ello sugiere que existe un espacio de mejora. Según, la UIT las fortalezas de Chile en ciberseguridad son la robustez de su marco legal y sus mecanismos de cooperación, mientras que sus principales debilidades son los aspectos técnicos y su capacidad de implementación.

Otro marco de medición es el modelo de madurez en ciberseguridad de las naciones de la Universidad de Oxford **(CMM)**[3], en sus dimensiones de estrategia, cultura, formación, marcos legales y estándares, con rango que va de 0 a 5, representando 5 él óptimo. El modelo en si es dinámico y se va ajustando para reflejar el logro y avances entre mediciones. Actualmente Chile se encuentra en promedio entre un estado 2 y 3, según la última medición del año 2020 realizado por la OEA con apoyo del BID.

Cabe recordar que Chile lanzó en abril del 2017 su primera **Política Nacional de Ciberseguridad (PNCS)** para el periodo 2017-2022, con 5 objetivos y 43 medidas, lo que ha constituido un avance importante para enfrentar este desafío. También inicio, la tramitación de una nueva Ley de Delitos Informáticos y también se encuentra en trámite legislativo en el Senado la nueva Ley de Protección de Datos Personales que crea la nueva "Agencia Nacional de Protección de Datos". Y recientemente se ingresó para tramitación un marco de gobernanza en ciberseguridad, que crea nuevos organismos y define sus alcances. No obstante, todavía quedan pendientes una ley marco de protección de infraestructura crítica de la información y una ley de gobernanza de interoperabilidad. En materia de sensibilización y cultura sobre ciberseguridad, la Ley 21.113 de 2018, declara octubre como el **Mes Nacional de la Ciberseguridad**, y promueve ejercicios nacionales de ciberseguridad.[4]

Por otra parte, Chile se ha adherido al **Convenio de Budapest** para el combatir la ciberdelincuencia. Estos esfuerzos han buscado alinear la normativa vigente con los estándares internacionales y las mejores prácticas, como, por ejemplo, la relación de la ciberseguridad con el tratamiento de datos personales, los estándares de seguridad a cumplir en industrias reguladas y por el Estado, la tipificación de nuevos delitos informáticos, la definición de una política internacional sobre el ciberespacio y la ciberseguridad, entre otros.

Es fundamental que exista un acuerdo político nacional con visión de largo plazo para comprometer los esfuerzos de los gobiernos en evolucionar desde una estrategia de ciberseguridad hacia una política nacional del ciberespacio, con una relevante componente de ciberseguridad.

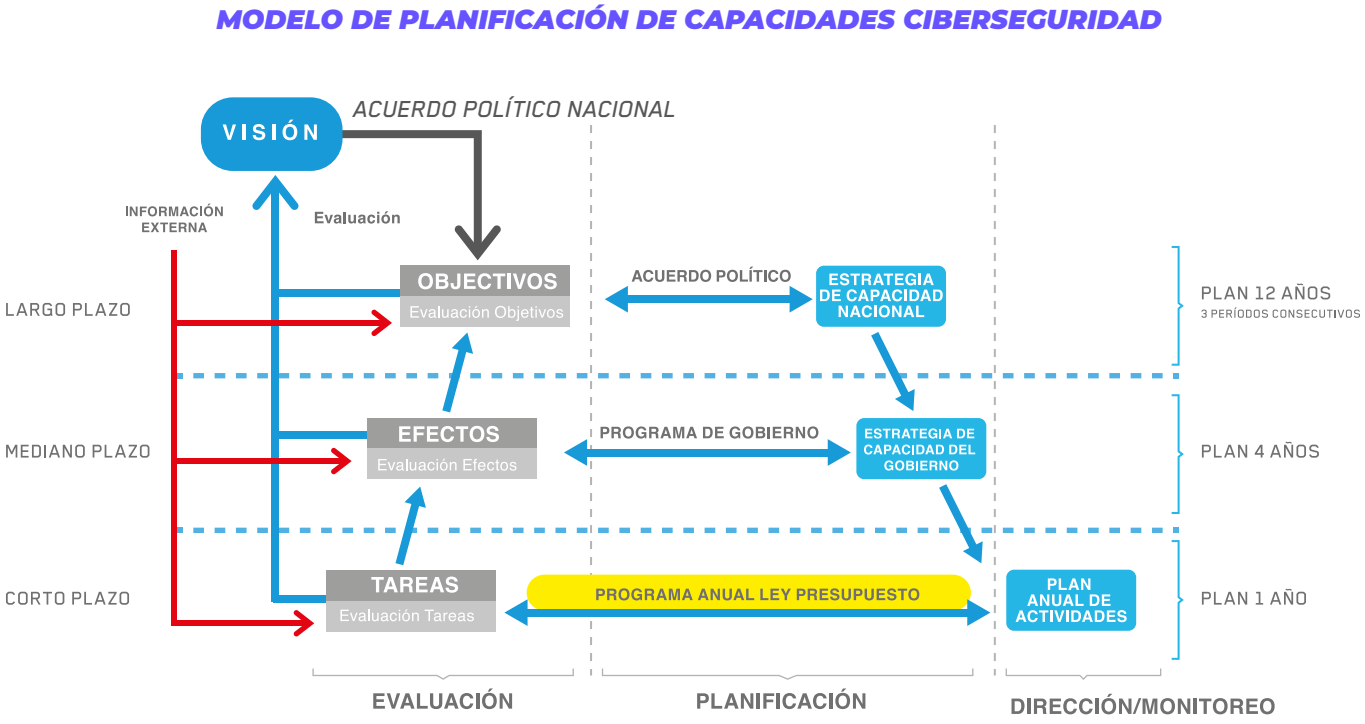
El marco jurídico de ciberseguridad se compone por una Ley de delitos informáticos y la Ley de gobernanza de interoperabilidad, además de los marcos normativos en materia de "La Protección de Datos Personales" y la "Protección de la Infraestructura Crítica de la Información" (el ámbito de alcance de la Ciberseguridad). Esto reside en una gobernanza de ciberseguridad a través de una Agencia Nacional que permita coordinar los diferentes equipos de respuesta ante incidentes de seguridad en tecnologías de la información sectoriales (Computer Security Incident Response Team, CSIRT) y tenga toda la información necesaria para determinar la "atribución" de un ciberataque al país, y a la vez apoyar la recuperación de la operatividad, resiliencia y mitigación de los efectos adversos de los ataques, generando elementos de prueba para su persecución.. Este marco jurídico permite dar forma a las distintas organizaciones necesarias para poder gestionar el "Sistema Nacional de Ciberseguridad" (véase la figura 1).

