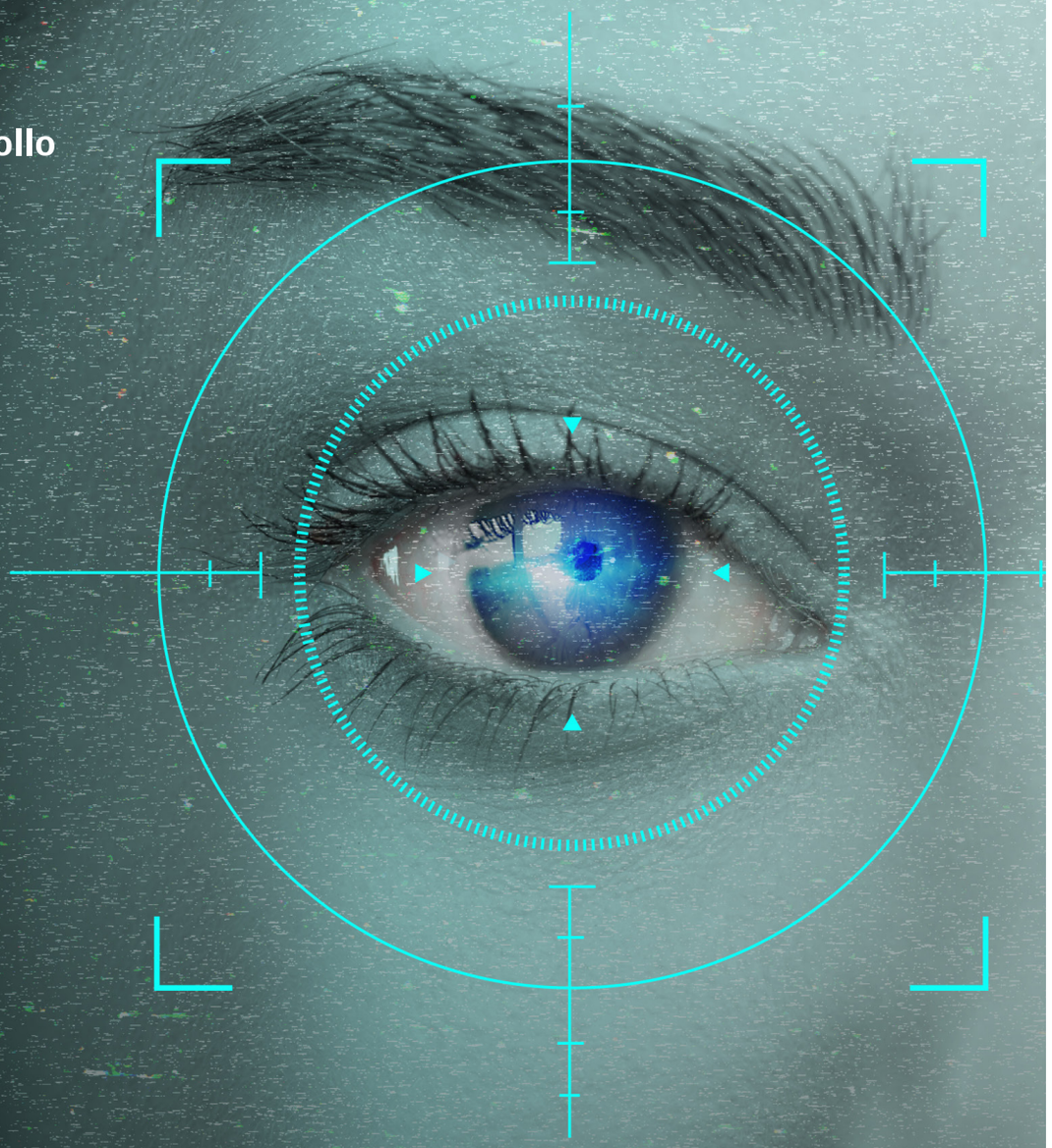
Universidad del Desarrollo
Facultad de Gobierno



WHITE PAPER

CIBERSEGURIDAD

JUAN PABLO SIMS | KENNETH PUGH | YUN-TSO LEE

INTRODUCCIÓN

La masificación de Internet es un fenómeno de la globalización que nos lleva en esta cuarta ola a preguntarnos cómo lo haremos para que sea nuestra vida segura dentro del Ciberespacio, cuya más reciente versión, el Metaverso, nos invita incluso a sumergirnos sensorialmente en él.