Figura 1 Marco jurídico de Ciberseguridad

Fuente: Equipo Legislativo Senador Kenneth Pugh

Para construir una estrategia nacional de ciberseguridad al 2035 se propone un modelo de planificación de capacidades de ciberseguridad de tres horizontes, considerando el largo plazo (12 años), el mediano plazo (4 años) y el corto plazo (un año). Esto permitirá generar el diseño de un sistema de planificación de capacidades por niveles. Se propone controlar el avance de la estrategia en el largo plazo, mediante el monitoreo de las tareas que se disponen cada año en la Ley de Presupuesto.

Figura 2 Modelo de Planificación de Capacidades Ciberseguridad



Fuente: Equipo Legislativo Senador Kenneth Pugh

OBJETIVO 1: ESTABLECER UN ECOSISTEMA DE CIBERSEGURIDAD NACIONAL DINÁMICO, ROBUSTO Y RESILIENTE

Se requiere instalar una visión articulada ecosistémica y dinámica para enfrentar los retos de ciberseguridad, como un área emergente y prioritaria de política pública en una sociedad que se vuelve cada vez más digital dependiendo de Internet y de la seguridad de su información y de la infraestructura que la almacena, procesa y transporta. Es esencial la integración pública privada al más alto nivel y la generación de "confianza digital" con nuevos sistemas de identidad y domicilio digital e interoperabilidad, junto con redes robustas y redundantes de traspaso de información digital, y con los sistemas de respaldo necesarios para ser altamente resilientes.

Es fundamental establecer una nueva gobernanza de Ciberseguridad, donde queden claramente definidas y determina las responsabilidades y los mandatos de los actores clave, tanto gubernamentales y no gubernamentales, los sistemas de reporte y respuesta y la adecuada asignación de recursos a los problemas y prioridades de ciberseguridad actuales y emergentes.

LÍNEAS DE INTERVENCIÓN:

- Implementar un sistema de interoperabilidad con encriptación que permita trazabilidad de la información y la integridad de ella, el traspaso transfronterizo seguro de datos. Se recomienda una plataforma abierta, gratuita y federada como X-Road ya instalada por gobierno de Colombia y distribuida por el Instituto Nórdico de Soluciones de Interoperabilidad.

- Incorporar un nuevo sistema de Identidad Digital con segundo factor de autenticación y biometría incorporado.

- Crear de un sistema nacional de acreditación de seguridad para acceso a distintos niveles de información, especialmente la sensible y clasificada.

- Desarrollar los CSIRTs (Equipos de Respuesta a Incidentes de Seguridad) de carácter sectorial (Gobierno, Defensa, y de cada sector industrial crítico).

- Crear la Agencia Nacional de Ciberseguridad y de Protección de Infraestructura Crítica de la Información.

- Crear el Centro de Operaciones de Ciberseguridad Nacional (COC) para conducción de crisis de impacto nacional y determinación de atribución de ataques junto al Consejo Nacional de Ciberseguridad.

- Crear de la Agencia Nacional de Protección de Datos Personales.

  Establecer el Foro Nacional de Ciberseguridad.

- Definir de la Estrategia Nacional contra campañas de Desinformación en Línea.

- Robustecer las redes de fibra óptica, con enlaces redundantes y respaldos con microondas y satelital. Contratación de servicios de almacenamiento seguro de datos en el territorio nacional o con protección similar.

OBJETIVO 2: ***CULTURA INTEGRAL DE CIBERSEGURIDAD NACIONAL***

Enfocado a la generación y disponibilidad de programas que sensibilizan sobre la ciberseguridad en todo el país, concentrándose en los riesgos y amenazas de ciberseguridad y las formas para enfrentarlos. Se incluye el desarrollo de una institucionalidad apropiada para difundir la ciberseguridad. Asimismo, se destaca la importancia de reportar incidentes, integrando la ciberseguridad en los procesos de manera que generen confianza hacia las operaciones en línea de los ciudadanos.