Necesitamos comprender entonces la importancia de la protección de los datos personales y la protección de la infraestructura crítica de la información como pilares de una nueva "República Digital", fundada en las bases de la interoperabilidad, que provea la necesaria trazabilidad de los actos y la integridad de la información, otorgándole la necesaria "certeza jurídica" a todos los actos digitales tanto del Estado, como de las personas (naturales y jurídicas) e incluso de los dispositivos conectados a la red. También debemos hacernos cargo de proteger a la democracia y el estado de derecho en la era de la inteligencia artificial, enfrentando las masivas campañas de desinformación en línea, además de proteger a la infraestructura crítica de los ataques de secuestro o bloque de sus sistemas, de actores cada vez más poderosos como lo son las amenazas persistentes y avanzadas.
Si bien se requieren nuevas leyes que regulen este nuevo mundo digital, necesitamos mejor educación digital, entendiendo que la verdadera transformación digital es la transformación de las personas y son ellas la primera y la última línea de defensa. Esa ciberhigiene desde edad temprana transforma rutinas en hábitos y robustecen una red de la cual todos dependemos, pero todos somos parte de la seguridad de ellas. Las personas serán siempre el factor que hace la diferencia en esto.

La tarea país más importante a abordar es precisamente preparar este nuevo capital intelectual humano y reconvertir a muchísimas personas que dejarán trabajos físicos y análogos por trabajos digitales, los que deben hacerse en el mejor ambiente de Ciberseguridad.

Habitar el Ciberespacio de forma constructiva y segura es el mayor desafío de la humanidad en este siglo, porque las tecnologías digitales puestas al servicio de las personas les pueden resolver sus problemas de forma más rápida y efectiva y al mundo a enfrentar mejor los conflictos medioambientales, energéticos y de alimentación.

Hace más de una década, las comunicaciones migraron desde 2G a 3G, lo que transformó la era de los conmutadores de circuitos en la era de los conmutadores de paquetes, iniciándose el proceso de transformación digital. Internet ha evolucionado desde una plataforma de intercambio de información a un pilar esencial de la vida moderna, incluyendo comercio, los servicios e infraestructura críticos, las redes sociales y la economía global en su conjunto. Miles de millones de personas se han beneficiado del crecimiento exponencial de las Tecnologías de la Información y Comunicación (TIC) y de sus oportunidades económicas y sociales. Si bien la dependencia de nuestra sociedad de la infraestructura digital está aumentando, la tecnología sigue siendo inherentemente vulnerable. La disponibilidad, integridad y la confidencialidad de la infraestructura de información y comunicaciones están siendo desafiadas por amenazas cibernéticas en rápida evolución.

La confianza de los ciudadanos y los países en el uso de las tecnologías se está viendo afectada por los problemas de ciberseguridad. Mientras disfrutamos de los dividendos de los avances tecnológicos, tenemos que enfrentar una realidad cotidiana: ¿me robarán mi billetera electrónica? ¿se verán comprometidos los datos de mi empresa? ¿mi infraestructura nacional quedará paralizada por un ataque? Estas amenazas se han transformado desde una película de ciencia ficción a un problema real de la vida cotidiana. Con el rápido crecimiento y popularidad de Internet, los gobiernos, las infraestructuras críticas, las empresas y los ciudadanos dependen en gran medida de las capacidades confiables de las redes, poniendo en riesgo el funcionamiento de estas instituciones y afectando en gran medida la vida pública y privada de la población. En la actualidad, América Latina se considera una zona de desastre importante para los ataques cibernéticos y el cibercrimen. El año 2021, los países de América Latina y el Caribe experimentaron más de 28.900 millones de intentos de ciberataque, esto es, un aumento del 600% con respecto a 2020. A esta situación la llamamos los dolores de la transformación digital, toda vez que, con perseverancia y trabajo constante, eventualmente serán mitigados por medio de la inversión en infraestructura, instituciones y profesionales capacitados. Esto permitirá continuar disfrutando de los dividendos de dicha transformación. Lo que tenemos que hacer ahora es tomar el camino correcto, a fin de dejar que este "dolor" pase lo más rápidamente.

DESAFÍOS ACTUALES DE CHILE

A continuación, resumiremos varios de los desafíos principales en nuestro país, todos los cuales contienen un elemento ligado a la ciberseguridad.

A. Confianza

Chile presenta una compleja crisis de confianza, la que tiene por objeto tanto a las instituciones como a las personas, situación que también ha afectado a varias industrias de nuestro país, especialmente producto de la pandemia vivida en los últimos años, debido a que no todas ellas se encontraban preparadas para enfrentar dicha realidad o no tuvieron los niveles de respuestas adecuados a las exigencias de sus clientes.

En tal sentido, la confianza constituye uno de los ejes centrales en el desarrollo digital de cualquier país. Por ejemplo, todo el comercio electrónico se fundamenta en la seguridad que las transacciones ocurrirán en la realidad, que podemos digitar los números de la tarjeta de crédito en una aplicación, que el dinero se transferirá y que el producto llegará a destino sin inconvenientes. En consecuencia, la confianza que surge con motivo de los usos de las tecnologías representa la plataforma habilitante para el crecimiento de una economía digital sana y vibrante.

B. Valores universales y deberes digitales

Los valores universales representan el conjunto de exigencias que se reclaman como parte del progreso de las sociedades, especialmente en lo que respecta al universo digital. En efecto, la protección de la adquisición y uso de datos personales, la sanción a nuevas formas de delitos informáticos, el acceso universal a internet o el derecho a la seguridad informática, constituyen una nueva categoría de valores que han surgido de manera conjunta con la masificación de internet y el desarrollo digital.

Por su parte, estos valores tienen una contracara que dicen relación con la ciberhigene, entendida como la conducta responsable y cautelosa que deben adoptar los usuarios al utilizar servicios informáticos. En ese sentido, este concepto se conecta con la toma de conciencia respecto a los riesgos que representa un uso irresponsable de internet, siendo uno de los aspectos basales de esta nueva economía, además de los deberes educativos y formativos que deben ser inculcados en los ciudadanos, especialmente los más vulnerables (como menores de edad y adultos mayores).

C.- Seguridad

Chile se encuentra viviendo un aumento sostenido en la cantidad y entidad de delitos. Según la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) realizada el año 2021, la percepción del aumento de la delincuencia alcanzó al 86,9% (en comparación con el 84,3% del año 2020). Por su parte, a victimización de los hogares urbanos en el caso de los delitos cibernéticos, alcanzó un 10,1%. Los delitos cibernéticos se refieren a estafas en compras por internet, suplantación de identidad en cuentas de correo electrónico o redes sociales, suplantación de identidad en cuentas bancarias o tarjera de crédito, amenazas de daño o ataque físico, acoso u extorsión y destrucción remota intencional del disco duro o contenidos del computador.

En una economía cada vez más digitalizada, el uso de datos y la analítica se vuelven temas relevantes, dentro de los cuales destacan la seguridad y protección de datos de los usuarios, de las empresas y del gobierno por la sensibilidad de éstos. En la actualidad, el 67% de las empresas en Latinoamérica no tienen responsables de ciberseguridad, lo que demuestra que esta situación tiene un enfoque reactivo y no proactivo, además de una baja cultura de los directivos de las empresas de equiparar el nivel de protección de datos ante la llegada de tecnologías habilitadoras, como lo es el 5G y la fibra óptica.

PRINCIPIOS RECTORES

A.- Neutralidad tecnológica

Constituye el pilar fundamental del desarrollo digital y de la industria de las telecomunicaciones en Chile y el mundo. Se define como aquel en que ninguna tecnología, ningún proveedor ni ningún equipo, independiente del país de origen, será favorecido o perjudicado, siendo los operadores relevantes o los usuarios finales libres de elegir aquella que mejor se adecúe a sus necesidades. En Chile, tanto la industria digital como su regulación tienen una larga tradición de respeto a dicho principio, lo que se ha manifestado en la normativa y jurisprudencia relacionada a dicha industria. En consecuencia, resulta necesario que cualquier política pública tenga la suficiente flexibilidad y capacidad de adaptarse a los cambios tecnológicos que cada vez se van produciendo de manera más rápida y vertiginosa.