LÍNEAS DE INTERVENCIÓN:

- Desarrollar programas de ciberhigiene en la sociedad para menores de edad a partir de los 2 y hasta los 12 años.
- Desarrollar programas de formación en habilidades digitales orientadas a la ciberseguridad durante toda la formación escolar.
- Crear programas que mitiguen la violencia en redes desde edad temprana y hagan frente a situaciones de ciberacoso en menores.
- Desarrollar programas de acompañamiento digital a Adultos Mayores para mitigar riesgos a los que son expuestos en el Ciberespacio.
- Ejecutar los ejercicios nacionales de ciberseguridad los meses de octubre de acuerdo a la Ley 21.113 y desarrollar un contundente programa de difusión y actualización de conocimientos ese mes.
- Desarrollar en el mes de noviembre actividades tendientes a mejorar la capacidad de respuesta de la infraestructura crítica nacional ante incidentes o ataques digitales y promover y actualizar conocimiento de nuevas amenazas
- Crear la cultura nacional que permita identificar y reportar incidentes de ciberseguridad a la autoridad nacional competente.
- Reforzar la confianza en el uso de la red y servicios en línea tanto públicos como privados.
- Generar mecanismos para asegurar la seguridad de la información personal.
- Establecer programas alternativos al Servicio Militar para la formación de especialistas en ciberdefensa.

OBJETIVO 3: ***GESTIÓN DEL TALENTO, DESARROLLO DE CAPACIDADES Y DE INDUSTRIA DE CIBERSEGURIDAD***

Aborda la disponibilidad y ejecución de programas de formación y educación en ciberseguridad, de alta calidad, con programas de capacitación y certificación de competencias, además de mejorar la colaboración entre el gobierno y la industria para asegurar que las inversiones educativas satisfagan las necesidades de educación en ciberseguridad en todos los sectores, en base a una entidad rectora con competencia en estas materias. La I&D+i son temas relevantes que se deben incentivar para generar una industria autosuficiente que apoye la gestión de ciberseguridad del país.

LÍNEAS DE INTERVENCIÓN:

- Crear el Instituto Nacional de Ciberseguridad (INCIBER) en Valparaíso para articular la red de investigación avanzada en ciberseguridad, desarrollo de talento ciber y formación avanzada de instructores y especialistas de distintas áreas, junto al establecimiento de medios de evaluación y acreditación de competencias, organización de ejercicios nacionales y actividades de promoción y de difusión de nuevos conocimientos en ciberseguridad.

- Ejecutar programas para identificar y desarrollar cibertalento a partir de los 14 años.

- Desarrollar habilidades digitales entregando competencias certificadas para alumnos de todas las edades a partir de los 18 años y sin ser requisito de ingreso una formación académica previa, usando la metodología francesa de la Escuela 42.

- Mejorar las ofertas educativas de ciberseguridad, estableciendo programas de formación y acreditación de competencias, de acuerdos a estándares nacionales e internacionales, para carreras técnicas y universitarias.

- Fomentar el desarrollo de becas de postgrado en Ciberseguridad, en universidades de alto prestigio mundial, para doctorados y post doc.

- Fomentar de la incorporación de mujeres a carreras de ciberseguridad para hacerse cargo de la brecha de género existente.

- Premiar anualmente a las mujeres destacadas en Ciberseguridad

- Reconocer anualmente a los líderes emergentes destacados de la Ciberseguridad

- Incentivar la formación y retención de especialistas en ciberseguridad para apoyar al Estado, los servicios de este, y a los actores económicos en general.

- Explorar la coordinación, y los recursos para desarrollar marcos educativos de ciberseguridad mejorados, con presupuesto y gasto basado en la demanda nacional de forma dinámica y con recursos de la ley de presupuesto.

- Incentivar la I&D+i en ciberseguridad fomentando el desarrollo de una nueva industria nacional significativa y eficiente que se proyecte en los mercados internacionales, con foco en el desarrollo regional y con presupuesto indexado a un % del PIB y aporte de privados.

- Colaborar en ciberseguridad entre el ámbito civil y las entidades de la defensa, mediante proyectos de tecnologías duales (uso civil y militar) junto con la existencia de recursos anuales adecuados disponibles para su ejecución.

OBJETIVO 4: MARCOS LEGALES Y REGULATORIOS EFECTIVOS Y DINÁMICOS, PROTECCIÓN DE DERECHOS EN EL CIBERESPACIO, Y PERSECUCIÓN DEL CIBERCRIMEN

Abordar las diversas leyes y regulaciones, junto a las disposiciones relativas a la ciberseguridad, incluidas las disposiciones legales y requisitos reglamentarios y procedurales, incluida la legislación sobre delitos informáticos ("Ciberdelitos" y "Cibercrimen") y evaluación del impacto en los derechos humanos. También considera los marcos legislativos relacionados con ciberseguridad, incluida la protección de datos, la protección infantil, la protección al consumidor y propiedad intelectual, así como las responsabilidades asociadas a quienes manejan, recopilan y almacenan ese tipo de información.