B.- Responsabilidad compartida

Una adecuada protección y promoción de la ciberseguridad requiere compartir la responsabilidad entre los distintos actores de la industria, ya sea a nivel de oferta, a nivel de usuario y a nivel de regulador. Cabe destacar que el ecosistema en esta materia es muy amplio, los cuales, si bien operan de manera individual dentro de sus respectivos ámbitos de acción, deben estar debidamente coordinados y regulados según los mismo criterios o estándares internacionales, para dar una respuesta conjunta frente a un incidente. El hecho de compartir esta responsabilidad en el actuar implica mejorar exponencialmente las condiciones al momento de producirse algún ataque.

La ciberseguridad es un desafío común que enfrenta toda la sociedad, incluidos los gobiernos, los reguladores, las organizaciones de la industria, las organizaciones que generan estándares, las empresas y los proveedores de tecnologías, ya sean de hardware o software. Si la seguridad cibernética se eleva a la altura de una ideología determinada o se relaciona con factores políticos, los desafíos del ciberespacio no podrán resolverse.

En general, podemos predefinir las siguientes responsabilidades:

- Los reguladores se encargan de la legislación, su aplicación y la supervisión de seguridad de extremo a extremo;
- Las organizaciones de estándares definen requisitos y soluciones modelos;
- El proveedor del equipo responde de la seguridad del producto en la capa inferior;
- Los operadores son responsables de la implementación de la red y la seguridad de la respectiva operación y mantenimiento;
- El proveedor de servicios es responsable de la seguridad de la aplicación.

C.- Colaboración dentro de la competencia (“coopetencia”)

La ciberseguridad revela una paradoja compleja de solucionar, puesto que cada empresa o institución tiene la obligación de tomar conciencia propia, ojalá a nivel gerencial y de accionistas, acerca de los riesgos que representa la utilización de las tecnologías en los procesos productivos, en la administración del negocio en particular y en la relación con el cliente. Asimismo, las decisiones estratégicas de cada empresa o institución y la competencia legítima que se produce entre ellas obligan al hermetismo en su accionar, por lo que resulta difícil hacer público cualquier decisión de negocio o cualquier hecho que afecte sus intereses comerciales y su reputación. Sin embargo, la ciberseguridad necesita salir de esta zona hermética e incluir el concepto de colaboración como un nuevo eje central del actuar de las empresas, al menos en esta dimensión, puesto que estamos en presencia de un problema global y que va a afectar, sin duda alguna, a cada uno de los actores de la sociedad.

D.- Cooperación con la autoridad

Este principio implica que tanto los órganos de administración del Estado como los privados deben cooperar con la autoridad competente en la materia para resolver los incidentes de ciberseguridad. Adicionalmente, en caso de ser necesario, también deberán cooperar entre distintos sectores, teniendo en cuenta la interconexión e interdependencia de los diversos sistemas y servicios.

La concreción de este principio resulta fundamental, toda vez que responde a la necesidad de comunicar a las autoridades competentes los respectivos incidentes de ciberseguridad y, además, la resolución conjunta de los mismos. Tanto el Estado como los privados debieran avanzar rápidamente en mejorar sus tecnologías, su capital humano y sus defensas a los ciberataques, sin perjuicio de lo cual será el propio Estado quien cumpla un rol esencial en el fortalecimiento de sus capacidades y en la formación y educación de las habilidades informáticas y digitales.

E.- Ciberseguridad como factor habilitante del desarrollo digital de Chile

El desarrollo digital ha avanzado de manera rápida en Chile, tanto en el despliegue de redes de alta velocidad como en el acceso a internet y en la adopción de la tecnología. Sin embargo, cada uno de los mencionados avances descansa sobre una premisa básica e indesmentible: la confianza. Confianza en, por ejemplo, i) incluir los datos de una tarjeta de crédito en un sitio de e-commerce, ii) efectuar transacciones electrónicas en una institución financiera, iii) postular a un subsidio del Estado, iv) solicitar un certificado o realizar un trámite ante el Registro Civil, o v) tener un vida digital en distintas plataformas sociales. Y esa confianza se traduce, en la práctica, en la ciberseguridad como una plataforma habilitante para que todos los usuarios puedan desenvolverse libremente y, de esa manera, se desarrolle la economía digital. En definitiva, la ciberseguridad trae consigo confianza hacia el mercado, hacia los consumidores y hacia el país en general.

REGULACIÓN EN CIBERSEGURIDAD, CIBERCRIMEN Y PROTECCIÓN DE DATOS

A diferencia de lo ocurrido con el desarrollo tecnológico en el país, el avance regulatorio no ha tenido el mismo ritmo. Los principales cuerpos normativos a tener en cuenta son los siguientes:

- Política Nacional de Ciberseguridad, período 2017-2022 2022-2027.
- Nueva Ley de Delitos Informáticos (N°21.459)
- Proyecto de Ley de Protección de Datos Personales
- Normativa técnica sectorial, emitidas por los reguladores de las industrias de telecomunicaciones, mercado financiero, casinos, seguridad social y energía.
- Estándares internacionales: ISO/IEC 27001, 27701, IEC 62443, ISO 15408, GSMA NESAS&SCAS y GSMA 5G “knowledge Base best practice”, entre otras.
- Mediciones internacionales: i) Modelo de Madurez de Oxford (CMM) y ii) Índice de Seguridad Global (GCI) de la Unión Internacional de Telecomunicaciones (UIT).
- Experiencia comparada: Brasil, Alemania, Finlandia, Singapur, Israel, Estonia, España Y Reino Unido.
- Estrategia Transformación Digital CHILE 2035, realizado por el Senado de Chile y CEPAL.

Proyecto de Ley Marco de Ciberseguridad

Su finalidad es establecer un marco general e implementar la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, la formación de una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado y resguardar la seguridad de la información de las personas en el ciberespacio. En ese sentido, se propone la creación de una nueva “Agencia Nacional de Ciberseguridad” (ANCI), encargada de normar y coordinar la protección de la infraestructura crítica de la información.

FACTORES QUE AYUDAN A DESARROLLAR EL MARCO DE LA CIBERSEGURIDAD, LA RESILIENCIA CIBERNÉTICA Y, POR ENDE, LA ESTABILIDAD DIGITAL Y ECONÓMICA DE CHILE CIBERSEGURIDAD, LA RESILIENCIA CIBERNÉTICA Y, POR ENDE, LA ESTABILIDAD DIGITAL Y ECONÓMICA DE CHILE

La ciberseguridad representa una plataforma habilitante del desarrollo social y de la economía digital del país. Esto implica un trabajo incesante, ya que se requerirá de una actualización permanente de nuestros sistemas informáticos y, especialmente, de una formación continua de la sociedad en su conjunto.

Proponemos tener en cuenta los siguientes factores que colaborarán con el desarrollo de un país más ciberseguro y un ecosistema más educado y resiliente:

A.- Apertura de mercado y aceptación de todas las soluciones disponibles.

Para una efectiva defensa ante ciberataques resulta imperioso no cerrarse a ninguna tecnología, sino que debemos siempre tener la libertad de elegir aquella que más se adecúe a los intereses y necesidades de cada usuario. Las políticas públicas deben defender el principio de neutralidad tecnológica, sin promover ni incentivar la discriminación entre ellas. Mientras más opciones existan y más competencia se genere en este mercado, más protegidos estaremos de los ciberataques, ya que también generará mayor inversión en investigación y desarrollo, lo cual traerá las tecnologías más avanzadas.

B.- Promoción de soluciones o tecnologías que promueven la responsabilidad

La seguridad de los sistemas informáticos y de las redes que se construyen para prestar servicios que pueden catalogarse de esenciales, como la energía, las telecomunicaciones o los servicios sanitarios, representan un engranaje complejo y altamente técnico. Por ello, el principio de responsabilidad resulta esencial, según el cual la seguridad de las redes, sistemas y datos pertenece a aquel que las ofrece o las opera, sin importar si éste es un ente público o privado. Las políticas públicas o regulaciones que se generen en un país deben evitar cualquier intento de dispersar, evadir o hacer que la responsabilidad sea difusa, dado que es la única manera de generar accountability en el fabricante de equipos o en el respectivo prestador de servicio.

La existencia de tecnologías abiertas, que requieran de integradores múltiples o que tengan problemas de soporte, puede generar vulnerabilidades importantes que, a la hora de algún incidente, no permitan determinar con claridad al responsable de la seguridad de los sistemas y redes. Por lo tanto, se requieren actores y tecnologías maduras y probadas, que no afecten los ciclos de vida de la tecnología y que cuenten con una matriz de responsabilidad nítida, para los efectos de hacerla valer cuando sea necesario. No obstante, esto no puede ir en desmedro de la promoción de innovación y desarrollo de nuevas tecnologías, siempre entendiendo la necesidad de agilizarlas y fomentarlas.