LÍNEAS DE INTERVENCIÓN:

- Actualizar permanentemente la Ley de Delitos Informáticos en base a evolución de la tecnología y los protocoles adicionales del Convenio de Budapest.
- Promulgar la nueva Ley de Protección de Datos Personales y su armonización permanente con el Reglamento Europeo de Protección de Datos (GDPR)
- Promulgar la Ley de Gobernanza de Ciberseguridad y Protección de la Infraestructura Crítica de la Información, junto con los nuevos delitos que dañan esta II.CC. como lo es el corte de cables de fibra óptica, y daños a la infraestructura pública digital
- Definir un mecanismo de registro de SIM Cards para conocer la identidad de sus dueños.
- Formar nuevas brigadas de Cibercrimen de la PDI en cada región de Chile, especializadas en investigaciones complejas y formación básica del establecimiento de sitios de suceso tecnológico y cadena de custodia digitales a todas las policías.
- Crear el Laboratorio de Investigación Avanzada de Cibercrimen en dependencias edificio Curauma de la PDI en Valparaíso
- Formar Fiscales en dirección de investigación y persecución de ciberdelito y Cibercrimen y formar jueces en materias de competencia de estos delitos digitales.
- Desarrollar en el Ministerio Publico, Fiscalías especializadas en Cibercrimen.
- Generar políticas, procesos y legislación para divulgación responsable de fallas de seguridad. Establecer una política o marco de divulgación responsable en organizaciones del sector público y privado y el derecho a la protección legal para aquellos que detectan e informan vulnerabilidades de sistemas, dentro de plazos acotados o con la anuencia de los responsables de las organizaciones.
- Establecer mecanismos de intercambio de información sobre ciberdelincuencia entre los sectores público y privado nacionales, incluida la cooperación con los prestadores de servicios de Internet y otros proveedores de tecnología.

- Identificar y auditar los activos de información, sectores y operadores críticos de forma regular, estableciendo exigencias de ciberseguridad a través de políticas y estándares de calidad de suministros y servicios, actualización, mantenimiento y protección de sistemas y equipos informáticos.

- Adoptar el manual de Tallin 2.0 sobre el Derecho Internacional aplicable a las Ciberoperaciones Militares.

OBJETIVO 5: COOPERACIÓN INTERNACIONAL Y LIDERAZGO REGIONAL EN CIBERSEGURIDAD

Asegurar la existencia y funcionamiento de mecanismos formales e informales que permiten la cooperación entre actores nacionales y transfronterizos para promover la ciberseguridad internacional mediante acuerdos que apunten a disuadir y combatir la ciberdelincuencia, y sus consecuencias. La colaboración internacional debe perseguir una colaboración eficaz en el compartir informaciones de ciberseguridad, manejo de incidentes, protocolos de manejo de información, y ser un nexo para el desarrollo de legislaciones comparables. Asimismo, hacer de nuestro país un referente regional para la ciberseguridad amparando convenios de colaboración internacional entre el estado, la academia y los principales referentes mundiales de la ciberseguridad.

LÍNEAS DE INTERVENCIÓN:

- Crear un Centro de Capacidades de Ciberseguridad para Iberoamérica, como un organismo no gubernamental basado en Universidades Nacionales, asociado a la red de centros de investigación apoyados por el Centro Global de Capacidades de Ciberseguridad de la Universidad de Oxford.

- Crear un ejercicio internacional regional a ser ejecutado en Chile por el INCIBER para que los equipos oficiales de los distintos CSIRT de la región se conozcan personalmente.

- Establecer nexos formales de intercambio y colaboración por parte de la institucionalidad nacional, tanto en el ambiente público como privado, y de la academia, con las principales instancias internacionales y referentes en materias de ciberseguridad, tanto de gobiernos amigos como de organismos internacionales.

- Participar en las principales entidades rectoras de Internet, y de aquellas instancias internacionales en que el Estado de Chile ha sido invitado, idealmente mediante un Embajador en misión especial para el Ciberespacio.

- Promulgar la Política Internacional de Chile para el Ciberespacio, donde se señale nuestra postura respecto de la seguridad y neutralidad de la red.

- Establecer mecanismos de intercambio de información y evidencia sobre ciberdelincuencia entre distintos países firmantes del acuerdo del Convenio de Budapest.

- Participar con una delegación nacional en el ejercicio Cyberex en España realizado por Incibe los meses de septiembre de cada año y aquellos en que se invite a una delegación nacional, como los organizados en Grecia por ENISA y EE. UU.

- Participar anualmente en el ejercicio militar Locked Shields en Tallin Estonia, en el Centro de Excelencia de (CCDCOE)

METAS

- Creación del **Instituto Nacional de Ciberseguridad** y del **Centro de Capacidades de Ciberseguridad de Iberoamérica** al 2023
- Creación de las **nuevas agencias nacionales de Protección de Datos Personales y de Ciberseguridad y Protección de Infraestructura Críticas de la Información** al 2025
- Creación de la totalidad de los **CSIRT sectoriales** y **COC Nacional** al 2030
- **Inversión del gasto en I+D+i de Ciberseguridad** como porcentaje del PIB enun 0,1% al 2025 y en 0,2% al 2030
- Formación de **10.000 profesionales certificados en Ciberseguridad** al 2035, donde al menos el 30% de ellos sean mujeres.
- **Alcanzar el 2035 una "Madurez en Ciberseguridad"** cercana al Estado 5 o "Dinámico" para una nación, de acuerdo con el CMM de la Universidad de Oxford, en todos los Factores con al menos evaluación Estado 4 y medido de forma externa.

1- Reporte Fundación País Digital, 2021

2- Cybersecurity Capacity Maturity Model for Nations (CMM) is a methodical framework designed to review a country's cybersecurity capacity. **(https://gcscc.ox.ac.uk/the-cmm)**

3- Esto sigue el ejemplo de Estados Unidos que en octubre tiene el "Cybersecurity Awareness Month" al igual que la Unión Europea que tiene el "European Cybersecurity Month"

The progress in digital transformation cannot be made without an adequate cybersecurity strategy. In line with its reality, Chile must establish policies and means to protect its IT and communications assets and its resilience in possible vulnerabilities or failures.

Cybersecurity is a broad concept ranging from protecting personal data to safeguarding critical information infrastructure. It also encompasses all activities associated with the protection of systems, networks, software, devices, and data from unauthorized access or illicit use and, at the same time, the practice of ensuring the confidentiality, integrity, and availability of information[1]. Over the last decade, has been a growing concern about the importance of Cybersecurity and its impact on humanity.

Considering the amplitude of the concept of Cybersecurity, a holistic approach is required, which establishes multiple protection barriers between various systems, networks, programs, and data (Fundación País Digital, 2021)[2]. Creating an influential culture of hygiene, prevention, and defense against possible digital risks is necessary.

In assessing Chile's current cybersecurity situation, various international indicators are considered. According to the Cybersecurity Index developed by the International Telecommunications Union (ITU, 2020). Chile's level of Cybersecurity lags significantly behind that of the OECD countries and the most advanced economies. Chile ranks 74th globally, behind several Latin American countries such as Brazil, Mexico, Uruguay, and the Dominican Republic. The last suggests that there is room for improvement. According to the ITU, Chile's strengths in Cybersecurity are the robustness of its legal framework and its cooperation mechanisms, while its main weaknesses are technical aspects and its implementation capacity.

Another measurement framework is the Oxford University Cybersecurity Maturity Model of Nations **(CMM)**[3]. Its dimensions of strategy, culture, training, legal frameworks, and standards range from 0 to 5, with 5 representing the optimum. The model itself is dynamic and is adjusted to reflect achievement and progress between measurements. Currently, Chile has an average of status 2 and 3, according to the 2020 latest measure conducted by the OAS with support from the IDB.

We must recall that in April 2017, Chile launched its first **National Cybersecurity Policy (PNCS)** for the years 2017-2022, with five objectives and 43 measures, which has been a significant step forward in facing this challenge. It also initiated the processing of a new Law on Computer Crimes and a new personal data protection law creating the new National Data Protection Agency in the Senate. And a cybersecurity governance framework, which creates new bodies and defines their scope, was recently submitted for processing. However, a framework law on critical information infrastructure protection and a law on interoperability governance are still pending. In terms of cybersecurity awareness and culture, Law #21.113 of 2018 declares October as the National **Cybersecurity Month** and promotes national cybersecurity exercises[4].

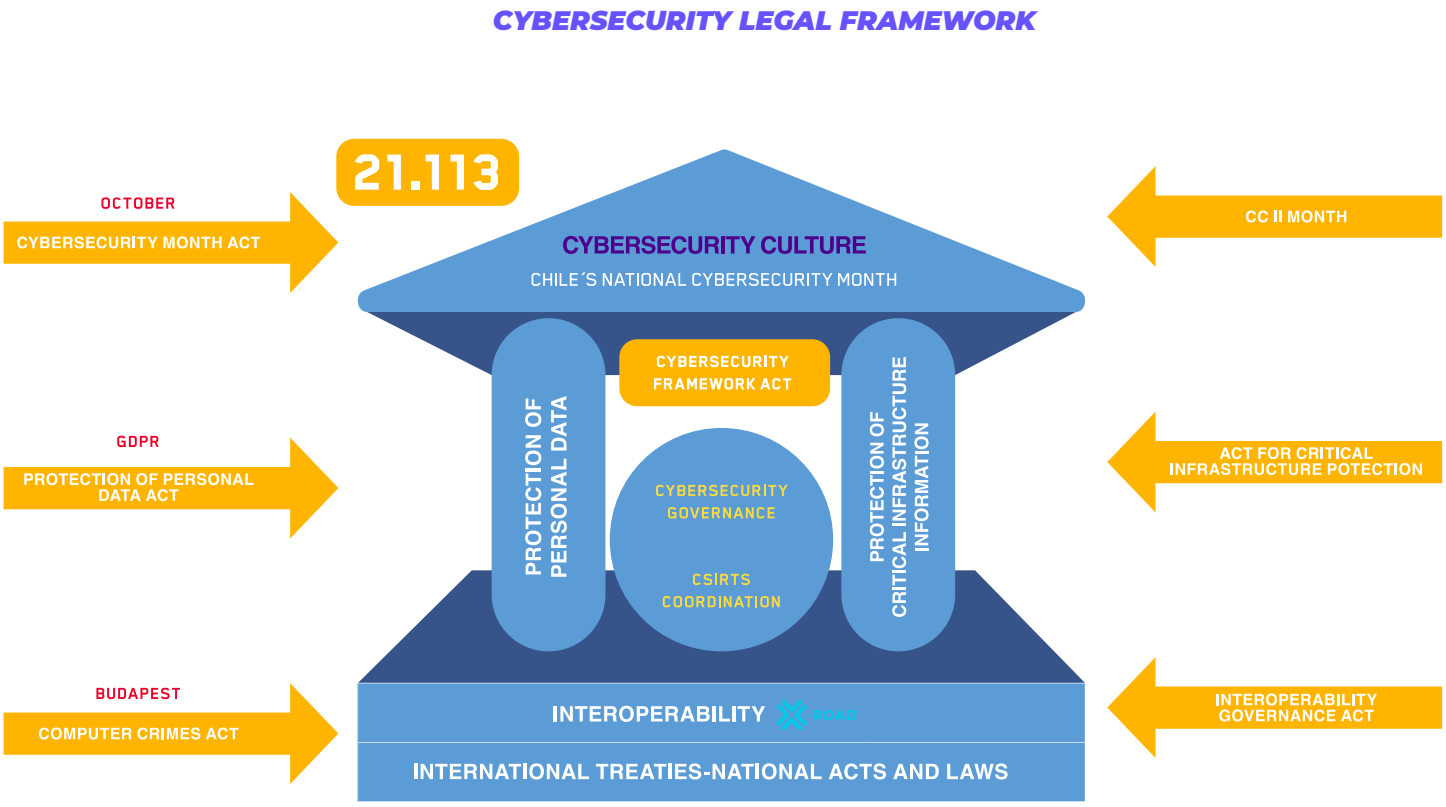
Chile has also acceded to the **Budapest Convention** on Combating Cybercrime. These efforts have sought to align current regulations with international standards and best practices;