C.- La ciberseguridad es un asunto eminentemente técnico, basado en evidencia tecnológica

Con el desarrollo y masificación de internet, se ha generado, paralelamente, una industria enfocada en la realización de fraudes y ataques a las redes y sistemas informáticos. Actualmente, existe una creciente industria global de empresas que se dedican a resolver tales dificultades, a instalar soluciones para cada cliente, a prevenir de los riesgos y a capacitar a los trabajadores. Más allá de las motivaciones que tengan quienes realizan ataques o fraudes informáticos, la seguridad de las redes y sistemas sobre las cuales se ejecutan tales delitos es un asunto esencialmente técnico, que se enfrenta de manera técnica y se supera con soluciones técnicas. Por lo tanto, consideraciones ajenas a la evidencia empírica no deben tener cabida ni en las políticas públicas ni en las regulaciones, ya que ello desvirtúa el sentido y la esencia de la protección a la seguridad de redes y sistemas, convirtiéndolo en un nido de intereses geopolíticos que responden a otras motivaciones y que no tienen como finalidad principal la preservación de la ciberseguridad. La protección de nuestros sistemas requiere el más alto grado de profesionalismo y responsabilidad, por lo que debemos asegurarnos que la creación y construcción de este ecosistema sea siempre guiado por los motivos correctos, a fin de que la respuesta a un ciberataque sea siempre realizada desde un prisma imparcial.

¿QUÉ HACEMOS AHORA?

En virtud de la realidad descrita y debido al desafío creciente y permanente que debemos enfrentar como país con respecto a la ciberseguridad, sugerimos enfocarnos y avanzar en los siguientes aspectos:

A. Actualizar la legislación y su regulación respectiva.
Acciones principales: i) agilizar la tramitación del Proyecto de ley marco de ciberseguridad y del Proyecto de ley de protección de datos; ii) adecuar la regulación sectorial a la nueva legislación.

B.Activar el conocimiento y capital humano en ciberseguridad.
Acciones principales: i) acuerdos público-privados con instituciones de educación; ii) creación de un instituto de ciberseguridad.

C. Reforzar las capacidades del Estado.
Acciones principales: i) cursos de formación al interior del Estado; ii) agilizar la creación de la Agencia Nacional de Ciberseguridad; iii) agilizar la implementación de la Ley de Transformación Digital del Estado;

D. Mantener la apertura de mercado.
Acciones principales: i) mantener el respeto irrestricto al principio de neutralidad tecnológica y no discriminación; ii) consagrar dicho principio de manera expresa en el proyecto de ley marco de ciberseguridad.

E. Seguir estándares igualitarios e internacionalmente aceptados.
Acciones principales: i) continuar utilizando estándares internacionalmente aceptados, maduros y probados, tales como las normas ISO, 3GPP y GSMA, entre otros.

F. Transformación digital de las empresas.
Acciones principales: i) tomar los resguardos adecuados al momento que las instituciones y empresas inicien sus procesos de transformación digital; ii) contar con un profesional (o área, dependiendo del tamaño de la empresa o institución) dedicado exclusivamente a los asuntos de ciberseguridad (CISO)

G. Reconversión laboral.
Acciones principales: i) ejecutar programas de capacitación a los desconectados, tanto en el sector público como en el privado; ii) generar incentivos para la realización de dichos programas de capacitación.

H. Protección y gobernanza de los datos.
Acciones principales: i) acelerar la tramitación del proyecto de ley de protección de datos actualmente en el Congreso Nacional; ii) ejecutar programas de capacitación y formación para la debida toma de conciencia que significa la entrega de datos y su uso en el ciberespacio.

I. Aplicación de modelos de madurez.
Acciones principales: i) implementación de modelos de madurez en las diversas instituciones del sector público y empresas del sector privado, tales como el GCI de la ITU o el CMM de Oxford.

J. Análisis y aplicación de mejores prácticas.
Acciones principales: i) generar alianzas con organismos internacionales, a fin de establecer una colaboración en compartir mejores prácticas.

K. Chile como hub digital en ciberseguridad.
Acciones principales: i) ejecución de programas de talento digital; ii) crear las condiciones para fomentar la exportación de servicios; iii) formar especialistas en ciberseguridad.