for example, the relationship between Cybersecurity and personal data processing, the security standards to be met in regulated industries and by the Government, the classification of new cybercrimes, the definition of an international policy on Cyberspace and Cybersecurity, among others.

There must be a long-term national political agreement to commit governments' efforts to evolve from a cyber sec°urity strategy to a national cyberspace policy with a relevant cyber security component.

The cybersecurity legal framework is composed of a Computer Crime Act and the Interoperability Governance Act, in addition to the regulatory frameworks on the "Protection of Personal Data" and the "Protection of Critical Information Infrastructure" (the scope of Cybersecurity). This lies in cybersecurity governance through a National Agency that allows coordination of different sectoral CSIRTs (Computer Security Incident Response Team) responding to TI incidents and having all the necessary information to determine the "attribution" of a cyber-attack to the country. And at the same time, support the recovery of the operability, resilience, and mitigation of the adverse effects of the attacks, generating elements of evidence for their prosecution. This legal framework allows the shaping of different organizations needed to manage the National Cybersecurity System (see Figure 1).

Figure 1 Cybersecurity Legal Framework

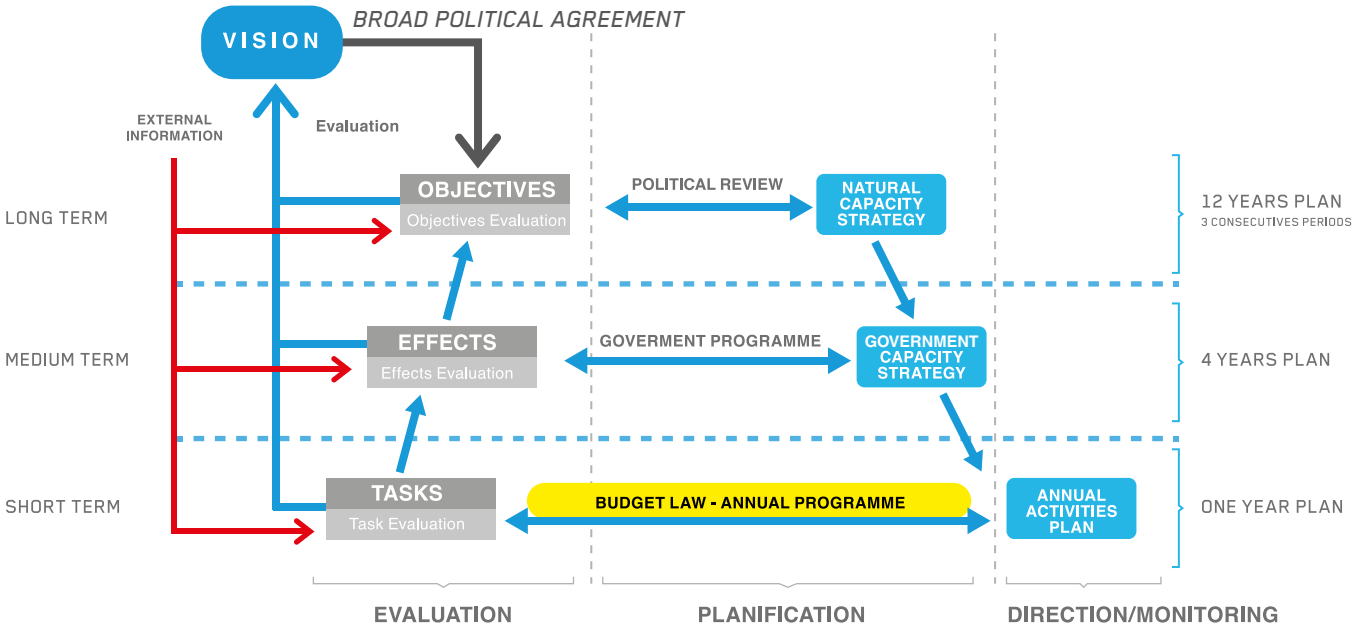


Source: Senator Kenneth Pugh Legislative Team

Building a national cybersecurity strategy for 2035, a three-horizon cybersecurity capability planning model is proposed, considering the long term (12 years), the medium-term (4 years), and the short term (one year). To allow the design of a tiered capability planning system to generate. Proposes monitoring the strategy's progress in the long term by monitoring the tasks set out each year in the Budget Law.

Figure 2 Cybersecurity Capacity Planning Model

NATIONAL CAPACITY "PLANNING MODEL"



Source: Senator Kenneth Pugh Legislative Team

OBJECTIVE 1: ***ESTABLISH A DYNAMIC, ROBUST, AND RESILIENT NATIONAL CYBERSECURITY ECOSYSTEM***

An articulated, ecosystemic, and dynamic vision is needed to address cybersecurity challenges as an emerging and priority area of public policy in a society becoming increasingly digital and reliant on the Internet and the security of its information and the infrastructure that stores, processes, and transports it. Public-private integration at the highest level and creating "digital trust" are essential, with new digital identity and address systems, interoperability, robust and redundant digital information handover networks, and the critical backup systems to be highly resilient.

It is essential to establish new cyber security governance setting the responsibilities and mandates of key governmental and non-governmental actors, reporting, and response systems. The appropriate allocation of resources to current and emerging cyber security issues and priorities is clearly defined and determined.

INTERVENTION LINES:

- Implement an interoperability system with encryption that allows traceability and information integrity and secure cross-border data transfer. An open, free and accessible, and federated platform such as X-Road, already installed by the Colombian Government and distributed by the Nordic Institute for Interoperability Solutions NIIS, is recommended.
- Incorporate a new Digital Identity system with second-factor authentication and embedded biometrics.
- Create a national security accreditation system for access to different levels of information, susceptible and classified information.
- Develop sectoral CSIRTs (Security Incident Response Teams) (Government, Defence, and critical industrial sectors).
- Create the National Cybersecurity and Critical Information Infrastructure Protection Agencies
- Create the National Cybersecurity Operations Centre (COC) to manage crises of national impact and determine the attribution of attacks together with the National Cybersecurity Council.
- Establish the National Agency for the Protection of Personal Data. Establish the National Cybersecurity Forum.
- Define the National Strategy against online disinformation campaigns.
- Strengthen fiber-optic networks with redundant links, microwave and satellite backup, and contract secure data storage services in the national territory or with similar protection.

OBJECTIVE 2: ***COMPREHENSIVE NATIONAL CYBERSECURITY CULTURE***

We must focus on the generation and availability of programs that raise awareness of Cybersecurity throughout the country, concentrating on cybersecurity risks and threats and ways to address them. This includes the development of appropriate institutions to spread Cybersecurity. It also highlights the importance of incident reporting and integrating Cybersecurity into processes to build trust and confidence in citizens' online operations.

INTERVENTION LINES:

- Develop cyber hygiene programs in society for minors from 2 to 12 years of age.
- Develop cyber security-oriented digital skills training programs throughout school education.
- Create programs that mitigate violence on networks from an early age and address cyberbullying situations in minors.
- Develop digital accompaniment programs for older adults to mitigate the risks to which they are exposed in Cyberspace.
- Carry out national cybersecurity exercises in October following Law # 21.113 and develop a solid program to propagate and update knowledge that month.
- Develop in November activities to improve the response capacity of the critical national infrastructure to incidents or digital attacks and promote and update knowledge of new threats.
- Create a national culture to identify and report cybersecurity incidents to the competent national authority.
- Strengthen confidence in using the public and private online networks and services.
- Create mechanisms to ensure the security of personal information.
- Establish alternative programs to the Military Service for the training of cyber defense specialists.

OBJECTIVE 3: ***TALENT MANAGEMENT, CAPACITY BUILDING, AND CYBER SECURITY INDUSTRY DEVELOPMENT***

Training and skills certification programs address the availability and delivery of high-quality cybersecurity training and education programs. Improve collaboration between Government and industry to ensure that educational investments meet the cybersecurity education needs of all sectors, based on a leading entity with cybersecurity competence. R&D+i are relevant issues that should be encouraged to generate a self-sufficient industry to support the country's cyber security management.

INTERVENTION LINES:

- Form the National Cybersecurity Institute (INCIBER) in Valparaiso to articulate the network of advanced research in Cybersecurity, development of cyber talent, and advanced training of instructors and specialists in different areas. Together with the establishment of evaluation and competencies, accreditation means organizing national exercises and activities to promote and spread new knowledge in Cybersecurity.

- Implement programs to identify and develop cyber-talent from the age of 14.

- Develop digital skills by delivering certified competences for pupils of all ages from 18 years old and without prior academic training as an entry requirement, using the French School 42 methodology.

- According to national and international standards, improve cybersecurity education offers, and establish training and competence accreditation programs for technical and university careers.

- Encourage the development of postgraduate scholarships in Cybersecurity at world-class universities for doctorates and post-docs.

- Encourage the incorporation of women into cybersecurity careers to address the existing gender gap.

- Annually award outstanding women in Cybersecurity.

- Recognize outstanding emerging leaders in Cybersecurity on an annual basis.

- Incentivize the training and retention of cybersecurity specialists to support the state, state services, and economic actors in general.

- Explore coordination and resources to develop enhanced cybersecurity education frameworks, with budget and spending based on national demand proactive and resourced through the budget law.

- Incentivize R&D+i in cyber security by fostering the development of a significant and efficient new national industry that projects itself into international markets, focusing on regional development and a budget indexed to a % of GDP and private funding.

- Collaborate in Cybersecurity between civilian and defense entities through dual technology projects (civilian and military use) with adequate annual resources available for their implementation.

OBJECTIVE 4: ***EFFECTIVE AND DYNAMIC LEGAL AND REGULATORY FRAMEWORKS, PROTECTION OF RIGHTS IN CYBERSPACE, AND PROSECUTION OF CYBERCRIME***

Address the various laws and regulations, along with provisions relating to Cybersecurity, including legal conditions and regulatory and procedural requirements, including cybercrime legislation ("Cyberoffense" and "Cybercrime") and human rights impact assessments. It also considers legislative frameworks related to Cybersecurity, including data protection, child protection, consumer protection, intellectual property, and the responsibilities associated with those who handle, collect, and store such information.

INTERVENTION LINES:

- Permanently update the Law on Computer Crimes based on technological evolution and Budapest Convention new additional protocols.
- Enact the new Personal Data Protection Act and its permanent harmonization with the European Data Protection Regulation (GDPR).
- Enact the Cybersecurity Governance and Critical Information Infrastructure Protection Acts with new offenses that damage CII, such as cutting fiber-optic cables and public digital infrastructure damages.
- Define a mechanism for registering SIM cards to know the identity of their owners.
- Form new PDI (Civil Police) cybercrime brigades in Chile's regions, specializing in complex investigations and basic training in establishing technological crime scenes and digital chain of custody for all police forces.
- Create the Advanced Cybercrime Investigation Laboratory in the PDI's Curauma building in Valparaíso.
- Train prosecutors to investigate and prosecute cyberoffences and cybercrime and train judges in matters relating to these digital crimes.
- Develop specialized cybercrime prosecution teams in the Public Prosecutor's Office.
- Generate policies, processes, and legislation for responsible disclosure of security breaches. Establish a guideline or framework for responsible disclosure in public and private sector organizations and the right to legal protection for those who detect and report system vulnerabilities within limited timeframes or with the consent of those responsible for the organizations.
- Establish information-sharing mechanisms on cybercrime between the national public and private sectors, including cooperation with Internet service providers and other technology providers.

- Identify and audit critical information assets, sectors, and operators regularly, establishing cyber-security requirements through policies and standards for quality supplies and services, upgrading, maintenance, and protecting IT systems and equipment.

- Adopt the Tallinn 2.0 Manual on International Law applicable to Military Cyber Operations.

OBJECTIVE 5: ***INTERNATIONAL COOPERATION AND REGIONAL LEADERSHIP IN CYBER SECURITY***

Ensure the existence and functioning of formal and informal mechanisms that enable cooperation between national and cross-border actors to promote international Cybersecurity through agreements aimed at deterring and combating cybercrime and its consequences. International collaboration should pursue effective collaboration in cybersecurity information sharing, incident management, and information management protocols and be a nexus for developing comparable legislation. Likewise, to make our country a regional benchmark for Cybersecurity by supporting international collaboration agreements between the state, academia, and the world's main cybersecurity benchmarks.

INTERVENTION LINES:

- Create a Cybersecurity Capacity Centre for Ibero-America, as a non-governmental body based in national universities, associated with the research centers network supported by the Global Cybersecurity Capacity Centre of Oxford University.

- Create a regional international exercise in Chile by INCIBER for the official teams of the different CSIRTs in the region to meet in person.

- Establish formal exchange and collaboration links between national institutions, public and private sectors, and academia, with the leading international bodies and benchmarks in cybersecurity matters, both from friendly governments and international organizations.

- Participate in the leading Internet governing bodies and those international bodies to which the State of Chile has been invited, ideally through an ambassador on a special mission for Cyberspace.

- Promulgate Chile's International Policy for Cyberspace, stating our position on security and neutrality of the network.

- Establish mechanisms for information end evidence exchange on cybercrime between different signatory countries of the Budapest Convention agreement.

- Participate, with a national delegation, in the Cyberex exercise in Spain carried out by Incibe in September each year and those organized in Greece by ENISA and the USA.

- Participate annually in the Locked Shields military exercise in Tallinn, Estonia, at the Centre of Excellence (CCDCOE).

GOALS

- Creation of the **National Cybersecurity Institute and the Ibero-American Cybersecurity Capabilities Centre** by 2023.
- Creation of a **National Agency for Personal Data Protection and Cybersecurity** and Critical Creation of all sectoral CSIRTs and National COCs by 2030
- **Investment in cybersecurity R&D&I** spending as a percentage of GDP by 0.1% by 2025 and 0.2% by 2030
- **Training 10,000 certified cybersecurity professionals** by 2035, where at least 30% will be women.
- Achieve by 2035 a **Cybersecurity Maturity** close to State 5 or dynamic for a nation, according to Oxford's University CMM., with all factors with at least a State 4 assessment and measured externally.

1- Report by Fundación País Digital, 2021

2- Cybersecurity Capacity Maturity Model for Nations (CMM) is a methodical framework designed to review a country's cybersecurity capacity. **(https://gcscc.ox.ac.uk/the-cmm)**

3- This follows the US example stating October as the "Cybersecurity Awareness Month" and European Union has the "European Cybersecurity Month".

ESTRATEGIA DE TRANSFORMACIÓN DIGITAL

DIGITAL TRANSFORMATION STRATEGY

CHILE DIGITAL 2035

CIBERSEGURIDAD/CYBERSECURITY

mesaciberseguridad@senado.cl